CUBIC SIEVES, A PRIMITIVE-RATIO CUT AND A 20/37 BOUND FOR THE *abc* EXCEPTIONAL SET

RUIYI ZHANG

ABSTRACT. We prove $N_1(X) \ll_\varepsilon X^{20/37+\varepsilon}$, where $N_\lambda(X)$ counts the *abc* triples of exponent λ in $[1, X]^3$. The previous full bound was $X^{13/20+\varepsilon}$. We use the anatomic reduction of Bernert, Browning, Lichtman and Teräväinen. Five families add new rows. The first two are an archimedean cover and a row from Heath-Brown's uniform bound for diagonal cubic curves. Spacing gives 30 two-arm clauses. Cubic characters and a fourth moment of Dirichlet L-functions give the cubic-sieve rows. Cochrane and Shi's fourth moment gives the moment rows. An exact Farkas certificate with 394 633 leaves gives exponent 20/37 for the box count. On each leaf the multipliers of all rows except nonnegativity sum to at most 586/201. Exact rows are included in this sum. This pays for the losses at $\lambda = 1$.

1. INTRODUCTION

For this paper $\mathbb{N} = \{1, 2, \ldots\}$. For $n \neq 0$ put $\mathrm{rad}(n) = \prod_{p|n} p$, and write $\omega(n) = \#\{p : p \mid n\}$, with $\omega(1) = 0$. Following [2], call $(a, b, c) \in \mathbb{N}^3$ with $\gcd(a, b, c) = 1$ an *abc triple of exponent* λ if

$$a + b = c, \qquad \mathrm{rad}(abc) < c^\lambda. \tag{1.1}$$

Let $N_\lambda(X)$ count these triples in $[1, X]^3$. The *abc* conjecture of Masser and Oesterlé implies that $N_\lambda(X) = O_\lambda(1)$ for $\lambda < 1$, so $\lambda = 1$ is the endpoint of interest.

The bound $N_\lambda(X) \ll_\varepsilon X^{2\lambda/3+\varepsilon}$ is classical [2, Proposition 1.1]; it comes from de Bruijn's count [5] of integers with restricted radical. For $\lambda \geq 2$, Kane's result [10] gives $N_\lambda(X) \ll_\varepsilon X^{\lambda-1+\varepsilon}$ [2, Section 1]. On $2 \leq \lambda \leq 3$ it matches $N_\lambda(X) \gg X^{\lambda-1-\varepsilon}$. Granville's unpublished work gives the lower bound for $1 < \lambda \leq 3$, as reported in [2, Section 1]. The question is Mazur's. It can hold only for $\lambda \leq 3$, since $N_\lambda(X) \leq \#\{(a, b, c) \in [1, X]^3 : a + b = c\} = O(X^2)$. Browning, Lichtman and Teräväinen [3, Theorem 1.2] gave the first power saving below $2\lambda/3$, for $0.99 < \lambda < 1.001$. Bernert [1, Theorem 1] proved

$$N_\lambda(X) \ll_\varepsilon X^{(23\lambda+3)/40+\varepsilon} \qquad (0 < \lambda < 2), \tag{1.2}$$

so $N_1(X) \ll_\varepsilon X^{13/20+\varepsilon}$. In the merged paper, [2, Theorem 1.2] states (1.2) for $0 < \lambda \leq 2$. Its Theorem 1.3 gives 0.6 for $0 < \lambda < 1$, with a constant depending on λ. At $\lambda = 1$: a remark at the end of [1, Section 4] sketches $8/13 = 0.6153\ldots$; Li [11] obtains $56/85 = 0.6588\ldots$ from the method of [3], its limit without further optimisation by his account.

2020 *Mathematics Subject Classification.* Primary 11D75; Secondary 11N25, 11N36, 11L40, 11D25, 11Y16.

Key words and phrases. abc conjecture, exceptional set, radical, anatomy of integers, power sieve, character sums, Farey fractions, linear programming certificate.

Theorem 1. *$N_1(X) \ll_\varepsilon X^{20/37+\varepsilon}$, where $20/37 = 0.5405\ldots$*

Since $N_\mu \le N_1$ for $\mu \le 1$, Theorem 1 also improves [2, Theorem 1.3] on $0 < \mu < 1$, with a constant independent of μ. Among the estimates cited here, the resulting exponent is $\min\{2\mu/3, 20/37\}$ for $0 < \mu \le 1$. Thus the new exponent is best known for $30/37 < \mu \le 1$; it ties the classical exponent at $\mu = 30/37$. Its crossing with the Bernert exponent alone is $\mu = 689/851$.

Section 2 recalls the anatomic reduction of [3, 1, 2]. Fix $\varepsilon_0 > 0$ and $d = d(\varepsilon_0)$. Every triple lies in a box. In a box, each side is a fixed coefficient times $\prod_{i\le d} \mathfrak{s}_i^i$. The roots $\mathfrak{s}_i$ have fixed dyadic sizes. The three side values are pairwise coprime. Let $\mathcal{B}_d$ count the root-factorization tuples in a box, with distinct factorizations counted separately, and put $D = \log_X \mathcal{B}_d$. The proof is the chain. Section 2 works at a generic scale X and exponent λ; Lemma 12.2 applies it at the scale Y of (2.1), with $\lambda := \mu$ and base-Y logarithms. The quantity V_s is the weighted exponent of the root product, excluding its fixed coefficient, as defined in Section 6; $h_d = d(d+1)/2$. The quantity ρ is the largest finite right-hand-side shift in Lemma 12.2. The bound on ρ holds for $Y \ge Y_0(\varepsilon_0, d)$. Smaller Y contribute $O_{\varepsilon_0,d}(1)$, and $\mu \le 0$ contributes nothing (Section 13).

$$N_1(X) \ll (\log X)^2 \max_{Y\le X,\ \mu\le 1} N_\mu^*(Y), \qquad N_\mu^*(Y) \ll Y^{\varepsilon_0} \max \mathcal{B}_d,$$

$$D \le \frac{20}{37} + \Lambda_U \rho, \qquad \Lambda_U = \frac{586}{201}, \qquad \rho \le 19\varepsilon_0,$$

from (2.1), (2.3), Theorem 2 with Lemma 12.1, and Lemma 12.2. Since $19\Lambda_U + 1 = \frac{11335}{201}$, choosing ε_0 with $\frac{11335}{201}\,\varepsilon_0 < \varepsilon/2$ proves Theorem 1.

The inequalities for D are linear in 28 exponents. They are the root and tail coordinates of the three sides, D, and three auxiliary Fourier variables. BBLT's Theorem 1.3 gives the 3/5 bound. Its Proposition 6.1 lists the 22 inherited inequalities used here. We add the tail rows and the cut. Tail roots (Section 3) of index at least seven cost X^{τ_s} to enumerate. Here $\tau_s = s - \sum_{i\le 6} s_i$. The tail product is at least X^{v_s}, where $v_s \ge 7\tau_s$. The cut (Section 5) fixes all but two coprime products u, v on two sides:

$$\gcd(u, v) = 1, \qquad u \equiv \xi v \pmod{M}, \qquad 0 < u \le U_{\mathrm{cut}}, \quad 0 < v \le V_{\mathrm{cut}}.$$

Here M is built from roots on the third side, and ξ lies in one of $X^{o(1)}$ classes. Lemma 4.1 counts these by $1 + 2U_{\mathrm{cut}}V_{\mathrm{cut}}/M$. There are

$$3\,(64^2 - 1)\,127 = 1\,560\,195 \tag{1.3}$$

cuts.

The paper adds five further families.

- *Archimedean* (Section 6). One of the side values n_a, n_b is at least $n_c/2$. In the limiting coordinates, $V_a, V_b \le V_c$, and $V_c \le V_a$ or $V_c \le V_b$. At finite scale, $V_a, V_b \le V_c + \varepsilon_0/2$, and one of $V_c \le V_a + 3\varepsilon_0/2 + \log_Y 2^{1+h_d}$ or $V_c \le V_b + 3\varepsilon_0/2 + \log_Y 2^{1+h_d}$ holds.
- *Cubic* (Section 7). Fix all roots but the three cube roots. Heath-Brown's bound [8, Theorem 1.3] for primitive points on $\alpha x^3 + \beta y^3 = \gamma z^3$, uniform in the coefficients, gives $D \le L - p_3$. Here L and p_i are as in Section 2.
- *Spacing* (Section 8). Consecutive ℓth powers are far apart: 30 two-arm clauses.

- *Cubic sieve* (Section 9). Write one side as Mx^3. Sieve with cubic characters modulo primes $p \equiv 1 \pmod 3$. The error term needs a smooth fourth moment of character sums. It comes from the fourth moment of Dirichlet L-functions in [6, Lemma 4]: 1774 clauses.
- *Moments* (Section 10). Expand the congruence of the cut modulo M by characters. The fourth moment of Cochrane and Shi [4, Theorem 1] bounds the nonprincipal part: 188 976 clauses.

Section 11 proves $D \le 20/37$ from these rows. The certificate is a finite trie. Each internal node splits on one clause, one child per arm. Each leaf carries nonnegative rational Farkas multipliers. There are 394 633 leaves, depth 49, and no infeasible leaf. On a leaf the multipliers of all rows except nonnegativity sum to at most $\Lambda_U = 586/201$, whence the term $\Lambda_U \rho$. This includes exact rows. A point of the installed system attains 20/37; the qualification on this optimum appears in Section 11.2.

Section 12 treats $\mu = 1$. In the proof of Theorem 1, the dyadic reduction only requires $0 < \mu \le 1$. At this endpoint the row $L \le 1$ of [2] is unavailable: the proof of [2, Theorem 1.3] uses $\varepsilon_0 \le (1-\mu)/3$. We use $L \le 1 + 3\varepsilon_0/4$ instead. The L-native Fourier and geometry rows cost $18\varepsilon_0$ and $6\varepsilon_0$. After the choice of Y_0 in Lemma 12.2, every new row costs at most $2\varepsilon_0$. Hence $\rho = 18\varepsilon_0 + o_{\varepsilon_0,d}(1)$ and $\Lambda_U \rho = \frac{3516}{67}\,\varepsilon_0 + o_{\varepsilon_0,d}(1)$.

The proof in [2] does not use the determinant method; [3] used it together with Thue equations. Lemma 4.1 is an elementary lattice-point count of the kind used in [2, Proposition 4.1]. The cut applies it to two sides at once, with modulus M built from roots on the third side.

Imported statements are cited where used. Citations of [2] refer to arXiv: 2410.12234v2 (to appear in C. R. Math.); each imported statement was checked against it. The dyadic reduction (2.1) is only stated in [2, Section 2]; Section 2 proves it. Appendix A reproves the estimates of [2, Propositions 2.3, 3.1 and 4.1] for our boxes. They use the divisor bound, the count of solutions of $x^j - y^j = m$ (Lemma A.1) and the lattice-point bound [7, Lemma 3] (Theorem C). The new rows use the cubic bound [8, Theorem 1.3] and the fourth moments [6, Lemma 4] and [4, Theorem 1]. The cubic-sieve character expansion (Section 9) also uses the classical Jacobi-sum bound [9]. No conjecture is assumed. Theorem 2 has multiplier bound Λ_U. It is computer-assisted and uses a certificate checked by the standard-library programs in Appendix C. The analytic reductions and row families are proved in the text.

2. The anatomic reduction

Throughout this section $0 < \lambda \le 2$, $\varepsilon > 0$ is arbitrary, $\varepsilon_0 > 0$ is fixed before X, and $d = d(\varepsilon_0)$. We take $\varepsilon_0 \le 4/7$, so that the folded index $k = \lceil 4/\varepsilon_0 \rceil$ of [2, Lemma 2.2] is at least 7 (Section 3.1). Implied constants depend only on $\varepsilon, \varepsilon_0, d$; λ occurs only through the displayed $\ll_\lambda$ in (2.1). They never depend on the box, the coefficients or X.

Write $N^*_\lambda(X)$ for the number of triples counted by $N_\lambda(X)$ that satisfy in addition $c \ge X/2$ and $\operatorname{rad}(abc) \ge c^\lambda/2$. A dyadic decomposition and the pigeonhole principle give

$$N_\lambda(X) \ll_\lambda (\log X)^2 \max_{1 \le Y \le X} \max_{\mu \le \lambda} N^*_\mu(Y), \tag{2.1}$$

as in [2, Section 2]. In the application $\lambda = 1$, and the bounds below for $N^*_\mu(Y)$ are uniform in $0 < \mu \le 1$ (Lemma 12.2).

Proof of (2.1). Let (a, b, c) be counted by $N_\lambda(X)$. Then $c \ge 2$ and $a, b < c \le X$. Choose $l \ge 1$ with $c \in (X2^{-l}, X2^{1-l}]$ and put $Y = X2^{1-l} \le X$. Thus $Y/2 < c \le Y$. Put

$$\mu_i = \lambda - i/\log_2 X \qquad (0 \le i \le \lceil \lambda \log_2 X \rceil).$$

Here $\log_2 X = (\log X)/(\log 2)$. There are $O(\log X)$ such exponents, all at most λ, and the last is at most 0. With $r = \mathrm{rad}(abc)$, we have $r < c^{\mu_0}$ and $r \ge 1 \ge c^{\mu_m}$ for the last index m. Choose the largest i with $r < c^{\mu_i}$. Then $r \ge c^{\mu_{i+1}} \ge c^{\mu_i}/2$, since $c \le X$. Hence the triple is counted by $N^*_{\mu_i}(Y)$. There are $O(\log X)$ choices of Y and $O(\log X)$ choices of μ_i, which proves the claim. □

For $\mu \le 0$, $N^*_\mu(Y) = 0$: its defining condition would require $1 \le \mathrm{rad}(abc) < c^\mu \le 1$. Thus the maximum in (2.1) may be restricted to $0 < \mu \le \lambda$.

For $n \ge 1$ write $[n] = \{1, \dots, n\}$. Here $x \sim A$ means $A \le x < 2A$, as in [1]; [2] writes $x \sim A$ for $x \in (A, 2A]$.

Let $d \in \mathbb{N}$ and $(a_0, b_0, c_0) \in \mathbb{N}^3$. Let $\mathbf{A}, \mathbf{B}, \mathbf{C} \in \mathbb{N}^d$ have entries powers of two, 1 included. Put $\mathfrak{a}_0 = a_0$, $\mathfrak{b}_0 = b_0$, $\mathfrak{c}_0 = c_0$ and

$$\mathcal{B}_d = \#\Big\{ (\mathfrak{a}_i, \mathfrak{b}_i, \mathfrak{c}_i)_{i=1}^d \in \mathbb{N}^{3d} : \begin{array}{c} \mathfrak{a}_i \sim A_i,\ \mathfrak{b}_i \sim B_i,\ \mathfrak{c}_i \sim C_i \quad (1 \le i \le d), \\ a_0 \prod_{i \le d} \mathfrak{a}_i^i + b_0 \prod_{i \le d} \mathfrak{b}_i^i = c_0 \prod_{i \le d} \mathfrak{c}_i^i, \\ \gcd\big(\prod_{i=0}^d \mathfrak{a}_i, \prod_{i=0}^d \mathfrak{b}_i, \prod_{i=0}^d \mathfrak{c}_i\big) = 1 \end{array} \Big\}. \tag{2.2}$$

For a side write $S_j \in \{A_j, B_j, C_j\}$ for its dyadic root size. When the side s must be named, write $S_{s,j}$. Recall $h_d = d(d+1)/2$. Equation (2.2) counts root-factorization tuples, not distinct side-value triples; different factorizations are counted separately. It is the B_d of [2], under our dyadic convention, with no condition within a side. We write $\mathcal{B}_d$ to avoid a clash with the size B_d.

Every interval $[A, 2A) \cap \mathbb{N}$ has exactly A integers, including $[1, 2) \cap \mathbb{N} = \{1\}$. We keep every root coordinate, including those equal to 1. The statements of [2, Propositions 2.3, 3.1 and 4.1] assume windows $(A, 2A]$ with $A \ge 1$, which exclude roots equal to 1. So we do not cite them for our boxes. We rerun the window-dependent steps of the reduction below. Appendix A proves the pair, Fourier and geometry bounds in our convention (Lemmas A.2, A.3 and A.4). Their constants depend only on ε_0 and d.

Roots equal to 1 occur: in [2, Lemma 2.2], $m_j = \prod_{p^j \| n} p$ and $n_j = m_j$ for $j \ne k$, the folded index. So $n_j = 1$ unless some prime has multiplicity exactly j. As n has at most $\omega(n)$ distinct multiplicities, all but at most $\omega(n)$ indices $j \le d$, $j \ne k$, give $n_j = 1$. Our convention assigns these roots the size $A_i = 1$ and keeps all d indices in (2.2). By the proof of [2, Proposition 2.1], each $\varepsilon_0 > 0$ has a $d = d(\varepsilon_0)$ with

$$N^*_\lambda(X) \ll_{\varepsilon_0} X^{\varepsilon_0} \max \mathcal{B}_d, \tag{2.3}$$

the maximum over pairwise coprime $1 \le a_0, b_0, c_0 \le X^{\varepsilon_0}$ and dyadic $A_i, B_i, C_i \in [1, X]$ with

$$\begin{gathered} 2^{-O_d(1)} X^\lambda \le \prod_{j \le d} A_j B_j C_j \le X^{\lambda + 3\varepsilon_0/4}, \\ \prod_{j \le d} A_j^j \le X, \qquad \prod_{j \le d} B_j^j \le X, \qquad X^{1-\varepsilon_0/2} \le \prod_{j \le d} C_j^j \le X, \end{gathered} \tag{2.4}$$

The power of two depends only on d. We rederive the lower bounds below. The upper bounds and the pigeonhole step of the source proof hold verbatim under $[A, 2A)$, since $A_i \le \mathfrak{a}_i < 2A_i$. The lower bound uses the nontrivial branch of [2, Lemma 2.2]: $\varepsilon_0 < 4$, so the parameter $\varepsilon_0/4 < 1$ and $k = \lceil 4/\varepsilon_0 \rceil \le d$. Since $c \ge X/2$,

$$\prod_{j \le d} A_j B_j C_j \ge 2^{-3d} \operatorname{rad}(abc) \ge 2^{-3d-\lambda-1} X^{\lambda} \ge 2^{-3d-3} X^{\lambda},$$

since $\lambda \le 2$. Each of the $3d$ roots loses at most a factor 2; the source proof prints 2^{-d} here. The weighted lower bound for the c-roots is

$$\prod_{j \le d} C_j^j \ge 2^{-h_d} \prod_{j \le d} \mathfrak{c}_j^j.$$

The factorization uses parameter $\varepsilon_0/4$, so $c_0 \le X^{\varepsilon_0/4}$ and $\prod_{j \le d} \mathfrak{c}_j^j = c/c_0 \ge 2^{-1} X^{1-\varepsilon_0/4}$. Since $C_j \ge \mathfrak{c}_j/2$,

$$\prod_{j \le d} C_j^j \ge 2^{-h_d-1} X^{1-\varepsilon_0/4} \ge X^{1-\varepsilon_0/2} \quad \text{if } X \ge Y_{\mathrm{red}} := 2^{4(h_d+1)/\varepsilon_0}.$$

This gives the lower bound in (2.4). The global threshold $Y_0(\varepsilon_0, d) \ge Y_{\mathrm{red}}$ is fixed in Lemma 12.2. This suffices, since d is fixed before X. Fix such a box. For a side $s \in \{a, b, c\}$ set

$$s_i = \log_X S_i \ (1 \le i \le d), \qquad s = \log_X \prod_{i \le d} S_i = \sum_{i \le d} \log_X S_i. \tag{2.5}$$

Index 0 is not a coordinate: a_0, b_0, c_0 are the integer coefficients. From here on a, b, c denote coordinates, not the triple. Boxes with $\mathcal{B}_d = 0$ do not attain the maximum in (2.3) unless $N_\lambda^*(X) = 0$. So $\mathcal{B}_d \ge 1$, and we set

$$D = \log_X \mathcal{B}_d \ge 0.$$

For the tail put

$$\tau_s = s - \sum_{i \le 6} s_i = \sum_{7 \le j \le d} \log_X S_j, \qquad v_s = \sum_{7 \le j \le d} j \log_X S_j. \tag{2.6}$$

Put $L = a + b + c$ and $p_i = a_i + b_i + c_i$; a bare p is a prime. Moving a dyadic endpoint at scale X changes the root coordinates by

$$\Delta s_i, \ \Delta s = O_d\!\left(\frac{1}{\log X}\right). \tag{2.7}$$

The left inequality of (2.4) uses $\prod_{j \le d} n_j \ge \operatorname{rad}(n)$ with no loss, while in this direction [2, Lemma 2.2] gives only $\operatorname{rad}(n) \le n^{\varepsilon_0} \prod_j n_j$. In the proof of that lemma $m_j = \prod_{p^j \| n} p$, and, for the folded index k, $n_j = m_j$ for $j \ne k$ and $n_k = m_k \prod_{j > d} m_j^{\lfloor j/k \rfloor}$. Since $d \ge k$, $\lfloor j/k \rfloor \ge 1$ for $j > d$, so

$$\prod_{j \le d} n_j \ \ge \ \prod_{j \le d} m_j \prod_{j > d} m_j \ = \ \operatorname{rad}(n).$$

Lemma 2.1. *The three side values of a box are pairwise coprime. Hence every factor of one side is a unit modulo every factor of another side.*

Proof. A prime dividing two side values divides the third by the equation in (2.2). If it divides $a_0 \prod_{i=1}^d \mathfrak{a}_i^i$, it divides $\prod_{i=0}^d \mathfrak{a}_i$; likewise on the other sides. This contradicts the gcd condition in (2.2). □

The index $i = 0$ in this gcd condition is needed. With $d = 1$, the choice

$$a_0 = b_0 = 1, \quad \mathfrak{a}_1 = \mathfrak{b}_1 = 2, \quad c_0 = 4, \quad \mathfrak{c}_1 = 1$$

satisfies the condition with $i \geq 1$: $\gcd(2, 2, 1) = 1$. Yet its side values 2, 2, 4 share the prime 2. The full condition excludes it: $\gcd(2, 2, 4) = 2$.

Nothing is assumed within a side. Roots of one side may share primes with a_0. Unenumerated roots are recovered by a divisor bound, not by squarefreeness.

2.1. **The inherited rows.** For these limiting rows take $0 < \lambda \leq 1$. The finite box bound is $L \leq \lambda + 3\varepsilon_0/4 \leq 1 + 3\varepsilon_0/4$. We use this endpoint envelope throughout, so no choice of ε_0 depends on the gap $1 - \lambda$. Lemmas A.2 and A.3 and Corollary A.5 are our forms of [2, Propositions 2.3, 3.1 and 4.1]. In the coordinates (2.5) they yield the 22 inequalities of [2, Proposition 6.1]. We display them in exact limiting form, as Section 11 uses them. At finite resolution each right-hand side rises by the amount in Lemma 12.2 and Table 12.1; (2.9) and (2.10) hold exactly. The reduction has constants depending only on ε_0, d. So do the bounds of Appendix A. They use λ only through $ABC \leq X^{\lambda+3\varepsilon_0/4}$ in Corollary A.5. The condition $\varepsilon_0 \leq (1 - \mu)/3$ occurs only in the final step of the proof of [2, Theorem 1.3], where it ensures $ABC \leq X^{\mu+3\varepsilon_0} \leq X$.

The radical bound in (2.4) gives [2, (6.1)],

$$L \leq 1, \tag{2.8}$$

derived there for $\lambda < 1$. At $\lambda = 1$ only $L \leq 1 + 3\varepsilon_0/4$ holds (Lemma 12.2). Roots sum into their side, [2, (6.2)]:

$$\sum_{i \leq 6} s_i \leq s \qquad (s = a, b, c). \tag{2.9}$$

The side-value bound in (2.4) gives [2, (6.3)],

$$7s - 1 \leq 6s_1 + 5s_2 + 4s_3 + 3s_4 + 2s_5 + s_6 \qquad (s = a, b, c). \tag{2.10}$$

Two sides determine the third up to a divisor factor (Lemma A.2). This is [2, (6.4)]:

$$D \leq \min(a + b,\ a + c,\ b + c). \tag{2.11}$$

Geometry of numbers (Corollary A.5) gives the thirteen min-disjunctions [2, (6.5)–(6.9)], labelled (G1)–(G13) in Appendix B. The Fourier estimate (Lemma A.3) gives [2, (6.10)],

$$\sum_{s=a,b,c} \max(s_2 + s_4 + s_6,\ s_3 + s_6,\ s_5) \leq 4L - 6D. \tag{2.12}$$

One argument per maximum gives 27 linear rows. Section 11 encodes them with three auxiliary variables.

The `Python` listing of [2, Appendix A] transcribes the first line of [2, (6.9)] as `p1+a2+b3+a3`, where the displayed formula reads $p_1 + a_2 + b_3 + c_3$. We use the displayed formula. It is what Corollary A.5 gives with the printed second argument $1 - a_2 - 2b_3 - 2c_3$. For (2.10) we use

$$7s - 1 \leq 7s - \sum_{i \leq d} i\, s_i = \sum_{i \leq 6} (7 - i)s_i + \sum_{7 \leq i \leq d} (7 - i)s_i \leq \sum_{i \leq 6} (7 - i)s_i, \tag{2.13}$$

since $7 - i \leq 0$ for $i \geq 7$. In our system (2.10) is the sum of the two tail rows of Section 3, so it is redundant.

3. The multiplicity-at-least-seven tail

The tail rows we use are

$$\tau_s \ge 0, \qquad v_s \ge 7\tau_s, \qquad \sum_{i\le 6} i\, s_i + v_s \le 1 \qquad (s = a, b, c). \tag{3.1}$$

The first is (2.9). The second: $\log_X S_j \ge 0$, with weight $j \ge 7$ in v_s and weight 1 in τ_s. The third is the side-value bound in (2.4). Adding the last two,

$$(v_s - 7\tau_s) + (1 - \sum_{i\le 6} i s_i - v_s) \ge 0,$$

that is, $\sum_{i\le 6} i s_i + 7\tau_s \le 1$; with $\tau_s = s - \sum_{i\le 6} s_i$ this is (2.10). With the upper row $v_s \le d\tau_s$, these rows describe the real relaxation of the pairs (τ_s, v_s) exactly. We omit that row, so the system $\mathcal{S}$ of Section 11 is free of d.

Lemma 3.1. *Fix a side $s \in \{a, b, c\}$ and let $M_{\mathrm{tail}} = \prod_{7\le j\le d} \mathfrak{s}_j^{\,j}$ with $\mathfrak{s}_j \sim S_j$. Then*

$$\begin{aligned} \#\{(\mathfrak{s}_7, \dots, \mathfrak{s}_d) \in \mathbb{N}^{d-6} : \mathfrak{s}_j \sim S_j\} &\le \prod_{7\le j\le d} S_j = X^{\tau_s}, \\ M_{\mathrm{tail}} &\ge \prod_{7\le j\le d} S_j^{\,j} = X^{v_s}, \end{aligned} \tag{3.2}$$

and every prime p dividing M_{tail} does so with $\mathrm{ord}_p(M_{\mathrm{tail}}) \ge 7$, where ord_p denotes the p-adic valuation.

Proof. Each interval $[S_j, 2S_j)$ contains exactly S_j integers, which gives the count, and $\mathfrak{s}_j \ge S_j$ gives the modulus bound. If $p \mid \mathfrak{s}_j$ with $j \ge 7$ then $\mathrm{ord}_p(M_{\mathrm{tail}}) \ge j \ge 7$. □

The count is exact for $[N, 2N)$ and for $(N, 2N]$. A closed $[N, 2N]$ would overcount by a factor of up to 2^{d-6}, attained when all $S_j = 1$.

So the tail costs X^{τ_s} to enumerate. The bound is on roots, not on $\mathrm{rad}(M_{\mathrm{tail}})$, and uses no squarefreeness. Let σ and T be the modulus side and index set of Section 5. Then M_{tail} divides the side value and is at least X^{v_σ}. Hence T may contain the tail.

3.1. Folded roots.

For the rest of the proof fix $0 < \varepsilon_0 \le 4/7$. This is allowed, as ε_0 is arbitrarily small at the endpoint step. In [2, Lemma 2.2] the very high multiplicities are folded into one index k. The folded root need not be squarefree; the remainder goes into n_0. The proof of [2, Proposition 2.1] uses that lemma with parameter $\varepsilon_0/4$. So

$$k = \lceil 4/\varepsilon_0 \rceil, \qquad d = 6\lceil (4/\varepsilon_0)^2 \rceil.$$

Then $k \ge 7$, and $d \ge 6(4/\varepsilon_0)^2 > 4/\varepsilon_0 + 1 > k$. So the folded root lies in the tail, M_{tail} still divides the side value, and $\mathrm{ord}_p(n_k^k) = k\,\mathrm{ord}_p(n_k) \ge 7$ for $p \mid n_k$. The overlap of n_0 and n_k is within one side, so Lemma 2.1 is untouched. Unenumerated roots are recovered by Lemma 4.3. The folding costs the factor $X^{3\varepsilon_0/4}$ in the upper radical bound of (2.4). It also costs the choice of a_0, b_0, c_0 in the X^{ε_0} of (2.3). Both are already charged. It changes neither Lemma 3.1 nor (3.1).

4. Three lattice and divisor lemmas

Lemma 4.1. *Let $M \geq 1$, let ξ be a unit modulo M and let $U, V \geq 1$. Then*

$$\#\{(u,v) \in \mathbb{N}^2 : u \leq U,\ v \leq V,\ \gcd(u,v) = 1,\ u \equiv \xi v\ (M)\} \leq 1 + \frac{2UV}{M}. \tag{4.1}$$

Proof. Put $\mathcal{L}_\xi = \{(u,v) \in \mathbb{Z}^2 : u \equiv \xi v\ (M)\}$, of index M in $\mathbb{Z}^2$. Any two of its points have determinant in $M\mathbb{Z}$. Positive collinear integer points with $\gcd(u,v) = 1$ coincide. Thus the points of $\mathcal{L}_\xi$ with $\gcd(u,v) = 1$ in $[1,U] \times [1,V]$ have distinct slopes; order them by slope. Consecutive points span with 0 a triangle of area $\geq M/2$. These triangles have disjoint interiors and lie in $[0,U] \times [0,V]$. With P points, $(P-1)M/2 \leq UV$. □

The proof does not use that ξ is a unit. The constant 2 is sharp. For odd $n \geq 3$ take $U = n$, $V = n+4$, $M = n^2 + 2n - 4$, $\xi = n - 1$. The primitive points are $(n-1, 1)$, $(n, n+4)$, $(1, n+3)$, with consecutive determinants M, and $(P-1)M/(UV) \to 2$.

Lemma 4.2. *Let $1 \leq q \leq 6$, let $M \geq 1$ and let K be a unit modulo M. The congruence $\eta^q \equiv K \pmod{M}$ has at most $8^{\omega(M)}$ solutions in units η, hence $X^{o(1)}$ solutions uniformly for $M \leq X^{O(1)}$.*

Proof. The solution set is empty or a coset of the kernel of $\eta \mapsto \eta^q$. Odd prime power: the unit group is cyclic, so the kernel has order at most $q \leq 6$. Modulus 2^e, $e \leq 2$: the unit group has order at most 2. Modulus 2^e, $e \geq 3$: $(\mathbb{Z}/2^e\mathbb{Z})^\times \cong C_2 \times C_{2^{e-2}}$, so the kernel has order $\gcd(q,2)\gcd(q,2^{e-2}) \leq 8$; the 2-part of $q \leq 6$ is at most 4. Multiply by the Chinese remainder theorem. As $\omega(M) \ll \log M/\log\log M$ for $M \geq 3$,

$$8^{\omega(M)} = \exp\big(O(\log M/\log\log M)\big) = X^{O(1/\log\log X)} \qquad (M \leq X^{O(1)}).$$

The form $C^{\omega(M)} \ll_{C,\delta} M^\delta$, for fixed $C \geq 1$ and $\delta > 0$, alone gives no rate. For $M \leq 2$ there is one class. No bound $B^{\omega(M)}$ with $B < 8$ holds. For $q = 4$, $e \geq 4$, the group $C_2 \times C_{2^{e-2}}$ has $\gcd(4,2)\gcd(4,2^{e-2}) = 8$ fourth roots of unity. And $q = 4$ occurs in (5.2). Local kernel size 8 occurs only for 2^e, $e \geq 4$, $q = 4$. So for $\omega(M) \geq 2$ the product of local kernel sizes is at most $8 \cdot 6^{\omega(M)-1} < 8^{\omega(M)}$. □

Lemma 4.3. *Write $\operatorname{div}(N) = \#\{m \in \mathbb{N} : m \mid N\}$ for $N \in \mathbb{N}$. For $r \geq 1$ and positive integers $e_1, \dots, e_r$,*

$$\#\{(x_1, \dots, x_r) \in \mathbb{N}^r : x_1^{e_1} \cdots x_r^{e_r} = N\} \leq \operatorname{div}(N)^{r-1} \ll_{r,\delta} N^\delta \qquad (\delta > 0),$$

uniformly in $e_1, \dots, e_r$. For $N \geq 3$ the maximal-order bound gives the rate

$$\operatorname{div}(N)^{r-1} = \exp\big(O_r(\log N/\log\log N)\big),$$

so for $N \leq X^{O_d(1)}$ and $r \leq d$ the count is $X^{O_d(1/\log\log X)}$.

Proof. Each x_i divides N. The equation determines x_r from $x_1, \dots, x_{r-1}$, for any e_i. Apply the divisor bound and, for the rate, the maximal order of $\operatorname{div}(N)$. □

Thus an unfactored product of roots determines those roots up to $X^{o(1)}$.

5. The cut

Fix a box. Let (y,z) be the other two sides in alphabetical order: (b,c), (a,c), (a,b) for $\sigma = a,b,c$. Write $[6] = \{1,2,3,4,5,6\}$. Choose a nonempty

$$T \subseteq \{1,2,3,4,5,6,\mathrm{tail}\},$$

$$\kappa_T = \sum_{t \in T \cap [6]} \sigma_t + \mathbf{1}_{\mathrm{tail} \in T} \tau_\sigma, \qquad \Omega_T = \sum_{t \in T \cap [6]} t\,\sigma_t + \mathbf{1}_{\mathrm{tail} \in T} v_\sigma. \tag{5.1}$$

Here κ_T is the selected root mass for this section. The symbols u, v, M, ξ below are local to the cut and are not the corresponding symbols in Sections 9 and 10; v is also distinct from the tail coordinate v_σ. Choose free sets $R_y, R_z \subseteq [6]$, not both empty, and put

$$q = \gcd(\gcd R_y, \gcd R_z), \qquad F = \sum_{i \in R_y} i\, y_i + \sum_{j \in R_z} j\, z_j, \tag{5.2}$$

with $\gcd \emptyset = 0$. For such a choice (σ, T, R_y, R_z), the quantities in (5.1)–(5.2) are fixed by the box and the index sets. As $R_y \cup R_z \neq \emptyset$, $1 \le q \le 6$ and q divides every element of $R_y \cup R_z$. By the choice of d in Section 3.1, $d = 6\lceil (4/\varepsilon_0)^2 \rceil \ge 294$, so the tail notation applies. Write $\max\{t,0\} = \max\{t,0\}$.

Proposition 5.1. *Let a box satisfy the constraints after* (2.3)*, with* $\mathcal{B}_d \ge 1$*. Then*

$$D \le \Big(y - \sum_{i \in R_y} y_i\Big) + \Big(z - \sum_{j \in R_z} z_j\Big) + \kappa_T + \max\{\frac{F}{q} - \Omega_T, 0\} + o_{\varepsilon_0,d}(1), \tag{5.3}$$

uniformly over the finitely many choices of (σ, T, R_y, R_z)*.*

For later use write

$$\mathsf{A}_{\mathrm{cut}} = \Big(y - \sum_{i \in R_y} y_i\Big) + \Big(z - \sum_{j \in R_z} z_j\Big) + \kappa_T, \qquad \mathsf{B}_{\mathrm{cut}} = F/q - \Omega_T.$$

The limiting form of (5.3) is $D \le \mathsf{A}_{\mathrm{cut}} + \max(0, \mathsf{B}_{\mathrm{cut}})$.

Proof. Sizes. The box fixes $n_{a,0} = a_0$, $n_{b,0} = b_0$ and $n_{c,0} = c_0$. Write $n_{\sigma,0}, n_{y,0}, n_{z,0}$ for these coefficients and $S_{\sigma,i}, S_{y,i}, S_{z,i}$ for the dyadic root sizes of the σ, y, z sides. Besides (2.2), the proof uses the dyadic ranges and $\prod_i A_i^i$, $\prod_i B_i^i$, $\prod_i C_i^i \le X$. So all products and cofactors are at most $X^{O_d(1)}$, and Lemmas 4.2 and 4.3 cost $X^{o(1)}$. The coefficients enter no size estimate.

Enumeration. Write $\mathfrak{m}_i, \mathfrak{y}_i, \mathfrak{z}_i$ for the roots of the σ-, y- and z-sides, so $\mathfrak{m}_i \sim S_{\sigma,i}$, $\mathfrak{y}_i \sim S_{y,i}$, $\mathfrak{z}_i \sim S_{z,i}$. Enumerate: the roots of y outside R_y; of z outside R_z; the selected roots of σ. Tails go through Lemma 3.1. The y- and z-tails are never in $R_y, R_z \subseteq [6]$, so they are enumerated too. The cost is

$$X^{(y - \sum_{i \in R_y} y_i) + (z - \sum_{j \in R_z} z_j) + \kappa_T + o_{\varepsilon_0,d}(1)}. \tag{5.4}$$

Modulus. The tail roots of σ are $\mathfrak{m}_j$, $j \ge 7$. Put

$$M = \prod_{t \in T \cap [6]} \mathfrak{m}_t^t\, M_{\mathrm{tail}}^{\mathbf{1}_{\mathrm{tail} \in T}}, \qquad M_{\mathrm{tail}} = \prod_{7 \le j \le d} \mathfrak{m}_j^j. \tag{5.5}$$

Then M divides the σ-side value. Also $\mathfrak{m}_t \ge S_{\sigma,t} = X^{\sigma_t}$ (left-closed intervals), and Lemma 3.1 bounds the tail. So

$$M \ge X^{\Omega_T}. \tag{5.6}$$

Put

$$u = \prod_{i \in R_y} \mathfrak{y}_i^{i/q}, \qquad v = \prod_{j \in R_z} \mathfrak{z}_j^{j/q}, \tag{5.7}$$

an empty product being 1; the exponents are integers by (5.2).

Congruence. By Lemma 2.1, every factor of the y- and z-sides is a unit modulo M. This covers the coefficients, the enumerated roots, u and v. The equation of (2.2) modulo M gives

$$(uv^{-1})^q \equiv K \pmod{M} \tag{5.8}$$

with

$$K \equiv \epsilon_{\mathrm{cut}} E_z E_y^{-1} \pmod{M}, \qquad \epsilon_{\mathrm{cut}} = \begin{cases} -1, & \sigma = c, \\ +1, & \sigma \neq c, \end{cases} \tag{5.9}$$

where

$$E_y = n_{y,0} \prod_{i \in [6] \setminus R_y} \mathfrak{y}_i^i \prod_{7 \le j \le d} \mathfrak{y}_j^j,$$
$$E_z = n_{z,0} \prod_{j \in [6] \setminus R_z} \mathfrak{z}_j^j \prod_{7 \le j \le d} \mathfrak{z}_j^j.$$

So K is a unit fixed by the enumerated data.

Count. By Lemma 4.2, $\xi = uv^{-1}$ lies in one of $X^{o(1)}$ classes. By Lemma 2.1, $\gcd(u, v) = 1$. Also

$$u \le 2^{\sum_{i \in R_y} i/q} \prod_{i \in R_y} S_{y,i}^{i/q} =: U_{\mathrm{cut}}, \qquad v \le 2^{\sum_{j \in R_z} j/q} \prod_{j \in R_z} S_{z,j}^{j/q} =: V_{\mathrm{cut}},$$

with $U_{\mathrm{cut}}, V_{\mathrm{cut}} \ge 1$; the powers of 2 cost $O_d(1/\log X)$, as $\sum_{r \le 6} r = 21$. Hence

$$U_{\mathrm{cut}} = X^{\sum_{i \in R_y} i\, y_i/q + O_d(1/\log X)}, \qquad V_{\mathrm{cut}} = X^{\sum_{j \in R_z} j\, z_j/q + O_d(1/\log X)},$$

so $U_{\mathrm{cut}} V_{\mathrm{cut}} = X^{F/q + O_d(1/\log X)}$. Lemma 4.1 and (5.6) bound the pairs (u, v) in one class by

$$1 + \frac{2U_{\mathrm{cut}} V_{\mathrm{cut}}}{M} \ll_d X^{\max\{F/q - \Omega_T, 0\} + O_d(1/\log X)}. \tag{5.10}$$

Recovery. Lemma 4.3 recovers the free roots from u, v up to $X^{o(1)}$. Then the y- and z-side values are known, and the equation fixes the σ-side value. Divide by $n_{\sigma,0}$ and the selected roots:

$$Q_\sigma = \prod_{i \in [6] \setminus T} \mathfrak{m}_i^i \left(\prod_{7 \le j \le d} \mathfrak{m}_j^j \right)^{1 - \mathbf{1}_{\mathrm{tail} \in T}}.$$

Lemma 4.3 recovers these unselected roots up to $X^{o(1)}$. Multiplying (5.4) by $X^{o(1)}$ and (5.10) gives (5.3). □

If one free set is empty, $U_{\mathrm{cut}} = 1$ or $V_{\mathrm{cut}} = 1$, and Lemma 4.1 still applies. The exponent q depends only on the index sets R_y, R_z, not on which roots equal 1. Counting coefficients is charged to (2.3): inside a box a_0, b_0, c_0 are fixed.

Count: 64 subsets of [6] per counted side, 127 sets T, three sides σ. Without the pair of empty free sets this is $3(64^2 - 1)127 = 1\,560\,195$, as in (1.3).

6. Archimedean rows

Throughout Sections 6–8, assume $0 < \mu \le 1$. Take $\varepsilon_0 \le 4/7$ and $d = d(\varepsilon_0)$ as fixed in Section 3.1. Fix a box admissible in (2.3) at scale Y, with λ replaced by μ and $\mathcal{B}_d \ge 1$. Of the constraints (2.4) only the side-value bounds are used below, with the coefficient bound $1 \le n_{s,0} \le Y^{\varepsilon_0}$. We also use the equation, the gcd condition and the windows of (2.2). For the finite estimates take $Y \ge Y_0$, the threshold of Lemma 12.2; it depends only on ε_0, d, and $Y_0 \ge \exp(\exp(1))$. All coordinates s, τ_s, v_s, L, p_i from Section 2 are now read at base Y. The integer side values are denoted by n_s; V_s is the exponent coordinate of the root product, not of n_s. The root mass of side s is $s = \sum_{i \le d} s_i$. Put $s_i = \log_Y S_{s,i}$ and $D = \log_Y \mathcal{B}_d$.

$$V_s = \log_Y \prod_{j \le d} S_{s,j}^{j} = \sum_{i \le 6} i\, s_i + v_s \qquad (s = a, b, c). \tag{6.1}$$

For a tuple of the box write $n_s = n_{s,0} \prod_{j \le d} \mathfrak{s}_j^{\,j}$ for its side values, so $n_a + n_b = n_c$. Here $n_{s,0}$ is the coefficient a_0, b_0 or c_0 on side s. Since $S_j \le \mathfrak{s}_j < 2S_j$ and $1 \le n_{s,0} \le Y^{\varepsilon_0}$,

$$Y^{V_s} \le n_s < 2^{h_d}\, n_{s,0}\, Y^{V_s} \le 2^{h_d}\, Y^{V_s + \varepsilon_0}. \tag{6.2}$$

The side-value constraints of (2.4) read

$$V_a \le 1, \qquad V_b \le 1, \qquad 1 - \frac{\varepsilon_0}{2} \le V_c \le 1. \tag{6.3}$$

Lemma 6.1.

$$V_a \le V_c + \frac{\varepsilon_0}{2}, \qquad V_b \le V_c + \frac{\varepsilon_0}{2}.$$

Proof. By (6.3), $V_a \le 1 \le V_c + \varepsilon_0/2$. Likewise for V_b. □

Lemma 6.2. *At least one of*

$$V_c \le V_a + \frac{3\varepsilon_0}{2} + \log_Y 2^{1+h_d}, \qquad V_c \le V_b + \frac{3\varepsilon_0}{2} + \log_Y 2^{1+h_d}$$

holds.

Proof. As $\mathcal{B}_d \ge 1$, choose one tuple of the box. Then $n_a, n_b \ge 1$ and $n_a + n_b = n_c$, so $\max(n_a, n_b) \ge n_c/2$. Suppose $n_a \ge n_c/2$. By (6.3) and (6.2),

$$Y^{1-\varepsilon_0/2} \le Y^{V_c} \le n_c \le 2n_a < 2^{1+h_d}\, Y^{V_a + \varepsilon_0}.$$

Take $\log_Y$:

$$1 \le V_a + \frac{3\varepsilon_0}{2} + \log_Y 2^{1+h_d}.$$

With $V_c \le 1$ this is the first inequality. If $n_b \ge n_c/2$, the same argument gives the second. □

The choice in Lemma 6.2 uses one tuple. The conclusion concerns the dyadic endpoints, so it holds for the whole box.

Corollary 6.3. *Put* $\rho_{\mathrm{arch}} = 3\varepsilon_0/2 + \log_Y 2^{1+h_d}$. *Every nonempty admissible box satisfies*

$$V_a \le V_c + \rho_{\mathrm{arch}}, \qquad V_b \le V_c + \rho_{\mathrm{arch}}, \tag{6.4}$$

and at least one arm of

$$V_c \le V_a + \rho_{\mathrm{arch}} \quad \textit{or} \quad V_c \le V_b + \rho_{\mathrm{arch}}. \tag{6.5}$$

Proof. Lemmas 6.1 and 6.2, and $\varepsilon_0/2 \le \rho_{\mathrm{arch}}$. □

In the limit $\rho_{\mathrm{arch}} \to 0$, the first arm of (6.5) with (6.4) gives $V_a = V_c \ge V_b$, the second $V_b = V_c \ge V_a$. A cover node of the certificate carries both arms.

7. The cubic row

We use the following theorem of Heath-Brown [8, Theorem 1.3], with its counting function ρ renamed $\mathcal{R}$. In this theorem B is a height and a, b, c are coefficients.

Theorem A ([8, Theorem 1.3])**.** *Let $\mathcal{R}(B; a, b, c)$ be the number of integer solutions x, y, z to the equation*

$$ax^3 + by^3 + cz^3 = 0$$

with $\gcd(x, y, z) = 1$ *and* $\max(|x|, |y|, |z|) \le B$*. Then*

$$\mathcal{R}(B; a, b, c) \ll_\varepsilon B^\varepsilon$$

for any $\varepsilon > 0$, uniformly for all non-zero integer a, b, c.

The implied constant depends on ε alone. The coefficients need not be coprime or positive.

Proposition 7.1. *For every $\varepsilon_1 > 0$,*

$$D \le \sum_{s=a,b,c} (s - s_3) + \varepsilon_1 + O_{\varepsilon_1}\Big(\frac{1}{\log Y}\Big) = L - p_3 + \varepsilon_1 + O_{\varepsilon_1}\Big(\frac{1}{\log Y}\Big). \tag{7.1}$$

The implied constant depends only on ε_1.

Proof. Enumeration. Send a tuple of the box to its roots $(\mathfrak{a}_i, \mathfrak{b}_i, \mathfrak{c}_i)_{i \ne 3}$ and to $(x_a, x_b, x_c) = (\mathfrak{a}_3, \mathfrak{b}_3, \mathfrak{c}_3)$. This map is injective. As $\#\{\mathfrak{s} : \mathfrak{s} \sim S\} = S$, the first component takes at most

$$\prod_{s=a,b,c} \prod_{i \le d,\ i \ne 3} S_{s,i} = Y^{\sum_s (s - s_3)}$$

values. The tail roots $i \ge 7$ are enumerated one by one, as in Lemma 3.1.

Equation. Fix the first component. Put

$$\alpha = a_0 \prod_{i \ne 3} \mathfrak{a}_i^i, \qquad \beta = b_0 \prod_{i \ne 3} \mathfrak{b}_i^i, \qquad \gamma = c_0 \prod_{i \ne 3} \mathfrak{c}_i^i.$$

These are positive integers. The equation of (2.2) becomes

$$\alpha x_a^3 + \beta x_b^3 + (-\gamma) x_c^3 = 0.$$

Primitivity. $x_a \mid n_a$, $x_b \mid n_b$, $x_c \mid n_c$, and the side values are pairwise coprime by Lemma 2.1. Hence $\gcd(x_a, x_b, x_c) = 1$.

Height. $1 \le x_a < 2A_3 \le 2\big(\prod_j A_j^j\big)^{1/3} \le 2Y$ by (6.3). Likewise $x_b, x_c < 2Y$.

Count. By Theorem A with $B = 2Y$ and coefficients $(\alpha, \beta, -\gamma)$, the number of (x_a, x_b, x_c) is at most $\mathcal{R}(2Y; \alpha, \beta, -\gamma) \le C(\varepsilon_1)(2Y)^{\varepsilon_1}$, uniformly in α, β, γ. Hence

$$\mathcal{B}_d \le C(\varepsilon_1)\, 2^{\varepsilon_1}\, Y^{\sum_s (s - s_3) + \varepsilon_1}.$$

Take $\log_Y$. □

The bound is uniform in the coefficients a_0, b_0, c_0 and in the enumerated roots. A constant depending on α, β, γ would not give a row.

8. Spacing rows

Choose $e \in \{a,b,c\}$, either ordering (y,z) of the other two sides, and $2 \le \ell \le 6$. Put

$$\mathsf{A}_{\mathrm{sp}} = y + (z - z_\ell), \qquad \mathsf{B}_{\mathrm{sp}} = V_e - V_z + z_\ell. \tag{8.1}$$

Here y and z also denote the root masses of these sides, as in (2.5).

For side e, write $n_{e,0}$ for its coefficient and $\mathfrak{e}_j$ for its roots (Section 6). Choose K_d so that

$$\operatorname{div}(N)^{d-1} \le Y^{K_d/\log\log Y} \quad \text{if } Y \ge \exp(\exp(1)), \quad N \le 2^{h_d} Y;$$

such a constant exists by the divisor bound.

Proposition 8.1.

$$D \le \mathsf{A}_{\mathrm{sp}} + \max\{\mathsf{B}_{\mathrm{sp}}, 0\} + \varepsilon_0 + O_d\Big(\frac{1}{\log\log Y}\Big). \tag{8.2}$$

Proof. Signs. From $n_a + n_b = n_c$,

$$n_e = \varsigma_y n_y + \varsigma_z n_z, \qquad (\varsigma_y, \varsigma_z) = \begin{cases} (1,1), & e = c, \\ (-1,1), & e \ne c,\ z = c, \\ (1,-1), & e \ne c,\ y = c. \end{cases}$$

This ordering need not be the alphabetical order used in Section 5.

Enumeration. Enumerate all roots $\mathfrak{y}_j$ $(j \le d)$ of y and all roots $\mathfrak{z}_j$ $(j \le d,\ j \ne \ell)$ of z. As $\#\{\mathfrak{s} : \mathfrak{s} \sim S\} = S$, there are

$$\prod_{j \le d} S_{y,j} \prod_{j \ne \ell} S_{z,j} = Y^{y+z-z_\ell} \tag{8.3}$$

choices. Fix one. Then n_y is fixed, and

$$n_z = \Pi_z\, x^\ell, \qquad \Pi_z = n_{z,0} \prod_{j \ne \ell} \mathfrak{z}_j^{\,j}, \qquad x = \mathfrak{z}_\ell \in [S_{z,\ell}, 2S_{z,\ell}).$$

Interval. By (6.2), n_e lies in an interval I_e of length $|I_e| < 2^{h_d} Y^{V_e + \varepsilon_0}$. Then

$$x^\ell = \varsigma_z \frac{n_e - \varsigma_y n_y}{\Pi_z} \in J, \qquad J = \varsigma_z \frac{I_e - \varsigma_y n_y}{\Pi_z},$$

an interval of length $|I_e|/\Pi_z$. As $\Pi_z \ge \prod_{j \ne \ell} S_{z,j}^{\,j} = Y^{V_z - \ell z_\ell}$,

$$|J| < 2^{h_d}\, Y^{V_e - V_z + \ell z_\ell + \varepsilon_0}.$$

Spacing. Let $\mathcal{X}$ be the integers $x \in [S_{z,\ell}, 2S_{z,\ell})$ for which $x^\ell \in J$, and put $m = |\mathcal{X}|$. If $m = 0$, this enumeration choice contributes nothing. Otherwise write $x_1 < \cdots < x_m$ for $\mathcal{X}$. For $i \ge 2$,

$$x_i^\ell - x_{i-1}^\ell \ge \ell\, x_{i-1}^{\ell-1} \ge S_{z,\ell}^{\ell-1} = Y^{(\ell-1)z_\ell}.$$

So $(m-1)Y^{(\ell-1)z_\ell} \le x_m^\ell - x_1^\ell < |J|$, and

$$m < 1 + 2^{h_d} Y^{\mathsf{B}_{\mathrm{sp}} + \varepsilon_0} \le 2^{1+h_d}\, Y^{\max\{\mathsf{B}_{\mathrm{sp}}, 0\} + \varepsilon_0}. \tag{8.4}$$

This includes $S_{z,\ell} = 1$, where $x = 1$ and $m \le 1$.

Recovery. Given x, n_z and then $n_e = \varsigma_y n_y + \varsigma_z n_z$ are fixed. Put $N = n_e/n_{e,0} = \prod_{j \le d} \mathfrak{e}_j^{\,j} < 2^{h_d} Y$. By Lemma 4.3 the roots of e take at most $Y^{K_d/\log\log Y}$ values.

Total. Multiply (8.3), (8.4) and the recovery factor:

$$\mathcal{B}_d \le 2^{1+h_d}\, Y^{\mathsf{A}_{\mathrm{sp}}+\max\{\mathsf{B}_{\mathrm{sp}},0\}+\varepsilon_0+O_d(1/\log\log Y)}.$$

Take $\log_Y$; 2^{1+h_d} costs $O_d(1/\log Y)$. □

Corollary 8.2. *Put*

$$\rho_{\mathrm{sp}} = \varepsilon_0 + \frac{K_d}{\log\log Y} + \log_Y 2^{1+h_d}.$$

This is the error in (8.2)*. For each of the* $3\cdot 2\cdot 5 = 30$ *choices of* (e,y,z,ℓ)*, a nonempty admissible box satisfies at least one arm of*

$$D \le \mathsf{A}_{\mathrm{sp}} + \rho_{\mathrm{sp}} \quad \textit{or} \quad D \le \mathsf{A}_{\mathrm{sp}} + \mathsf{B}_{\mathrm{sp}} + \rho_{\mathrm{sp}}. \tag{8.5}$$

Proof. $\mathsf{A}_{\mathrm{sp}} + \max\{\mathsf{B}_{\mathrm{sp}},0\} = \max(\mathsf{A}_{\mathrm{sp}}, \mathsf{A}_{\mathrm{sp}}+\mathsf{B}_{\mathrm{sp}})$. □

All these errors are μ-free. With $\varepsilon_1 = \varepsilon_0$, each is at most $2\varepsilon_0$ for $Y \ge Y_0$. Table 12.1 lists them with the others.

9. Cubic-sieve rows

9.1. **Setting.** Fix $\varepsilon_0 \le 4/7$ and $d = d(\varepsilon_0)$ as in Section 3.1. Assume $Y \ge Y_0$, the threshold of Lemma 12.2. Fix parameters for a nonempty box counted by $\mathcal{B}_d$ in (2.3) at scale Y, and put $D = \log_Y \mathcal{B}_d$. For each side $s \in \{a,b,c\}$, write $n_{s,0}$ for its coefficient and $\mathfrak{r}_{s,j} \sim S_{s,j}$ $(1 \le j \le d)$ for its roots. The symbols M, x, u, v, U, V, ξ below are local to this section. Its M is the canonical coefficient of (9.3). The modulus Q is local to each analytic-input lemma and to Steps 5–7 of Proposition 9.10. Here v_s is the tail coordinate, while v is a represented-side label. The integer V (as in $V_{\mathfrak{o}}$, $V(\mathbf{u})$, V_ι) is distinct from the coordinate V_s. The side values

$$n_s = n_{s,0} \prod_{j\le d} \mathfrak{r}_{s,j}^{\,j}$$

satisfy $n_a + n_b = n_c$ and are pairwise coprime by Lemma 2.1. The coordinates are

$$\begin{aligned} s_{s,j} &= \log_Y S_{s,j}, \qquad r_s = \sum_{j\le d} s_{s,j}, \qquad t_s = \sum_{7\le j\le d} s_{s,j}, \\ v_s &= \sum_{7\le j\le d} j\, s_{s,j}, \qquad V_s = \sum_{j\le 6} j\, s_{s,j} + v_s. \end{aligned} \tag{9.1}$$

In the notation of Section 2, $r_s = s$ and $t_s = \tau_s$; the coordinate $s_{s,j}$ is the earlier s_j. By (2.4), $V_s \le 1$. Hence $n_s \le n_{s,0}\prod_j (2S_{s,j})^j \le 2^{d^2} Y^{1+\varepsilon_0} \le Y^2$ for large Y.

Fix a *powered side* σ. Its two *represented sides* u, v and the sign ϵ_{pw} are

$$(\sigma;u,v;\epsilon_{\mathrm{pw}}) \in \{(a;b,c;-1),\ (b;a,c;-1),\ (c;a,b;+1)\}, \qquad n_v + \epsilon_{\mathrm{pw}}\, n_u = n_\sigma > 0. \tag{9.2}$$

So $\sigma \in \{a,b\}$ uses the positive difference $n_c - n_u$. The side $\sigma = c$ uses the sum $n_a + n_b$. Put

$$M = n_{\sigma,0}\, \mathfrak{r}_{\sigma,1}\mathfrak{r}_{\sigma,2}^2\mathfrak{r}_{\sigma,4}\mathfrak{r}_{\sigma,5}^2 \prod_{7\le j\le d} \mathfrak{r}_{\sigma,j}^{\,j}, \qquad x = \mathfrak{r}_{\sigma,3}\mathfrak{r}_{\sigma,4}\mathfrak{r}_{\sigma,5}\mathfrak{r}_{\sigma,6}^2. \tag{9.3}$$

Then $n_\sigma = Mx^3$. We call M the canonical coefficient. Its labels are the tuple

$$(\mathfrak{r}_{\sigma,j})_{j\in\{1,2,4,5,7,\dots,d\}}.$$

Put

(9.4)

$$\mathcal{C}_\sigma = r_\sigma - s_{\sigma,3} - s_{\sigma,6}, \qquad W_\sigma = v_\sigma + s_{\sigma,1} + 2s_{\sigma,2} + s_{\sigma,4} + 2s_{\sigma,5}, \qquad R_\sigma = r_u + r_v.$$

Here R_σ is the combined root mass of the represented sides. Put $\zeta_\sigma = \log_Y n_{\sigma,0}$. The coefficient range in (2.3) gives $0 \le \zeta_\sigma \le \varepsilon_0$. Since each labelled root lies in $[S_{\sigma,j}, 2S_{\sigma,j})$, the finite-box modulus satisfies

(9.5)

$$W_\sigma + \zeta_\sigma \le \log_Y M < W_\sigma + \zeta_\sigma + \frac{\left(6 + \sum_{7\le j\le d} j\right)\log 2}{\log Y} = W_\sigma + \zeta_\sigma + O_d\!\left(\frac{1}{\log Y}\right).$$

Lemma 9.1. (i) *There are at most $Y^{\mathcal{C}_\sigma}$ label tuples.*

(ii) *Every label tuple gives $M \ge Y^{W_\sigma}$.*

(iii) $W_\sigma - \mathcal{C}_\sigma = s_{\sigma,2} + s_{\sigma,5} + (v_\sigma - t_\sigma) \ge 0$.

(iv) *A given integer $M \le Y^2$ arises from $Y^{o_d(1)}$ label tuples.*

Proof. (i) $\#\{\mathfrak{r} : \mathfrak{r} \sim S\} = S$, and $\prod_{j\ne 3,6} S_{\sigma,j} = Y^{r_\sigma - s_{\sigma,3} - s_{\sigma,6}}$. (ii) $n_{\sigma,0} \ge 1$ and $\mathfrak{r}_{\sigma,j} \ge S_{\sigma,j}$, so $M \ge Y^{W_\sigma}$. Also

$$M \le n_{\sigma,0} \prod_{j\le d} \mathfrak{r}_{\sigma,j}^{\,j} < 2^{h_d} Y^{V_\sigma + \varepsilon_0} \le Y^2$$

for large Y, since $V_\sigma \le 1$ and $\varepsilon_0 < 1$. (iii) Expand (9.4); $v_\sigma \ge 7t_\sigma$ by (9.1). (iv) $n_{\sigma,0}$ is fixed; apply Lemma 4.3 to $M/n_{\sigma,0}$ with $r = d-2$. □

All $o(1)$ below tend to 0 as $Y \to \infty$, for fixed ε_0, d and the parameter θ of the sieve. They are uniform in the box.

9.2. **Analytic inputs.** Fix once and for all $w \in C^\infty(\mathbb{R})$ with $0 \le w \le 1$, $\operatorname{supp} w \subset [1/2, 4]$ and $w = 1$ on $[1, 2]$. For a Dirichlet character χ, extended by 0 on nonunits, and $N \ge 1$ put

$$F_N(\chi) = \sum_{n\ge 1} \chi(n)\, w(n/N). \tag{9.6}$$

We quote the all-character estimate of [6, Lemma 4]. In this section Q denotes the modulus of an analytic input, or the modulus $M\mathfrak{p}_1\mathfrak{p}_2$ of Steps 5–7 of Proposition 9.10. It is local to that input or step. It differs from the cut cofactor Q_σ and the geometry forms Q_j. The $L(s,\chi)$ below is the Dirichlet L-function, not the root mass L; s in this subsection is a complex variable.

Lemma 9.2 ([6, Lemma 4], "Hybrid fourth moment estimate")**.** *Let $H \ge 2$ and $q_0 \ge 2$. Then*

$$\sum_{\chi} \int_{|t|\le H} \left|L(\tfrac{1}{2} + it, \chi)\right|^4 dt \ll H\varphi(q_0)\log(Hq_0)^4,$$

where the sum is over all characters modulo q_0.

The all-character estimate in Lemma 9.2 is the only input needed for the next lemma. Since $\varphi(Q) \le Q$, it implies the weaker form used below.

Lemma 9.3. *For $H \ge 2$ and $Q \ge 2$,*

$$\sum_{\chi \bmod Q} \int_{|t|\le H} |L(\tfrac{1}{2} + it, \chi)|^4\, dt \ll HQ\log(HQ)^4.$$

Proof. Apply Lemma 9.2 with $q_0 = Q \geq 2$ and use $\varphi(Q) \leq Q$. In our applications $Q \leq Y^{O_{d,\theta}(1)}$. The factor $Q/\varphi(Q)$ lost here is paid in Step 7 of Proposition 9.10. □

Lemma 9.4. *For all integers $Q \geq 2$ and reals $N \geq 1$,*

$$\sum_{\substack{\chi \bmod Q \\ \chi \neq \chi_0}} |F_N(\chi)|^4 \ll Q\, N^2 \log(2Q)^4. \tag{9.7}$$

The implied constant depends only on w.

Proof. Let $\widetilde{w}(s) = \int_0^\infty w(y) y^{s-1} dy$. It is entire. Four integrations by parts give, for $\frac{1}{2} \leq \Re s \leq 2$,

$$\widetilde{w}(s) = \frac{1}{s(s+1)(s+2)(s+3)} \int_0^\infty w^{(4)}(y)\, y^{s+3} dy \ll (1+|s|)^{-4}.$$

By Mellin inversion,

$$F_N(\chi) = \frac{1}{2\pi i} \int_{(2)} L(s,\chi)\, \widetilde{w}(s)\, N^s\, ds.$$

Let $\chi \neq \chi_0$. Its partial sums $A_\chi(y) = \sum_{n \leq y} \chi(n)$ satisfy $|A_\chi(y)| \leq \varphi(Q)$. Partial summation gives $L(s,\chi) = s \int_1^\infty A_\chi(y) y^{-s-1} dy$. Thus $L(s,\chi)$ is holomorphic in $\Re s > 0$, and $|L(s,\chi)| \leq 2Q(1+|s|)$ for $\Re s \geq \frac{1}{2}$. The integrand is therefore $\ll QN^2(1+|s|)^{-3}$ on $\frac{1}{2} \leq \Re s \leq 2$. Move the line to $\Re s = \frac{1}{2}$; there is no pole. With $k_w(t) = |\widetilde{w}(\frac{1}{2} + it)| \ll (1+|t|)^{-4}$,

$$|F_N(\chi)| \leq \frac{N^{1/2}}{2\pi} \int_{\mathbb{R}} \big|L(\tfrac{1}{2} + it, \chi)\big|\, k_w(t)\, dt.$$

Hölder with respect to $k_w(t)\, dt$ gives

$$\begin{aligned} |F_N(\chi)|^4 &\leq \frac{N^2}{(2\pi)^4} \Big(\int k_w \Big)^3 \int_{\mathbb{R}} \big|L(\tfrac{1}{2} + it, \chi)\big|^4 k_w(t)\, dt \\ &\ll N^2 \int_{\mathbb{R}} \big|L(\tfrac{1}{2} + it, \chi)\big|^4 (1+|t|)^{-4} dt. \end{aligned}$$

Sum over $\chi \neq \chi_0$ and enlarge to all $\chi \bmod Q$. Split $|t| \leq 2$ and $2^{j-1} < |t| \leq 2^j$ ($j \geq 2$). By Lemma 9.3 with modulus Q and $H = 2^j$,

$$\sum_{\chi \neq \chi_0} |F_N(\chi)|^4 \ll N^2 \sum_{j \geq 1} 2^{-4(j-1)}\, 2^j Q \log(2^j Q)^4 \ll N^2 Q \log(2Q)^4 \sum_{j \geq 1} 2^{4-3j} j^4.$$

The last sum converges. □

Lemma 9.5. *For $N', N'' \geq 1$ and a Dirichlet character χ, put*

$$G(\chi) = F_{N'}(\chi) F_{N''}(\chi^2), \qquad Z_0 = 4^6 (N' N''^2)^2.$$

For every integer $Q \geq 1$ and $\delta > 0$,

$$\sum_{\chi \bmod Q} |G(\chi)|^4 \ll_\delta \varphi(Q)\, (N'N'')^2\, Z_0^\delta \Big(1 + \frac{Z_0}{Q}\Big). \tag{9.8}$$

The sum includes the principal character.

Proof. Complete multiplicativity gives

$$G(\chi)=\sum_{n\ge1}A(n)\chi(n),\qquad A(n)=\sum_{n_1n_2^2=n}w(n_1/N')\,w(n_2/N'')\ge0.$$

The coefficients do not depend on χ. Then $G(\chi)^2=\sum_m B(m)\chi(m)$ with $B=A*A\ge0$. Now $B(m)=0$ unless $m\le(4N'(4N'')^2)^2=Z_0$, and

$$B(m)\le\#\{(n_1,n_2,n_3,n_4):n_1n_2^2n_3n_4^2=m\}\ll_\delta m^\delta$$

by Lemma 4.3. Also

$$\sum_m B(m)=\Big(\sum_n A(n)\Big)^2=\Big(\sum_{n_1}w(n_1/N')\Big)^2\Big(\sum_{n_2}w(n_2/N'')\Big)^2\le(16N'N'')^2.$$

Orthogonality over all characters modulo Q gives

$$\sum_{\chi\bmod Q}|G(\chi)|^4=\sum_{\chi\bmod Q}\Big|\sum_m B(m)\chi(m)\Big|^2=\varphi(Q)\sum_{\substack{m\equiv m'\pmod Q\\(mm',Q)=1}}B(m)B(m').$$

For fixed m, at most $1+Z_0/Q$ integers $m'\in[1,Z_0]$ satisfy $m'\equiv m\pmod Q$. Hence the right side is at most

$$\varphi(Q)\sum_m B(m)\cdot\max_{m'\le Z_0}B(m')\cdot\Big(1+\frac{Z_0}{Q}\Big).$$

Insert the two bounds. □

Lemma 9.6. *Let ℓ be prime, ψ a nonprincipal and ν any character modulo ℓ, and $\epsilon\in\{\pm1\}$. Then*

$$\Big|\sum_{t\in(\mathbb{Z}/\ell)^\times}\nu(t)\,\psi(1+\epsilon t)\Big|\le\sqrt{\ell}.$$

Proof. If ν is principal the sum is $\sum_{y\in\mathbb{F}_\ell}\psi(y)-\psi(1)=-1$. Otherwise substitute $y=-\epsilon t$. The sum becomes $\nu(-\epsilon)\mathcal{J}(\nu,\psi)$ with $\mathcal{J}(\nu,\psi)=\sum_{y\in\mathbb{F}_\ell}\nu(y)\psi(1-y)$, both characters nonprincipal. Then $|\mathcal{J}(\nu,\psi)|=\sqrt{\ell}$ if $\nu\psi$ is nonprincipal and $|\mathcal{J}(\nu,\psi)|=1$ otherwise [9, Ch. 8, §3]. □

Lemma 9.7. *Let $M\ge1$, and let $\mathfrak{p}_1\ne\mathfrak{p}_2$ be primes not dividing M. Put $Q=M\mathfrak{p}_1\mathfrak{p}_2$. Let ξ be a character modulo $\mathfrak{p}_1\mathfrak{p}_2$. Assume its components modulo $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are both nonprincipal. Let $\tilde\xi$ be the character modulo Q induced by ξ, and fix $\epsilon\in\{\pm1\}$. There are coefficients $c_\epsilon(\alpha)\in\mathbb{C}$ for characters α modulo Q, with*

$$|c_\epsilon(\alpha)|\le\sqrt{\mathfrak{p}_1\mathfrak{p}_2},\tag{9.9}$$

such that for all integers U,V

$$\mathbf{1}_{(UV,Q)=1}\,\mathbf{1}_{M\mid V+\epsilon U}\,\xi\Big(\frac{V+\epsilon U}{M}\Big)=\frac{\overline{\xi(M)}}{\varphi(Q)}\sum_{\alpha\bmod Q}c_\epsilon(\alpha)\,\alpha(U)\,(\tilde\xi\bar\alpha)(V).\tag{9.10}$$

The left side is read as 0 when $M\nmid V+\epsilon U$.

Proof. If $(UV, Q) > 1$, then $\alpha(U)(\tilde{\xi}\bar{\alpha})(V) = 0$ for every α, and both sides vanish. Let $(UV, Q) = 1$. By the Chinese remainder theorem each α is $\alpha = \eta\nu$ with unique $\eta \bmod M$ and $\nu \bmod \mathfrak{p}_1\mathfrak{p}_2$; then $\tilde{\xi}\bar{\alpha} = \bar{\eta} \cdot \xi\bar{\nu}$. Define

$$c_\epsilon(\alpha) = \eta(-\epsilon)\, \hat{f}(\nu), \qquad \hat{f}(\nu) = \sum_{y \in (\mathbb{Z}/\mathfrak{p}_1\mathfrak{p}_2)^\times} \bar{\nu}(y)\, \xi(1 + \epsilon y).$$

Orthogonality on the finite group $(\mathbb{Z}/M)^\times$, for any M, gives

$$\frac{1}{\varphi(M)} \sum_{\eta \bmod M} \eta(-\epsilon U)\bar{\eta}(V) = \mathbf{1}_{-\epsilon U \equiv V \pmod M} = \mathbf{1}_{M \mid V + \epsilon U}.$$

Fourier inversion of $f(y) = \xi(1 + \epsilon y)$ on $(\mathbb{Z}/\mathfrak{p}_1\mathfrak{p}_2)^\times$, at $y = UV^{-1}$, gives

$$\frac{1}{\varphi(\mathfrak{p}_1\mathfrak{p}_2)} \sum_{\nu \bmod \mathfrak{p}_1\mathfrak{p}_2} \hat{f}(\nu)\, \nu(U)\, (\xi\bar{\nu})(V) = \xi(V)\, \xi(1 + \epsilon UV^{-1}) = \xi(V + \epsilon U).$$

Multiply; $\varphi(Q) = \varphi(M)\varphi(\mathfrak{p}_1\mathfrak{p}_2)$. The right side of (9.10) becomes

$$\overline{\xi(M)}\, \mathbf{1}_{M \mid V + \epsilon U}\, \xi(V + \epsilon U).$$

If $M \mid V + \epsilon U$, then $\xi(V + \epsilon U) = \xi(M)\, \xi((V + \epsilon U)/M)$ and $|\xi(M)| = 1$. This is (9.10). Write $\xi = \xi_{\mathfrak{p}_1}\xi_{\mathfrak{p}_2}$ and $\nu = \nu_{\mathfrak{p}_1}\nu_{\mathfrak{p}_2}$. The Chinese remainder theorem factors $\hat{f}(\nu)$ into two sums of the shape of Lemma 9.6, with $\psi = \xi_{\mathfrak{p}_1},\ \xi_{\mathfrak{p}_2}$. This gives (9.9). □

No division by x occurs in (9.10), and M need not be squarefree, odd or prime to x. For $\epsilon = +1$ this is the sum identity; for $\epsilon = -1$ the difference identity.

Lemma 9.8. *Let $K_{\mathrm{sv}} \geq 1$ and $\theta > 0$. Let $M \leq Y^{K_{\mathrm{sv}}}$ be a positive integer and*

$$\mathcal{P}_M = \{p \text{ prime}:\ p \equiv 1 \pmod 3,\ Y^\theta \leq p \leq 2Y^\theta,\ p \nmid M\}.$$

For $p \in \mathcal{P}_M$ fix a character $\chi_p \bmod p$ of exact order 3. Let $(\varpi_\iota, U_\iota, V_\iota, n_\iota)_{\iota \in \mathcal{I}}$ be a finite family with $\varpi_\iota \geq 0$ and nonzero integers $U_\iota, V_\iota, n_\iota$ satisfying $|U_\iota V_\iota n_\iota| \leq Y^{K_{\mathrm{sv}}}$. If $Y \geq Y_{\mathrm{sv}}(K_{\mathrm{sv}}, \theta)$, then $|\mathcal{P}_M| \geq Y^\theta/(3\theta \log Y)$ and

(9.11)

$$\sum_{\iota:\, n_\iota \in \mathrm{Cub}} \varpi_\iota \leq \frac{4}{|\mathcal{P}_M|} \sum_\iota \varpi_\iota + \frac{4}{|\mathcal{P}_M|^2} \sum_{\substack{\mathfrak{p}_1, \mathfrak{p}_2 \in \mathcal{P}_M \\ \mathfrak{p}_1 \neq \mathfrak{p}_2}} \Big| \sum_\iota \varpi_\iota\, \mathbf{1}_{(\mathfrak{p}_1\mathfrak{p}_2, U_\iota V_\iota) = 1}\, \chi_{\mathfrak{p}_1}(n_\iota)\overline{\chi_{\mathfrak{p}_2}(n_\iota)} \Big|,$$

where $\mathrm{Cub} = \{m^3 : m \in \mathbb{Z}\}$ is the set of integer cubes.

Proof. By the prime number theorem in progressions modulo 3,

$$\#\{p \in [Y^\theta, 2Y^\theta] : p \equiv 1 \pmod 3\} \geq \frac{Y^\theta}{2.5\, \theta \log Y}$$

for large Y. At most K_{sv}/θ of them divide M. This gives the bound for $|\mathcal{P}_M|$. For $\iota \in \mathcal{I}$ put

$$\mathcal{Z}_\iota = \sum_{\substack{p \in \mathcal{P}_M \\ p \nmid U_\iota V_\iota n_\iota}} \chi_p(n_\iota).$$

Since $0 < |U_\iota V_\iota n_\iota| \leq Y^{K_{\mathrm{sv}}}$, at most K_{sv}/θ primes of $\mathcal{P}_M$ divide $U_\iota V_\iota n_\iota$. If $n_\iota = m^3$ and $p \nmid n_\iota$, then $\chi_p(n_\iota) = \chi_p(m)^3 = 1$. So $n_\iota \in \mathrm{Cub}$ gives $\mathcal{Z}_\iota \geq |\mathcal{P}_M| - K_{\mathrm{sv}}/\theta \geq$

$|\mathcal{P}_M|/2$ for large Y. Hence

$$\mathbf{1}_{n_\iota\in\mathrm{Cub}} \le \frac{4|\mathcal{Z}_\iota|^2}{|\mathcal{P}_M|^2} \qquad (\iota\in\mathcal{I}).$$

Expand $|\mathcal{Z}_\iota|^2$. The diagonal terms $\mathfrak{p}_1=\mathfrak{p}_2$ equal 1, and there are at most $|\mathcal{P}_M|$ of them. For $\mathfrak{p}_1\neq\mathfrak{p}_2$, the conditions $\mathfrak{p}_1,\mathfrak{p}_2\nmid n_\iota$ may be dropped, because $\chi_{\mathfrak{p}_1}(n_\iota)=0$ when $\mathfrak{p}_1\mid n_\iota$. Multiply by ϖ_ι, sum over $\iota\in\mathcal{I}$, and use the triangle inequality in $(\mathfrak{p}_1,\mathfrak{p}_2)$. □

9.3. **Descriptors and the master estimate.** A *slot* is a pair (s,j) with $s\in\{u,v\}$ and $1\le j\le 6$. Its mass is $s_{s,j}$.

Definition 9.9. A *descriptor* is a triple $\mathfrak{D}=(\sigma,\mathcal{G},\mathcal{U})$. Here σ is a powered side; $\mathcal{G}$ is a set of *groups*, each of the form $g_s=\{(s,1),(s,2)\}$ with $s\in\{u,v\}$; $\mathcal{U}$ is a set of *singleton* slots disjoint from $\bigcup\mathcal{G}$; and $|\mathcal{G}|+|\mathcal{U}|=4$. Its retained set, retained mass, grouped lengths and generic exponent are

(9.12)
$$J=\mathcal{U}\cup\bigcup\mathcal{G},\qquad P_J=\sum_{(s,j)\in J}s_{s,j},\qquad \mathcal{L}_{g_s}=s_{s,1}+2s_{s,2},\qquad E_{\mathfrak{D}}=\mathcal{C}_\sigma+R_\sigma-\tfrac12 P_J.$$

Write $\widehat{\mathcal{U}}=\{\{(s,j)\}:(s,j)\in\mathcal{U}\}$ and $\mathcal{F}_{\mathfrak{D}}=\mathcal{G}\cup\widehat{\mathcal{U}}$ for the four analytic factors.

So $|J|=4$, 5 or 6. There are always four analytic factors, one per group and one per singleton. Aggregate tails are never slots. $\mathcal{G}=\emptyset$ is ordinary POW3.

Proposition 9.10. *Let $\mathfrak{D}$ be a descriptor and $\theta>0$ with*

$$W_\sigma+2\theta\ge 2\mathcal{L}_g \qquad (g\in\mathcal{G}). \tag{9.13}$$

Then

$$D\le\max\big(E_{\mathfrak{D}}+\theta,\ R_\sigma-\theta\big)+o(1). \tag{9.14}$$

Proof. Write $C=\mathcal{C}_\sigma$, $W=W_\sigma$, $R=R_\sigma$ and $\mathfrak{r}_{s,j}$, $S_{s,j}$ for the roots and sizes of the represented sides.

Step 1. Outer configurations. An outer configuration $\mathfrak{o}$ consists of the labels of M and all roots $\mathfrak{r}_{s,j}$ ($s\in\{u,v\}$, $1\le j\le d$, $(s,j)\notin J$). By Lemma 9.1(i) and $\#\{\mathfrak{r}\sim S\}=S$,

$$\#\{\mathfrak{o}\}\le Y^C\prod_{(s,j)\notin J}S_{s,j}=Y^{C+R-P_J}. \tag{9.15}$$

Fix $\mathfrak{o}$. For $(s,j)\in J$ write $\mathfrak{r}_{s,j}=\mathfrak{u}_{s,j}$ and $\mathbf{u}=(\mathfrak{u}_{s,j})_{(s,j)\in J}$. Then

$$n_u=U_{\mathfrak{o}}\prod_{(u,j)\in J}\mathfrak{u}_{u,j}^{j},\qquad n_v=V_{\mathfrak{o}}\prod_{(v,j)\in J}\mathfrak{u}_{v,j}^{j}, \tag{9.16}$$

with $U_{\mathfrak{o}},V_{\mathfrak{o}}$ fixed. Write $U(\mathbf{u}),V(\mathbf{u})$ for the right sides. Given $\mathfrak{o}$ and $\mathbf{u}$, (9.2) fixes $n_\sigma=V+\epsilon_{\mathrm{pw}}U$ and (9.3) fixes $x=(n_\sigma/M)^{1/3}$. By Lemma 4.3, $\mathfrak{r}_{\sigma,3}\mathfrak{r}_{\sigma,6}^2=x/(\mathfrak{r}_{\sigma,4}\mathfrak{r}_{\sigma,5})$ has $Y^{o(1)}$ solutions. Pairwise coprimality of the sides gives $(M,UV)=1$. Hence

$$\mathcal{B}_d\le Y^{o(1)}\sum_{\mathfrak{o}}N(\mathfrak{o}),$$
$$N(\mathfrak{o})=\#\Big\{\mathbf{u}:\ \begin{array}{l}\mathfrak{u}_{s,j}\sim S_{s,j},\ (M,UV)=1,\ M\mid V+\epsilon_{\mathrm{pw}}U,\\ (V+\epsilon_{\mathrm{pw}}U)/M\text{ is a positive integer cube}\end{array}\Big\}. \tag{9.17}$$

Step 2. Positive ambientization. For $\mathbf{u} \in \mathbb{N}^J$ put

$$\begin{aligned} \varpi_{\mathfrak{o}}(\mathbf{u}) &= \prod_{(s,j)\in J} w\big(\mathfrak{u}_{s,j}/S_{s,j}\big) \\ &\quad \cdot \mathbf{1}_{(M,UV)=1}\, \mathbf{1}_{V+\epsilon_{\mathrm{pw}}U\neq 0}\, \mathbf{1}_{M\mid V+\epsilon_{\mathrm{pw}}U}, \\ n(\mathbf{u}) &= \frac{V+\epsilon_{\mathrm{pw}}U}{M}. \end{aligned} \tag{9.18}$$

Since $w \geq 0$ and $w = 1$ on $[1, 2)$, pointwise

$$N(\mathfrak{o}) \leq \sum_{\mathbf{u}\in\mathbb{N}^J} \varpi_{\mathfrak{o}}(\mathbf{u})\, \mathbf{1}_{n(\mathbf{u})\in \mathrm{Cub}}. \tag{9.19}$$

We drop the condition $\gcd(U, V) = 1$ and the sharp dyadic windows of the retained roots, and keep $(M, UV) = 1$. We also weaken the positive-cube condition to: $n(\mathbf{u})$ is a nonzero integer cube. These changes only increase the count. We retain M, its labels, every unretained represented root and every tail in $\mathfrak{o}$. On the support, $\mathfrak{u}_{s,j} \leq 4S_{s,j}$, so $|UVn| \leq Y^8$ for large Y.

Step 3. Sieve. Apply Lemma 9.8 with $K_{\mathrm{sv}} = 8$ to the family $(\varpi_{\mathfrak{o}}(\mathbf{u}), U, V, n(\mathbf{u}))$ restricted to its support. Then

$$\begin{aligned} N(\mathfrak{o}) &\leq \frac{4}{|\mathcal{P}_M|} \sum_{\mathbf{u}} \varpi_{\mathfrak{o}}(\mathbf{u}) + 4 \max_{\substack{\mathfrak{p}_1,\mathfrak{p}_2\in\mathcal{P}_M \\ \mathfrak{p}_1\neq\mathfrak{p}_2}} |\mathcal{E}_{\mathfrak{p}_1,\mathfrak{p}_2}(\mathfrak{o})|, \\ \mathcal{E}_{\mathfrak{p}_1,\mathfrak{p}_2}(\mathfrak{o}) &= \sum_{\mathbf{u}} \varpi_{\mathfrak{o}}(\mathbf{u}) \mathbf{1}_{(\mathfrak{p}_1\mathfrak{p}_2,UV)=1}\, \xi(n(\mathbf{u})), \end{aligned} \tag{9.20}$$

with $\xi = \chi_{\mathfrak{p}_1}\bar{\chi}_{\mathfrak{p}_2}$, a character modulo $\mathfrak{p}_1\mathfrak{p}_2$ whose components are $\chi_{\mathfrak{p}_1}$ and $\bar{\chi}_{\mathfrak{p}_2}$, both nonprincipal. Also $|\mathcal{P}_M|^{-1} \leq Y^{-\theta+o(1)}$.

Step 4. Diagonal. Split $\mathfrak{o} = (\mathfrak{m}, \mathfrak{y})$ into the labels $\mathfrak{m}$ of M and the represented part $\mathfrak{y}$. For fixed $(\mathfrak{y}, \mathbf{u})$ the integers U, V are fixed and $V+\epsilon_{\mathrm{pw}}U \neq 0$ on the support. Then $M \mid V + \epsilon_{\mathrm{pw}}U$ leaves at most $\mathrm{div}(|V + \epsilon_{\mathrm{pw}}U|)$ values of M, each with $Y^{o(1)}$ label tuples by Lemma 9.1(iv). Hence

$$\begin{aligned} \sum_{\mathfrak{o}} \sum_{\mathbf{u}} \varpi_{\mathfrak{o}}(\mathbf{u}) &\leq Y^{o(1)} \sum_{\mathfrak{y}} \prod_{(s,j)\in J} \sum_{\mathfrak{u}\geq 1} w(\mathfrak{u}/S_{s,j}) \\ &\leq Y^{o(1)}\, Y^{R-P_J} \prod_{(s,j)\in J} 4S_{s,j} = Y^{R+o(1)}. \end{aligned}$$

The diagonal part of (9.20), summed over $\mathfrak{o}$, is therefore $\leq Y^{R-\theta+o(1)}$. Summing first over $\mathfrak{m}$ would give $Y^{C+R-\theta}$; the divisor recovery removes C.

Step 5. Fourier expansion. Fix $\mathfrak{o}$ and $\mathfrak{p}_1 \neq \mathfrak{p}_2$ in $\mathcal{P}_M$. Put $Q = M\mathfrak{p}_1\mathfrak{p}_2$. Since $\xi(0) = 0$ and $(M, UV) = 1$ is in $\varpi_{\mathfrak{o}}$,

$$\mathcal{E}_{\mathfrak{p}_1,\mathfrak{p}_2}(\mathfrak{o}) = \sum_{\mathbf{u}} \prod_{(s,j)\in J} w\big(\mathfrak{u}_{s,j}/S_{s,j}\big)\, \mathbf{1}_{(UV,Q)=1}\, \mathbf{1}_{M\mid V+\epsilon_{\mathrm{pw}}U}\, \xi\Big(\frac{V+\epsilon_{\mathrm{pw}}U}{M}\Big).$$

Apply Lemma 9.7. Dirichlet characters are completely multiplicative and vanish on nonunits, and $\mathbf{u}$ runs over a product set. So

$$\mathcal{E}_{\mathfrak{p}_1,\mathfrak{p}_2}(\mathfrak{o}) = \frac{\overline{\xi(M)}}{\varphi(Q)} \sum_{\alpha \bmod Q} c_{\epsilon_{\mathrm{pw}}}(\alpha)\, \alpha(U_{\mathfrak{o}})\, (\tilde{\xi}\bar{\alpha})(V_{\mathfrak{o}}) \prod_{f\in\mathcal{F}_{\mathfrak{D}}} \Phi_f\big(\gamma_f(\alpha)\big), \tag{9.21}$$

where $\gamma_f(\alpha)=\alpha$ if f lies on side u and $\gamma_f(\alpha)=\tilde{\xi}\bar{\alpha}$ if f lies on side v, and

$$\Phi_{\{(s,j)\}}(\chi)=F_{S_{s,j}}(\chi^j),\qquad \Phi_{g_s}(\chi)=G_s(\chi)=F_{S_{s,1}}(\chi)\,F_{S_{s,2}}(\chi^2).$$

For the group this uses $\chi(\mathfrak{u}_1)\chi(\mathfrak{u}_2)^2=\chi(\mathfrak{u}_1\mathfrak{u}_2^2)$. By (9.9),

$$|\mathcal{E}_{\mathfrak{p}_1,\mathfrak{p}_2}(\mathfrak{o})|\le\frac{\sqrt{\mathfrak{p}_1\mathfrak{p}_2}}{\varphi(Q)}\sum_{\alpha \bmod Q}\prod_{f\in\mathcal{F}_{\mathfrak{D}}}\bigl|\Phi_f(\gamma_f(\alpha))\bigr|. \tag{9.22}$$

This is one family of $\varphi(Q)$ modes. Each γ_f is a bijection of the character group modulo Q.

Step 6. Torsion modes. Here $Q=M\mathfrak{p}_1\mathfrak{p}_2$, as in Step 5. Let $\mathcal{T}_{\mathrm{tor}}=\{\alpha:\gamma_f(\alpha)^j=\chi_0$ for some $f=\{(s,j)\}\in\widehat{\mathcal{U}}\}$. The character group modulo Q is isomorphic to $(\mathbb{Z}/Q)^\times$, whose j-torsion has at most $j^{\omega(Q)+1}$ elements. So $|\mathcal{T}_{\mathrm{tor}}|\le 4\cdot 6^{\omega(Q)+1}=Y^{o(1)}$, as $Q\le Y^2\cdot 4Y^{2\theta}=Y^{O_{d,\theta}(1)}$. Trivially $|\Phi_f|\le\prod_{(s,j)\in f}4S_{s,j}$. By Lemma 9.1(ii), $\varphi(Q)\ge Q\,Y^{-o(1)}\ge Y^{W+2\theta-o(1)}$. The modes in $\mathcal{T}_{\mathrm{tor}}$ contribute to (9.22) at most

$$\frac{2Y^\theta}{Y^{W+2\theta-o(1)}}\,Y^{o(1)}\,4^6Y^{P_J}=Y^{P_J-W-\theta+o(1)}.$$

Sum over $\mathfrak{o}$ with (9.15). By Lemma 9.1(iii) the total is

$$Y^{C+R-W-\theta+o(1)}\le Y^{R-\theta+o(1)}.$$

Step 7. Generic modes. By Hölder with four exponents 4,

$$\sum_{\alpha\notin\mathcal{T}_{\mathrm{tor}}}\prod_{f\in\mathcal{F}_{\mathfrak{D}}}\bigl|\Phi_f(\gamma_f(\alpha))\bigr|\le\prod_{f\in\mathcal{F}_{\mathfrak{D}}}\Bigl(\sum_{\alpha\notin\mathcal{T}_{\mathrm{tor}}}\bigl|\Phi_f(\gamma_f(\alpha))\bigr|^4\Bigr)^{1/4}.$$

Singleton $f=\{(s,j)\}$: for $\alpha\notin\mathcal{T}_{\mathrm{tor}}$ the character $\gamma_f(\alpha)^j$ is nonprincipal. The map $\alpha\mapsto\gamma_f(\alpha)^j$ has fibres of size $\le 6^{\omega(Q)+1}$. Lemma 9.4 gives

$$\sum_{\alpha\notin\mathcal{T}_{\mathrm{tor}}}|\Phi_f(\gamma_f(\alpha))|^4\le 6^{\omega(Q)+1}\sum_{\chi\neq\chi_0}|F_{S_{s,j}}(\chi)|^4\le\varphi(Q)\,S_{s,j}^2\,Y^{o(1)}.$$

Here $Q/\varphi(Q)=Y^{o(1)}$, since $Q\le Y^{O_{d,\theta}(1)}$. Group $f=g_s$: γ_f is a bijection, so by Lemma 9.5

$$\sum_{\alpha}|G_s(\gamma_f(\alpha))|^4=\sum_{\chi \bmod Q}|G_s(\chi)|^4\le\varphi(Q)\,(S_{s,1}S_{s,2})^2\,Y^{o(1)}\Bigl(1+\frac{4^6Y^{2\mathcal{L}_{g_s}}}{Q}\Bigr).$$

Here $Q\ge MY^{2\theta}\ge Y^{W+2\theta}\ge Y^{2\mathcal{L}_{g_s}}$ by Lemma 9.1(ii) and (9.13). So the bracket is $\le 1+4^6$. The guard is closed: equality in (9.13) still leaves a bounded number of shifts $m'\equiv m \pmod Q$. Multiply the four bounds:

$$\sum_{\alpha\notin\mathcal{T}_{\mathrm{tor}}}\prod_{f\in\mathcal{F}_{\mathfrak{D}}}\bigl|\Phi_f(\gamma_f(\alpha))\bigr|\le\varphi(Q)\,Y^{o(1)}\prod_{(s,j)\in J}S_{s,j}^{1/2}=\varphi(Q)\,Y^{P_J/2+o(1)}.$$

In (9.22) the factor $\varphi(Q)$ cancels. Since $\sqrt{\mathfrak{p}_1\mathfrak{p}_2}\le 2Y^\theta$, the generic modes contribute $Y^{\theta+P_J/2+o(1)}$. Sum over $\mathfrak{o}$ with (9.15):

$$Y^{C+R-P_J+P_J/2+\theta+o(1)}=Y^{E_{\mathfrak{D}}+\theta+o(1)}.$$

Step 8. Assembly. By (9.17), (9.19), (9.20) and Steps 4, 6, 7,

$$\mathcal{B}_d\le Y^{o(1)}\bigl(Y^{R-\theta}+Y^{R-\theta}+Y^{E_{\mathfrak{D}}+\theta}\bigr).$$

Take $\log_Y$. □

The proof uses four fourth moments in every case. With two groups,

$$\sum_{\alpha} |G_s G_{s'} \Phi_f \Phi_{f'}| \le \|G_s\|_4 \|G_{s'}\|_4 \|\Phi_f\|_4 \|\Phi_{f'}\|_4,$$

over the one mode family; no mixed correlation and no eighth moment enter. Both guards are imposed at the same θ.

9.4. **Elimination of θ.**

Lemma 9.11. *Let $0 \le k \le 2$, let $E, R, \Gamma_1, \dots, \Gamma_k$ be real, and let $0 < \rho_0 \le 1$. Put*

$$\theta^* = \max\bigl(0, \tfrac{1}{2}(R-E), \Gamma_1, \dots, \Gamma_k\bigr), \qquad \Theta(\rho_0) = \{m\rho_0 : \ m \in \mathbb{Z},\ 1 \le m \le 4/\rho_0\},$$

and assume $\theta^* \le 3$. Some $\theta \in \Theta(\rho_0)$ satisfies $\theta \ge \Gamma_i$ for all i and

$$\max(E+\theta, R-\theta) \le \max\bigl(E, \tfrac{1}{2}(E+R), E+\Gamma_1, \dots, E+\Gamma_k\bigr) + \rho_0.$$

Proof. Let θ be the least element of $\Theta(\rho_0)$ with $\theta \ge \theta^*$. It exists since $\max \Theta(\rho_0) > 4 - \rho_0 \ge 3$. Then $\theta^* \le \theta \le \theta^* + \rho_0$. As $\theta \ge \frac{1}{2}(R-E)$, $R - \theta \le E + \theta$. So the left side is $E + \theta \le E + \theta^* + \rho_0$, and $E + \theta^*$ is the displayed maximum. □

Proposition 9.12. *Let $0 < \rho_0 \le 1$. There is $Y_{\mathrm{el}} = Y_{\mathrm{el}}(\varepsilon_0, d, \rho_0)$ such that for $Y \ge Y_{\mathrm{el}}$ and every descriptor $\mathfrak{D}$:*

(a) *if $\mathcal{G} = \emptyset$,*

$$D \le E_{\mathfrak{D}} + 2\rho_0 \quad \text{or} \quad D \le \tfrac{1}{2}(E_{\mathfrak{D}} + R_\sigma) + 2\rho_0; \tag{9.23}$$

(b) *if $\mathcal{G} = \{g\}$,*

$$D \le E_{\mathfrak{D}} + 2\rho_0 \quad \text{or} \quad D \le \tfrac{1}{2}(E_{\mathfrak{D}} + R_\sigma) + 2\rho_0 \quad \text{or} \quad D \le E_{\mathfrak{D}} + \mathcal{L}_g - \tfrac{1}{2}W_\sigma + 2\rho_0; \tag{9.24}$$

(c) *if $\mathcal{G} = \{g, g'\}$,*

$$\begin{aligned} &D \le E_{\mathfrak{D}} + 2\rho_0 \quad \text{or} \quad D \le \tfrac{1}{2}(E_{\mathfrak{D}} + R_\sigma) + 2\rho_0 \quad \text{or} \\ &D \le E_{\mathfrak{D}} + \mathcal{L}_g - \tfrac{1}{2}W_\sigma + 2\rho_0 \quad \text{or} \quad D \le E_{\mathfrak{D}} + \mathcal{L}_{g'} - \tfrac{1}{2}W_\sigma + 2\rho_0. \end{aligned} \tag{9.25}$$

Here $E_{\mathfrak{D}}$, P_J, $\mathcal{L}_g$ are as in (9.12) *and $\mathcal{C}_\sigma$, W_σ, R_σ as in* (9.4).

Proof. Write $\mathcal{G} = \{g^{(1)}, \dots, g^{(k)}\}$ and take $\Gamma_i = \mathcal{L}_{g^{(i)}} - \frac{1}{2}W_\sigma$ in Lemma 9.11. Its hypothesis holds: $\mathcal{C}_\sigma \ge 0$ and $P_J \le R_\sigma$ give $E_{\mathfrak{D}} \ge \frac{1}{2}R_\sigma \ge 0$. Also $R_\sigma \le 2$, since $r_s \le V_s \le 1$ for each represented side. Thus $\frac{1}{2}(R_\sigma - E_{\mathfrak{D}}) \le \frac{1}{4}R_\sigma \le \frac{1}{2}$; and $\Gamma_i \le \mathcal{L}_{g^{(i)}} \le V_s \le 1$. The chosen $\theta \in \Theta(\rho_0)$ satisfies (9.13). Proposition 9.10 at this θ gives

$$D \le \max\bigl(E_{\mathfrak{D}}, \tfrac{1}{2}(E_{\mathfrak{D}} + R_\sigma), E_{\mathfrak{D}} + \Gamma_1, \dots, E_{\mathfrak{D}} + \Gamma_k\bigr) + \rho_0 + o(1).$$

The grid $\Theta(\rho_0)$ and the set of descriptors are finite. So the $o(1)$ is $\le \rho_0$ for $Y \ge Y_{\mathrm{el}}$. Since $E_{\mathfrak{D}} + \max(0, \Gamma_i) = \max(E_{\mathfrak{D}}, E_{\mathfrak{D}} + \Gamma_i)$, the maximum is the largest arm. A bound by a maximum is the stated disjunction. □

Each clause is used together with the direct row (2.11), $D \le R_\sigma$. So (a) reads $D \le \min\bigl(R_\sigma, \max(E_{\mathfrak{D}}, \frac{1}{2}(E_{\mathfrak{D}} + R_\sigma))\bigr)$ up to the relaxation. A clause may not be replaced by the conjunction of its arms.

9.5. **The installed descriptor families.** Proposition 9.12 holds for every descriptor. The system of Section 11 installs the following finite families. For brevity, s_j in a descriptor denotes the slot (s,j); its mass is always $s_{s,j}$.

POW3(σ). $\mathcal{G}=\emptyset$, $\mathcal{U}=J$ any four of the twelve slots $u_1,\dots,u_6,v_1,\dots,v_6$. For $\sigma=b$ and $\sigma=c$ all $\binom{12}{4}=495$ sets are installed. For $\sigma=a$, install the 486 sets not containing $\{b_1,c_1,c_4\}$. The nine omitted sets are valid rows, but were not installed in the finite system. Including them would remove the displayed witness; the optimum of the enlarged system is not computed here.

GROUP12c(y). $\sigma=c$, $y\in\{a,b\}$, z the other represented side, $\mathcal{G}=\{g_y\}$, $\mathcal{U}=\{y_4,z_1,z_4\}$. Two clauses.

GROUP12ab(σ). $\sigma\in\{a,b\}$, z the represented side other than c, $\mathcal{G}=\{g_c\}$, $\mathcal{U}$ any three of $c_3,c_4,c_5,c_6,z_1,\dots,z_6$. In total $2\binom{10}{3}=240$ clauses.

GROUP1212ab(σ). $\sigma\in\{a,b\}$, z as before, $\mathcal{G}=\{g_c,g_z\}$, $\mathcal{U}$ any two of $z_3,z_4,z_5,z_6,c_3,c_4,c_5,c_6$. In total $2\binom{8}{2}=56$ clauses.

For these families, (9.4) and (9.12) read as follows. In GROUP12c(y),

$$C=c-s_{c,3}-s_{c,6},\qquad R=a+b,\qquad P_J=s_{y,1}+s_{y,2}+s_{y,4}+s_{z,1}+s_{z,4},$$
$$W=v_c+s_{c,1}+2s_{c,2}+s_{c,4}+2s_{c,5},\qquad \mathcal{L}_{g_y}=s_{y,1}+2s_{y,2}.$$

In GROUP12ab(σ) and GROUP1212ab(σ), $C=\sigma-s_{\sigma,3}-s_{\sigma,6}$, $W=v_\sigma+s_{\sigma,1}+2s_{\sigma,2}+s_{\sigma,4}+2s_{\sigma,5}$, $R=r_z+r_c$, $\mathcal{L}_{g_c}=s_{c,1}+2s_{c,2}$, $\mathcal{L}_{g_z}=s_{z,1}+2s_{z,2}$. Here a bare side letter is its root mass $r_s=\sum_{j\le d}s_{s,j}$ from (9.1).

All clauses of this section carry the one relaxation $2\rho_0$; we take $\rho_0=\varepsilon_0/2$. Table 12.1 records it.

10. Moment rows

10.1. **Setting.** Fix $\varepsilon_0\le 4/7$ and $d=d(\varepsilon_0)$ as in Section 3.1. Work in a nonempty box admissible in (2.3) at scale Y, and put $D=\log_Y\mathcal{B}_d$. Fix $\sigma\in\{a,b,c\}$, and let (y,z) be the other sides in alphabetical order. Choose nonempty $T\subseteq\{1,\dots,6,\mathrm{tail}\}$, with κ_T,Ω_T as in (5.1). Write $\mathfrak{m}_i$, $\mathfrak{y}_i$, $\mathfrak{z}_i$ for the roots of the σ-, y- and z-sides. Let M be the modulus (5.5), and

$$\epsilon_{\mathrm{mo}}=-1\ (\sigma=c),\qquad \epsilon_{\mathrm{mo}}=+1\ (\sigma\ne c).$$

Then the side values satisfy $n_y\equiv\epsilon_{\mathrm{mo}}\,n_z\pmod M$, as $M\mid n_\sigma$ and $n_a+n_b=n_c$. Here M is the cut modulus of (5.5); the cubic-sieve section uses its own local coefficient M. The function φ denotes Euler's totient.

A *block* is a pair $\beta=(s,j)$, where $s\in\{y,z\}$ and $1\le j\le d$. Its root x_β is $\mathfrak{y}_j$ or $\mathfrak{z}_j$. Let S_β be its dyadic size, and put $j_\beta=j$ and $h_\beta=\log_Y S_\beta$. Thus h_β is y_j or z_j; it is unrelated to $h_d=d(d+1)/2$. The block is *ordinary* when $j\le 6$. For a set $\mathcal{H}$ of blocks put $h_{\mathcal{H}}=\sum_{\beta\in\mathcal{H}}h_\beta$, and let $\mathcal{H}_y,\mathcal{H}_z$ be its blocks on y and z. Put

$$P_{\mathrm{mo}}=\sum_{\beta}h_\beta, \tag{10.1}$$

the sum over all $2d$ blocks: the total root mass of the sides y and z. Tails are included in P_{mo}.

All $o(1)$ terms below tend to 0 as $Y\to\infty$ for fixed ε_0 and d (and δ in Proposition 10.9). They are uniform in the box, in (σ,T) and in $\mathcal{H}$.

Lemma 10.1. *For $Y \ge Y_0$, $Y^{\Omega_T} \le M \le Y^2$ and $\varphi(M) \ge M/\operatorname{div}(M) \ge Y^{\Omega_T - o(1)}$. Every root x_β is prime to M. Moreover $\Omega_T \le 1$ and $h_\beta \le 1/j_\beta$.*

Proof. The lower bound is (5.6) at scale Y. M divides $\prod_j \mathfrak{m}_j^j < 2^{d(d+1)/2} Y^{V_\sigma} \le Y^2$ for large Y, by (2.4). Next $\varphi(M) = M \prod_{p|M}(1-1/p) \ge M 2^{-\omega(M)} \ge M/\operatorname{div}(M)$, and $\operatorname{div}(M) = Y^{o(1)}$ for $M \le Y^2$. Coprimality is Lemma 2.1. Finally $\Omega_T \le V_\sigma \le 1$ and $j_\beta h_\beta \le V_s \le 1$ by (2.4). □

10.2. **Reduction and orthogonality.** For a set $\mathcal{H}$ of blocks, a unit K modulo M and a character ψ modulo M put

$$\Sigma_\beta(\psi) = \sum_{S_\beta \le x < 2S_\beta} \psi(x),$$

$$N_{\mathcal{H}}(K) = \#\Big\{(x_\beta)_{\beta\in\mathcal{H}} : \begin{array}{c} S_\beta \le x_\beta < 2S_\beta,\ (x_\beta, M) = 1, \\ \prod_{\beta\in\mathcal{H}_y} x_\beta^{j_\beta} \equiv K \prod_{\beta\in\mathcal{H}_z} x_\beta^{j_\beta} \pmod M \end{array}\Big\}. \tag{10.2}$$

Lemma 10.2. *For every set $\mathcal{H}$ of blocks,*

$$\mathcal{B}_d \le Y^{\kappa_T + P_{\mathrm{mo}} - h_{\mathcal{H}} + o(1)} \max_K N_{\mathcal{H}}(K),$$

the maximum over the outer data fixed in the proof and over units K modulo the resulting M.

Proof. Enumeration. Enumerate the roots of σ selected by T. Its individual tail roots are among them exactly when tail $\in T$. Also enumerate the roots of all blocks outside $\mathcal{H}$, on y and z. A tail block in $\mathcal{H}$ remains unenumerated. As $\#\{x : S \le x < 2S\} = S$, there are $Y^{\kappa_T} \cdot Y^{P_{\mathrm{mo}} - h_{\mathcal{H}}}$ choices. Fix one. Then M is fixed.

Congruence. Write $n_y = \Pi_y \prod_{\mathcal{H}_y} x_\beta^{j_\beta}$ and $n_z = \Pi_z \prod_{\mathcal{H}_z} x_\beta^{j_\beta}$. The coefficients $n_{y,0}, n_{z,0}$ are fixed by the box, so Π_y, Π_z are fixed. They are units modulo M by Lemmas 10.1 and 2.1. So $n_y \equiv \epsilon_{\mathrm{mo}} n_z$ gives the congruence of (10.2) with $K \equiv \epsilon_{\mathrm{mo}} \Pi_z \Pi_y^{-1}$. The sign ϵ_{mo} equals ϵ_{cut} in (5.9). The roots x_β are units. So the remaining tuples number at most $N_{\mathcal{H}}(K)$.

Recovery. Given all roots of y and z, the side values n_y, n_z are fixed, hence n_σ. Divide by $n_{\sigma,0}$ and by the selected part. The quotient $Q_\sigma = \prod_{i\in[6]\setminus T} \mathfrak{m}_i^i \cdot (\prod_{j\ge 7} \mathfrak{m}_j^j)^{1-\mathbf{1}_{\mathrm{tail}\in T}} < 2^{d^2} Y$ determines the unselected roots of σ up to $\operatorname{div}(Q_\sigma)^{d-1} = Y^{o(1)}$ choices by Lemma 4.3. □

Lemma 10.3.

$$N_{\mathcal{H}}(K) = \frac{1}{\varphi(M)} \sum_{\chi \bmod M} \overline{\chi}(K) \prod_{\beta\in\mathcal{H}_y} \Sigma_\beta(\chi^{j_\beta}) \prod_{\beta\in\mathcal{H}_z} \Sigma_\beta(\overline{\chi}^{j_\beta}).$$

Proof. For units g_1, g_2, $\varphi(M)^{-1} \sum_\chi \chi(g_1)\overline{\chi}(g_2) = \mathbf{1}_{g_1 \equiv g_2}$. Take $g_1 = \prod_{\mathcal{H}_y} x_\beta^{j_\beta}$, $g_2 = K \prod_{\mathcal{H}_z} x_\beta^{j_\beta}$. Characters vanish on nonunits, so summing over all x_β in the windows imposes $(x_\beta, M) = 1$. Expand by complete multiplicativity. □

10.3. **Moment inputs.**

Lemma 10.4. *Let $j \ge 1$. Then $\#\{\chi \bmod M : \chi^j = \chi_0\} \le (2j)^{\omega(M)}$, and every fibre of $\chi \mapsto \chi^j$ has at most $(2j)^{\omega(M)}$ elements. For $j \le d$ and $M \le Y^2$ this is $Y^{o(1)}$.*

Proof. The character group is isomorphic to $(\mathbb{Z}/M)^\times$, and the fibres of a homomorphism are cosets of its kernel. By the Chinese remainder theorem count $\eta^j = 1$ locally. Odd p^e: cyclic, at most $\gcd(j, \varphi(p^e)) \le j$. 2^e: the group is 1, C_2 or $C_2 \times C_{2^{e-2}}$, at most $\gcd(j,2)\gcd(j,2^{e-2}) \le 2j$. Finally $\omega(M) \ll \log M/\log\log M$. □

We use the 2009 author-preprint formulation of [4, Theorem 1]; the published article is listed in the bibliography. The displayed bound is meaningful for $m \ge 3$, where $\log\log m > 0$. For $m = 1, 2$ the nonprincipal character set is empty, so those cases contribute zero.

Theorem B ([4, Theorem 1])**.** *For every integer $m \ge 3$ and integers a, B with $B > 0$ we have*

$$\frac{1}{\varphi(m)} \sum_{\chi \ne \chi_0} \Big| \sum_{x=a+1}^{a+B} \chi(x) \Big|^4 \ll 8^{\omega(m)} \operatorname{div}(m) (\log m)^3 (\log\log m)^7 B^2.$$

Here χ runs over all characters modulo m, including imprimitive characters. The published reference is J. Number Theory 130 (2010), no. 3, 767–785; the frozen source is the 2009 author preprint. The window $S \le x < 2S$ is $a = S - 1$, $B = S$.

Lemma 10.5. *Let $r, S, M \in \mathbb{N}$ with $r \ge 1$, $S \ge 1$ and $S^r \le M$. Then*

$$\sum_{\chi \bmod M} \Big| \sum_{S \le x < 2S} \chi(x) \Big|^{2r} \le (2^r + 1)\, \varphi(M)\, S^r \max_{n \le (2S)^r} \operatorname{div}(n)^{r-1}.$$

Proof. Expand the $2r$-th power and apply orthogonality. The left side is $\varphi(M)$ times the number of $(\mathbf{x}, \mathbf{x}') \in [S, 2S)^{2r}$ with all coordinates prime to M and $x_1 \cdots x_r \equiv x_1' \cdots x_r' \pmod M$. Fix $\mathbf{x}'$: S^r choices. Then $n = x_1 \cdots x_r < (2S)^r \le 2^r M$ lies in a fixed class modulo M: at most $2^r + 1$ values. Each n has at most $\operatorname{div}(n)^{r-1}$ factorizations by Lemma 4.3. □

Lemma 10.6. *Let β be a block, $j = j_\beta$, $S = S_\beta$, and $\mathcal{E}_j = \{\chi \bmod M : \chi^j = \chi_0\}$.*

(i) $\displaystyle\sum_{\chi \notin \mathcal{E}_j} |\Sigma_\beta(\chi^j)|^4 \le \varphi(M)\, S^2\, Y^{o(1)}$.

(ii) *If $r_{\max} \in \mathbb{N}$, $1 \le r \le r_{\max}$ and $S^r \le M$, then* $\displaystyle\sum_{\chi \bmod M} |\Sigma_\beta(\chi^j)|^{2r} \le \varphi(M)\, S^r\, Y^{o(1)}$, *the $o(1)$ depending on $r_{\max}$.*

Proof. (i) For $\chi \notin \mathcal{E}_j$, $\psi = \chi^j$ is nonprincipal, and each ψ has at most $(2j)^{\omega(M)}$ preimages (Lemma 10.4). So the sum is at most $(2j)^{\omega(M)} \sum_{\psi \ne \psi_0} |\Sigma_\beta(\psi)|^4$. For $M \le 2$ this vanishes. For $M \ge 3$ apply Theorem B with $m = M$, $a = S - 1$, $B = S$. Its factor is at most $\operatorname{div}(M)^4 (2\log Y)^{10} = Y^{o(1)}$. (ii) The same fibre bound reduces to all ψ; apply Lemma 10.5. The total factor is $(2j)^{\omega(M)}(2^{r_{\max}} + 1) \max_{n \le (2S)^r} \operatorname{div}(n)^{r-1}$, which is $Y^{O_{d, r_{\max}}(1/\log\log Y)}$. □

Lemma 10.7. *Let $\mathcal{X}$ be a set of characters modulo M and $\mathcal{H}$ a finite set. For $\beta \in \mathcal{H}$ let $f_\beta : \mathcal{X} \to \mathbb{C}$, $S_\beta \ge 1$, $C_{\mathrm{H}} \ge 1$ and integers $r_\beta \ge 1$ satisfy*

$$|f_\beta| \le S_\beta, \qquad \sum_{\chi \in \mathcal{X}} |f_\beta(\chi)|^{2r_\beta} \le C_{\mathrm{H}}\, \varphi(M)\, S_\beta^{r_\beta}.$$

Let $0 \le \vartheta_\beta \le 1$ with $\sum_\beta \vartheta_\beta/(2r_\beta) \le 1$. Then

$$\frac{1}{\varphi(M)} \sum_{\chi \in \mathcal{X}} \prod_{\beta \in \mathcal{H}} |f_\beta(\chi)| \le C_{\mathrm{H}}^{|\mathcal{H}|} \prod_{\beta \in \mathcal{H}} S_\beta^{1-\vartheta_\beta/2}.$$

Proof. $|f_\beta| \le S_\beta^{1-\vartheta_\beta} |f_\beta|^{\vartheta_\beta}$. Apply Hölder to the functions $|f_\beta|^{\vartheta_\beta}$ ($\vartheta_\beta > 0$) with exponents $2r_\beta/\vartheta_\beta$, and to the constant 1 with the complementary exponent. With $|\mathcal{X}| \le \varphi(M)$,

$$\begin{aligned} \sum_{\mathcal{X}} \prod_\beta |f_\beta|^{\vartheta_\beta} &\le \varphi(M)^{1-\sum \vartheta_\beta/(2r_\beta)} \\ &\quad \cdot \prod_\beta \big(C_{\mathrm{H}} \varphi(M) S_\beta^{r_\beta}\big)^{\vartheta_\beta/(2r_\beta)} \\ &\le C_{\mathrm{H}}^{|\mathcal{H}|} \varphi(M) \prod_\beta S_\beta^{\vartheta_\beta/2}. \end{aligned}$$

Multiply by $\prod_\beta S_\beta^{1-\vartheta_\beta}$. □

10.4. **The rows.**

Proposition 10.8 (CS4)**.** *Let $\mathcal{H}$ be a set of at most four blocks, in total over y and z. Then*

$$D \le \kappa_T + P_{\mathrm{mo}} - \min\Big(\Omega_T, \frac{h_{\mathcal{H}}}{2}\Big) + o(1). \tag{10.3}$$

Proof. If $\mathcal{H} = \emptyset$, then $N_\emptyset(K) = \mathbf{1}_{K \equiv 1 \pmod M} \le 1$, and the assertion is immediate. Write $h = h_{\mathcal{H}}$. By Lemma 10.2 it suffices to show $N_{\mathcal{H}}(K) \le Y^{\max(h-\Omega_T, h/2)+o(1)}$ uniformly in K. Expand by Lemma 10.3. Let $\mathcal{E} = \bigcup_{\beta \in \mathcal{H}} \mathcal{E}_{j_\beta}$, the characters for which some held power is principal. It contains χ_0.

Torsion. $|\mathcal{E}| \le 4(2d)^{\omega(M)} = Y^{o(1)}$ by Lemma 10.4. On $\mathcal{E}$ use $|\Sigma_\beta| \le S_\beta$. By Lemma 10.1 these characters contribute at most

$$\frac{|\mathcal{E}|}{\varphi(M)} \prod_\beta S_\beta \le Y^{h-\Omega_T+o(1)}.$$

Generic. Let $\mathcal{X}$ be the complement of $\mathcal{E}$. For $\chi \in \mathcal{X}$ and every β, χ^{j_β} and $\overline{\chi}^{j_\beta}$ are nonprincipal, and $|\Sigma_\beta(\overline{\chi}^{j_\beta})| = |\Sigma_\beta(\chi^{j_\beta})|$. Lemma 10.6(i) gives the hypothesis of Lemma 10.7 with $r_\beta = 2$, $C_{\mathrm{H}} = Y^{o(1)}$. Take $\vartheta_\beta = 1$; then $\sum_\beta \vartheta_\beta/4 = |\mathcal{H}|/4 \le 1$. The generic characters contribute at most $Y^{o(1)} \prod_\beta S_\beta^{1/2} = Y^{h/2+o(1)}$.

Total. $N_{\mathcal{H}}(K) \le Y^{o(1)}(Y^{h-\Omega_T} + Y^{h/2})$. With Lemma 10.2,

$$D \le \kappa_T + P_{\mathrm{mo}} - h + \max\Big(h - \Omega_T, \frac{h}{2}\Big) + o(1) = \kappa_T + P_{\mathrm{mo}} - \min\Big(\Omega_T, \frac{h}{2}\Big) + o(1).$$

□

No case distinction in Ω_T occurs. The proof holds for every $M \ge 1$; for $M \le 2$ the generic sum is empty. If $\mathcal{H} = \emptyset$ the row is trivial.

Proposition 10.9 (PS23)**.** *Let $0 < \delta \le 1/2$. Then*

$$D \le \kappa_T + P_{\mathrm{mo}} - \min\Big(\frac{P_{\mathrm{mo}}}{2}, \frac{2\Omega_T}{3}\Big) + d\delta + o(1), \tag{10.4}$$

the $o(1)$ depending on δ.

Proof. Paid blocks. Let $\mathcal{H} = \{\beta : h_\beta \ge \delta\}$ and $h = h_{\mathcal{H}}$. The other blocks number at most $2d$, so $P_{\mathrm{mo}} - h < 2d\delta$.

Orders. For $\beta \in \mathcal{H}$ put

$$r_\beta = 2 \quad (h_\beta > \Omega_T/2), \qquad r_\beta = \lfloor \Omega_T/h_\beta \rfloor \quad (h_\beta \le \Omega_T/2).$$

In the second case $2 \le r_\beta \le 1/\delta$, by Lemma 10.1, and $S_\beta^{r_\beta} = Y^{r_\beta h_\beta} \le Y^{\Omega_T} \le M$. In both cases

$$r_\beta h_\beta \ge \frac{2\Omega_T}{3}. \tag{10.5}$$

Indeed $2h_\beta > \Omega_T$ in the first case. In the second, put $t = \Omega_T/h_\beta \ge 2$: for $t < 3$, $\lfloor t \rfloor / t = 2/t > 2/3$; for $t \ge 3$, $\lfloor t \rfloor > t - 1 \ge 2t/3$.

Moments. Expand $N_{\mathcal{H}}(K)$ by Lemma 10.3. Let $\mathcal{E} = \bigcup_{\beta\in\mathcal{H}} \mathcal{E}_{j_\beta}$ and $\mathcal{X}$ its complement. On $\mathcal{X}$,

$$\sum_{\chi\in\mathcal{X}} |\Sigma_\beta(\chi^{j_\beta})|^{2r_\beta} \le \varphi(M)\, S_\beta^{r_\beta}\, Y^{o(1)} \qquad (\beta \in \mathcal{H}),$$

by Lemma 10.6(i) if $h_\beta > \Omega_T/2$, and by Lemma 10.6(ii) with $r_{\max} = \lfloor 1/\delta \rfloor$ if $h_\beta \le \Omega_T/2$.

Budget. Put $b_{\mathrm{H}} = \sum_{\beta\in\mathcal{H}} 1/(2r_\beta)$ and $\vartheta = \min(1, 1/b_{\mathrm{H}})$, with $\vartheta = 1$ if $\mathcal{H} = \emptyset$. Then $\sum_\beta \vartheta/(2r_\beta) \le 1$. By (10.5),

$$\frac{\vartheta}{2}\, h = \vartheta \sum_\beta \frac{r_\beta h_\beta}{2r_\beta} \ge \frac{2\Omega_T}{3}\, \vartheta b_{\mathrm{H}}.$$

If $b_{\mathrm{H}} \le 1$, then $\vartheta = 1$ and the saving $\vartheta h/2$ equals $h/2$. If $b_{\mathrm{H}} > 1$, then $\vartheta b_{\mathrm{H}} = 1$ and $\vartheta h/2 \ge 2\Omega_T/3$. In both cases $\vartheta h/2 \ge \min(h/2, 2\Omega_T/3)$.

Generic. Lemma 10.7 with $\vartheta_\beta = \vartheta$ and $|\mathcal{H}| \le 2d$ bounds the generic characters by $Y^{h - \vartheta h/2 + o(1)} \le Y^{h - \min(h/2, 2\Omega_T/3) + o(1)}$.

Torsion. $|\mathcal{E}| \le 2d(2d)^{\omega(M)} = Y^{o(1)}$. As in Proposition 10.8 these characters contribute $Y^{h - \Omega_T + o(1)}$. Since $\min(h/2, 2\Omega_T/3) \le \Omega_T$, this is dominated.

Total. By Lemma 10.2,

$$D \le \kappa_T + P_{\mathrm{mo}} - \min\Big(\frac{h}{2}, \frac{2\Omega_T}{3}\Big) + o(1).$$

Finally $\min(h/2, 2\Omega_T/3) \ge \min(P_{\mathrm{mo}}/2, 2\Omega_T/3) - (P_{\mathrm{mo}} - h)/2$ and $(P_{\mathrm{mo}} - h)/2 < d\delta$. □

If $h_\beta \le \Omega_T/2$, then $S_\beta^2 \le M$, and Lemma 10.6(ii) with $r = 2$ gives the bound of Lemma 10.6(i). Thus this proof invokes Theorem B only for blocks with $h_\beta > \Omega_T/2$. When every block is at most $\Omega_T/2$, the elementary moment suffices.

For larger blocks the elementary moment with Lemma 10.7 falls short. Take $\Omega_T = 1$ and four block masses

$$\frac{3}{5}, \quad \frac{17}{50}, \quad \frac{17}{50}, \quad \frac{1}{50}.$$

The target saving is $\min(P_{\mathrm{mo}}/2, 2\Omega_T/3) = 13/20$. With the elementary moment, the available orders satisfy $r_\beta \le \lfloor \Omega_T/h_\beta \rfloor$, giving $r = (1, 2, 2, 50)$. The best saving with per-block exponents is the fractional-knapsack value

$$\max_{\substack{0\le\vartheta_i\le 1 \\ \sum_i \vartheta_i/(2r_i)\le 1}} \frac{1}{2}\sum_i \vartheta_i h_i = \frac{161}{250}, \qquad (\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4) = \left(\frac{49}{50}, 1, 1, 1\right).$$

The greedy order is by the ratio $r_i h_i$. A uniform exponent instead gives $\vartheta = 100/101$ and saving $65/101$. Even the per-block optimum is short by

$$\frac{13}{20} - \frac{161}{250} = \frac{3}{500}.$$

The masses and Ω_T are homogeneous. Rescale them into the admissible region $L \le 1$. This concerns only that method. It is no counterexample to Proposition 10.9.

Corollary 10.10. *Put $\delta = \varepsilon_0/(2d)$. Fix $Y \ge Y_0$, a pair (σ, T), and a set $\mathcal{H}$ of at most four ordinary blocks. Then at least one arm of each displayed disjunction holds:*

$$D \le \kappa_T + P_{\mathrm{mo}} - \Omega_T + \rho_{\mathrm{CS}} \quad \text{or} \quad D \le \kappa_T + P_{\mathrm{mo}} - \tfrac{1}{2} h_{\mathcal{H}} + \rho_{\mathrm{CS}}, \tag{10.6}$$

$$D \le \kappa_T + \tfrac{1}{2} P_{\mathrm{mo}} + \rho_{\mathrm{PS}} \quad \text{or} \quad D \le \kappa_T + P_{\mathrm{mo}} - \tfrac{2}{3}\Omega_T + \rho_{\mathrm{PS}} \tag{10.7}$$

with $\rho_{\mathrm{CS}} = O_d(1/\log\log Y) \le \varepsilon_0/2$ and $\rho_{\mathrm{PS}} = \varepsilon_0/2 + O_{\varepsilon_0,d}(1/\log\log Y) \le \varepsilon_0$.

Proof. Propositions 10.8 and 10.9 apply, since $d\delta = \varepsilon_0/2$. The divisor, prime-factor and logarithmic factors are each $Y^{O_d(1/\log\log Y)}$. The exponents depend on d and $1/\delta$. The constants contribute $O(1/\log Y)$. The families are finite. A maximum gives the disjunction of its arms. □

The installed families are: $\mathrm{CS4}(\sigma, T, \mathcal{H})$ with $|\mathcal{H}| = 4$ ordinary blocks, $3 \cdot 127 \cdot \binom{12}{4} = 188\,595$ descriptors; and $\mathrm{PS23}(\sigma, T)$, $3 \cdot 127 = 381$ descriptors. Table 12.1 records the relaxation of each arm. The certificate fixes the actual held set $\mathcal{H}$ of each CS4 clause.

11. The finite system

The variables are the 28 nonnegative exponents

$$(a, b, c;\ a_1, \dots, a_6, b_1, \dots, b_6, c_1, \dots, c_6;\ v_a, v_b, v_c;\ f_a, f_b, f_c;\ D). \tag{11.1}$$

Here L, p_i, τ_s and V_s of (6.1) are linear forms. The auxiliary variables f_s encode (2.12):

$$\begin{gathered} f_s \ge s_2 + s_4 + s_6, \qquad f_s \ge s_3 + s_6, \qquad f_s \ge s_5 \qquad (s = a, b, c), \\ f_a + f_b + f_c \le 4L - 6D. \end{gathered} \tag{11.2}$$

A point satisfies (2.12) if and only if some f_s satisfy (11.2); take f_s the maximum. Since $\mathsf{A}_{\mathrm{cut}} + \max\{\mathsf{B}_{\mathrm{cut}}, 0\} = \max(\mathsf{A}_{\mathrm{cut}}, \mathsf{A}_{\mathrm{cut}} + \mathsf{B}_{\mathrm{cut}})$, the limiting cut (5.3) is the clause

$$D \le \mathsf{A}_{\mathrm{cut}} \quad \text{or} \quad D \le \mathsf{A}_{\mathrm{cut}} + \mathsf{B}_{\mathrm{cut}}. \tag{11.3}$$

Let $\mathcal{S}$ be the following system.

- 29 linear rows: (2.8), (2.9), (2.10), (2.11), the last two rows of (3.1) per side, the ten rows of (11.2), (7.1) and (6.4).
- The clauses of Table 11.1, each with all its arms.

All rows are in the limiting form of Table 12.1: every entry in its last column is dropped. A clause holds if one of its arms holds. It is never replaced by the conjunction of its arms. Coefficients, dyadic bounds, tail enumeration and recovery costs are inside the rows. So the theorems below are finite statements about (11.1).

The descriptor sets are those of Sections 5, 8, 9.5 and 10. The 242 one-group clauses are the two GROUP12c clauses and the 240 GROUP12ab clauses. In total

TABLE 11.1. The clauses of $\mathcal{S}$.

clause	arms	number	source
(G1)–(G13)	2	13	Appendix B
(6.5)	2	1	Corollary 6.3
(8.5)	2	30	Corollary 8.2
(11.3)	2	1 560 195	Proposition 5.1
(10.6)	2	188 595	Corollary 10.10
(10.7)	2	381	Corollary 10.10
(9.23)	2	1476	Proposition 9.12(a)
(9.24)	3	242	Proposition 9.12(b)
(9.25)	4	56	Proposition 9.12(c)

$\mathcal{S}$ has 29 linear rows and 1 750 989 clauses. The certificate below uses only these families.

11.1. **The certificate.**

Theorem 2 (Computer-assisted)**.** *Every nonnegative solution of $\mathcal{S}$ satisfies $D \le 20/37$.*

Proof. Write x for the vector (11.1). Let e_D be the unit vector in the D coordinate. The certificate is a finite rooted trie. Each internal node carries one clause of $\mathcal{S}$ and all its arms as children. Each leaf t carries a set $I(t)$ of rows. These are the linear rows of $\mathcal{S}$, the rows $-x_k \le 0$ and the arms on the path from the root to t. No other row is admissible. Write each row as $\langle g_i, x\rangle \le b_i$. The certificate gives $\eta_i \ge 0$ in $\mathbb{Q}$ on $I(t)$. The checker verifies at every leaf

$$\sum_{i\in I(t)} \eta_i g_i = e_D, \qquad \sum_{i\in I(t)} \eta_i b_i \le \frac{20}{37}. \tag{11.4}$$

Let $x \ge 0$ satisfy $\mathcal{S}$. At each internal node x satisfies one arm of its clause. Descend into that child. So x reaches a leaf t, and every row of $I(t)$ holds at x. Hence

$$D = \langle e_D, x\rangle = \sum_{i\in I(t)} \eta_i \langle g_i, x\rangle \le \sum_{i\in I(t)} \eta_i b_i \le \frac{20}{37}. \tag{11.5}$$ □

The checker also verifies that no leaf path is a prefix of another. The clause (6.5) may occur at any depth; every (6.5) node has both children. Put

$$\Lambda_U = \max_t \sum_{\substack{i\in I(t)\\ \text{not } -x_k\le 0}} \eta_i. \tag{11.6}$$

Each row is encoded in the normalisation of its displayed source and of Table C.1. In that normalisation its right-hand side rises by at most the entry of Table 12.1. The checker gives $\Lambda_U = 586/201$, attained at leaf 95 263. Tables 11.2 and 11.3 give the statistics. The combined row for the two grouped families in Table 11.3 records their certificate census together.

11.2. **The optimum.** Let x^* be the point

$$\begin{gathered} a = \tfrac{17}{37},\ a_1 = \tfrac{7}{37},\ a_3 = \tfrac{10}{37}; \qquad b = \tfrac{7}{37},\ b_1 = \tfrac{2}{37},\ v_b = \tfrac{35}{37}; \\ c = \tfrac{13}{37},\ c_1 = \tfrac{5}{37},\ c_4 = \tfrac{8}{37}; \qquad f_a = \tfrac{10}{37},\ f_c = \tfrac{8}{37}; \qquad D = \tfrac{20}{37}, \end{gathered} \tag{11.7}$$

with every unlisted coordinate zero.

TABLE 11.2. The certificate of Theorem 2.

leaves (all of kind `upper`)	394 633
internal nodes	394 243
nodes	788 876
depth	49
infeasible leaves	0
Λ_U	586/201
worst certificate value $\sum_i \eta_i b_i$	20/37
leaves with certificate value exactly 20/37	1 358
largest number of nonzero multipliers on a leaf	28
distinct cuts (11.3) on paths	17 256

TABLE 11.3. Census of the certificate by family. A row of a clause family is one of its arms.

family	internal nodes	distinct clauses on paths	distinct rows with $\eta_i > 0$	pairs (leaf, row) with $\eta_i > 0$
linear rows of $\mathcal{S}$			29	2 061 265
nonnegativity			21	2 478 333
(6.5)	4 972	1	2	26 673
(G1)–(G13)	27 223	13	26	675 941
(8.5)	15 468	30	60	479 423
(11.3)	236 038	17 256	34 116	2 417 940
(10.6)	48 765	10 649	21 220	644 485
(10.7)	61 110	155	310	673 495
(9.23)	387	75	149	1 924
(9.24), (9.25)	280	27	89	2 679

Proposition 11.1. *x^* satisfies $\mathcal{S}$. Thus 20/37 is the exact optimum of the installed system $\mathcal{S}$.*

Proof. The witness verifier of Appendix C checks every row and every arm at x^* in exact arithmetic. Table 11.4 gives the result. We check the binding rows by hand.

Linear rows. $L = 1$, and

$$V_a = \tfrac{7}{37} + 3 \cdot \tfrac{10}{37} = 1, \qquad V_b = \tfrac{2}{37} + \tfrac{35}{37} = 1, \qquad V_c = \tfrac{5}{37} + 4 \cdot \tfrac{8}{37} = 1.$$

So (6.4) and $\sum_{i \le 6} i s_i + v_s \le 1$ hold with equality. Also $\tau_a = \tau_c = 0$ and $\tau_b = 5/37$, so $v_b = 7\tau_b$. Then (2.10) holds with equality on all three sides. The pair rows give $b + c = 20/37 = D$. For (11.2), $f_a = a_3$, $f_b = 0$, $f_c = c_4$, and $f_a + f_b + f_c = 18/37 \le 28/37 = 4L - 6D$. For (7.1), $L - p_3 = 27/37$.

Clauses. One arm suffices. Both arms of (6.5) hold. For (G2), $P_2 = 24/37$, $Q_2 = 17/37$ and $L - Q_2 = 20/37$. For (8.5) with $(e, y, z, \ell) = (a, b, c, 2)$, $\mathsf{B}_{\mathrm{sp}} = V_a - V_c + c_2 = 0$ and $\mathsf{A}_{\mathrm{sp}} = b + c - c_2 = 20/37$. For (11.3) with $\sigma = c$, $T = \{1, 4\}$, $R_y = \{1, 3\}$, $R_z = \{1\}$: $q = 1$,

$$\mathsf{A}_{\mathrm{cut}} = (a - a_1 - a_3) + (b - b_1) + c_1 + c_4 = \tfrac{18}{37},$$
$$\mathsf{B}_{\mathrm{cut}} = (a_1 + 3a_3 + b_1) - (c_1 + 4c_4) = \tfrac{39}{37} - 1 = \tfrac{2}{37}.$$

For (10.7) with $\sigma = b$, $T = \{\mathrm{tail}\}$: $\kappa_T = \tau_b = 5/37$, $\Omega_T = v_b$, $P_{\mathrm{mo}} = a + c = 30/37$, and $\kappa_T + P_{\mathrm{mo}}/2 = 20/37$. For (10.6) with $\sigma = a$, $T = \{1\}$, $\mathcal{H} = \{b_1, b_2, c_1, c_4\}$: $\kappa_T = \Omega_T = 7/37$, and $\kappa_T + P_{\mathrm{mo}} - \Omega_T = b + c = 20/37$. For (9.23) with $\sigma = c$, $J =$

$\{a_1, a_2, a_3, b_1\}$: $C_c = 13/37$, $R_c = 24/37$, $P_J = 19/37$, and $E_{\mathfrak{D}} = 55/74 > 20/37$. This is the smallest bound within POW3(c). □

TABLE 11.4. Smallest bound at x^* per family. The bound of a clause is its largest arm. For (9.23)–(9.25) it is taken before intersection with (2.11). The other linear rows hold.

family	entries	smallest bound
(2.11)	3	20/37
(7.1)	1	27/37
(G1)–(G13)	13	20/37
(8.5)	30	20/37
(11.3)	1 560 195	20/37
(10.6)	188 595	20/37
(10.7)	381	20/37
POW3(a), (b), (c)	486, 495, 495	41/74, 26/37, 55/74
GROUP12c, group on a; on b	1; 1	33/37; 65/74
GROUP12ab(a); (b)	120; 120	21/37; 26/37
GROUP1212ab(a); (b)	28; 28	21/37; 26/37

The nine POW3(a) descriptors with $J \supseteq \{b_1, c_1, c_4\}$ are valid rows. They are not in $\mathcal{S}$. At x^* they have $P_J = 15/37$, $E_{\mathfrak{D}} = 39/74 < 20/37$ and $\frac{1}{2}(E_{\mathfrak{D}} + R_a) = 79/148 < 20/37$. Both arms fail at x^*. Leaving out valid rows keeps Theorem 2 true. The point x^* lies in the installed $\mathcal{S}$. Adding the nine valid rows removes this witness; the optimum of that enlarged system is not asserted here. The point is not an *abc* triple and gives no lower bound for $N_1(X)$.

12. Stability and the endpoint

Lemma 12.1. *Let $\rho \geq 0$ and $x \geq 0$. Suppose that, with right-hand sides raised by ρ,*

- *every linear row of $\mathcal{S}$ holds at x;*
- *every clause of $\mathcal{S}$ has an arm that holds at x.*

The rows $-x_k \leq 0$ are not relaxed. Then

$$D \leq \frac{20}{37} + \Lambda_U \rho. \tag{12.1}$$

Proof. Descend the trie as in the proof of Theorem 2, with relaxed arms. At the leaf, (11.5) with relaxed right-hand sides adds

$$\rho \sum_{i \text{ not } -x_k \leq 0} \eta_i \leq \Lambda_U \rho.$$ □

Lemma 12.2. *Let $0 < \mu \leq 1$. Let $Y_0 = Y_0(\varepsilon_0, d)$ be the largest of Y_{red} of Section 2, $\exp(\exp(1))$, $Y_{\mathrm{sv}}(8, \theta)$ for $\theta \in \Theta(\varepsilon_0/2)$, $Y_{\mathrm{el}}(\varepsilon_0, d, \varepsilon_0/2)$ and two further thresholds. The first is the point beyond which the statements made for large Y in Sections 6–10 hold. The second is the least Y beyond which each displayed vanishing loss, including $\log_Y 2^{1+h_d}$, is at most $\varepsilon_0/2$. It depends only on ε_0 and d. Let $Y \geq Y_0$, and take a nonempty box admissible in (2.3) at scale Y. Then every linear row of*

$\mathcal{S}$ holds in a μ-free form. So does at least one arm of every clause. Each right-hand side rises by at most the amount in Table 12.1. In particular (2.8) *becomes* $L \le 1 + 3\varepsilon_0/4$. *Consequently*

$$\rho = 18\varepsilon_0 + o_{\varepsilon_0,d}(1) \tag{12.2}$$

is admissible in Lemma 12.1, and $\rho \le 19\varepsilon_0$ *for* $\mu \le 1$ *and* $Y \in [Y_0, X]$.

TABLE 12.1. The relaxation carried by each family of $\mathcal{S}$. Here $\varepsilon_1 = \varepsilon_0$, $\rho_0 = \varepsilon_0/2$ and $\delta = \varepsilon_0/(2d)$.

family	source	raised by
(2.8)	[2, (6.1)]	$3\varepsilon_0/4$
(2.9), (2.10), (3.1), the f_s rows of (11.2)	definitions and (2.4)	0
(2.11)	Lemma A.2	$O_d(1/\log\log Y)$
Appendix B	Corollary A.5	$6\varepsilon_0 + o_{\varepsilon_0,d}(1)$
(2.12), the last row of (11.2)	Lemma A.3, D-coefficient 6	$18\varepsilon_0 + o_{\varepsilon_0,d}(1)$
(5.3), (11.3)	Proposition 5.1	$o_{\varepsilon_0,d}(1)$
(6.4)	Lemma 6.1	$\varepsilon_0/2$
(6.5), each arm	Lemma 6.2	$3\varepsilon_0/2 + \log_Y 2^{1+h_d}$
(7.1)	Proposition 7.1	$\varepsilon_0 + O_{\varepsilon_0}(1/\log Y)$
(8.5), each arm	Proposition 8.1	$\varepsilon_0 + O_d(1/\log\log Y)$
(9.23)–(9.25), each arm	Proposition 9.12	$2\rho_0 = \varepsilon_0$
(10.6), each arm	Corollary 10.10	$O_d(1/\log\log Y)$
(10.7), each arm	Corollary 10.10	$\varepsilon_0/2 + O_{\varepsilon_0,d}(1/\log\log Y)$

Proof. Run Section 2 at scale Y with λ replaced by μ and $\log_Y$ in place of $\log_X$ in (2.5). In (2.4), μ occurs only in the radical constraint. Its upper half is

$$L \le \mu + 3\varepsilon_0/4 \le 1 + 3\varepsilon_0/4, \tag{12.3}$$

the one row of $\mathcal{S}$ that depends on μ. Its lower half is

$$\mu \le L + O_d\Big(\frac{1}{\log Y}\Big). \tag{12.4}$$

The proof of [2, Theorem 1.3] uses the weaker radical bound

$$\prod_{j\le d} A_j B_j C_j \le Y^{\mu+3\varepsilon_0} \le Y.$$

This needs $\varepsilon_0 \le (1-\mu)/3$, false at $\mu = 1$ for every $\varepsilon_0 > 0$. It is the only use of $\mu < 1$ in that proof, and the visible source of its μ-dependent constant. We keep (12.3) as a relaxed row instead.

By (12.4), μ leaves the other rows. The other constraints of (2.4) are μ-free. So (2.9), (2.10), (3.1) and Lemma 3.1 are μ-free and exact. So are the rows $f_s \ge \cdots$ of (11.2), which define f_s. The constants of the reduction and of Appendix A depend only on ε_0 and d, not on μ. The condition $\varepsilon_0 \le (1-\mu)/3$ is needed for the separate step $ABC \le Y$ in the proof of [2, Theorem 1.3].

Pair row. [2, Proposition 2.3] has no rate in Y. Lemma A.2 at scale Y gives (2.11) with the factor $\Delta = Y^{O_d(1/\log\log Y)}$. So (2.11) costs $O_d(1/\log\log Y)$, as in Table 12.1.

Cut. The proof of Proposition 5.1 uses only the dyadic ranges, (2.2) and the fixed-d lemmas. The same argument at scale Y applies for every $0 < \mu \le 1$. Its divisor and root-class factors cost $O_d(1/\log\log Y)$.

Fourier and geometry. Lemma A.3 at scale Y contains no μ; its ε_0-exponent is $3\varepsilon_0$. Our Fourier row is κ_F times the logarithm of that bound, with

$$\kappa_F = \frac{[D]_{\mathrm{row}}}{[D]_{\mathrm{lemma}}} = \frac{6}{1} = \frac{[L]_{\mathrm{row}}}{[L]_{\mathrm{lemma}}} = \frac{4}{2/3} = \frac{1}{1/6} = 6$$

on the D, L and root terms. So $3\varepsilon_0$ becomes $18\varepsilon_0$. Corollary A.5 has ε_0-exponents $4\varepsilon_0$, $6\varepsilon_0$, and μ appears as Y^{μ} and $Y^{\mu-1}$. By (12.4), $\mu \to L$ costs $O_d(1/\log Y)$. The rows (G1)–(G13) have coefficient 1 on D and L, so they rise by at most $6\varepsilon_0$.

New rows. Sections 6–10 work at scale Y with $\log_Y$ coordinates. They use (2.2), the dyadic ranges, the coefficient bound and the μ-free constraints of (2.4). So their rows are μ-free. Their errors are those of Corollary 6.3, Proposition 7.1 with $\varepsilon_1 = \varepsilon_0$, Corollary 8.2, Proposition 9.12 with $\rho_0 = \varepsilon_0/2$, and Corollary 10.10 with $\delta = \varepsilon_0/(2d)$. For $Y \ge Y_0$ each is at most $2\varepsilon_0$. The cubic-sieve proofs use only $M \ge Y^{W_\sigma}$; the coefficient $n_{\sigma,0} \ge 1$ is the only coefficient property used in that bound. The factor $Q/\varphi(Q)$ is accounted for in Step 7 of Proposition 9.10. The factor six above multiplies only the printed $3\varepsilon_0$ of the Fourier row. No other row carries it.

These are the entries of Table 12.1; the largest is (12.2). All constants depend only on ε_0 and d, not on μ. The Y-dependent errors are the displayed $O_d(1/\log Y)$, $O_d(1/\log\log Y)$ and $o_{\varepsilon_0,d}(1)$ terms. They include the constants of the reduction in Section 2, of Lemma A.3 and of Corollary A.5. The Y_0 threshold absorbs them. □

By (12.2),

$$\Lambda_U \rho = \frac{586}{201}\big(18\varepsilon_0 + o_{\varepsilon_0,d}(1)\big) = \frac{3516}{67}\,\varepsilon_0 + o_{\varepsilon_0,d}(1). \tag{12.5}$$

The certificate has no infeasible leaf, so no infeasibility margin enters.

Lemma 12.2 removes the restriction $\lambda < 1$ of [2, Theorem 1.3]. At $\mu = 1$ the row (2.8) is lost, and Lemma 12.1 prices the relaxation ρ at $\Lambda_U \rho$ in the exponent. The constant does not depend on μ. $\mathcal{S}$, its certificate and Λ_U are free of ε_0 and d. So choosing ε_0 from Λ_U is not circular. The parameters are chosen in this order:

$$\varepsilon \;\longrightarrow\; \text{freeze certificate} \;\longrightarrow\; \varepsilon_0 \;\longrightarrow\; d = d(\varepsilon_0),$$
$$\delta = \frac{\varepsilon_0}{2d},\ \rho_0 = \frac{\varepsilon_0}{2},\ \varepsilon_1 = \varepsilon_0 \;\longrightarrow\; X.$$

The grid $\Theta(\rho_0)$ of Lemma 9.11 is finite once ρ_0 is fixed. Proposition 10.9 needs no tail cutoff: d is fixed before δ, and the paid blocks cost $d\delta = \varepsilon_0/2$.

13. Proof of Theorem 1

Fix $\varepsilon > 0$. Choose $\varepsilon_0 > 0$ with $\frac{11335}{201}\,\varepsilon_0 < \varepsilon/2$ and with folded index at least seven (Section 3.1). This fixes $d = d(\varepsilon_0)$, then δ, ρ_0 and $\varepsilon_1 = \varepsilon_0$ as above. The factors $8^{\omega(M)}$, $(2j)^{\omega(M)}$ and $\mathrm{div}(N)^{O_d(1)}$ are $Y^{o(1)}$ for fixed d (Lemmas 4.2, 4.3, 10.4); they need no budget. Dyadic constants and the count of boxes are inside (2.3).

Let $\mu \le 1$ and $Y \le X$. If $\mu \le 0$, then $N^*_\mu(Y) = 0$, as $\mathrm{rad}(abc) \ge 1 \ge c^\mu$. Let $0 < \mu \le 1$. If $Y < Y_0(\varepsilon_0, d)$, then $N^*_\mu(Y) \le Y^3 \ll_{\varepsilon_0,d} 1$. If $Y \ge Y_0$, then for a

nonempty box Lemma 12.2 raises every row and arm of $\mathcal{S}$ by at most $\rho \le 19\varepsilon_0$. So the stability and reduction losses are at most

$$19\Lambda_U\varepsilon_0 + \varepsilon_0 = \frac{11335}{201}\,\varepsilon_0 < \frac{\varepsilon}{2}.$$

Thus Theorem 2 and Lemma 12.1 give

$$\mathcal{B}_d \le Y^{20/37+\frac{11134}{201}\,\varepsilon_0}. \tag{13.1}$$

By (2.3) at scale Y, at a further cost Y^{ε_0}, $N_\mu^*(Y) \ll_\varepsilon Y^{20/37+\varepsilon/2}$. The constant depends only on ε. Finally (2.1) with $\lambda = 1$ absorbs $(\log X)^2$ and the maxima into the remaining $\varepsilon/2$. □

Appendix A. BBLT estimates in the half-open convention

We prove the pair, Fourier and geometry bounds of [2, Propositions 2.3, 3.1 and 4.1] for the boxes (2.2). The reduction [2, Proposition 2.1] is rerun in Section 2. Work at scale X with exponent λ, in a box satisfying (2.4). Windows are $\mathcal{I}(S) = [S, 2S) \cap \mathbb{N}$ with $S \ge 1$ a power of two, so $\#\mathcal{I}(S) = S$ and $\mathcal{I}(1) = \{1\}$. Roots equal to 1 are allowed. Put

$$A = \prod_{i\le d} A_i, \qquad B = \prod_{i\le d} B_i, \qquad C = \prod_{i\le d} C_i,$$

so $ABC = X^L$. For a side s with roots $\mathfrak{s}_i \in \mathcal{I}(S_{s,i})$ put $N_s = \prod_{i\le d} \mathfrak{s}_i^i$, so the side value is $n_{s,0}N_s$. Since $\mathfrak{s}_i < 2S_{s,i}$ and $\prod_i S_{s,i}^i \le X$,

$$1 \le N_s < 2^{h_d} X. \tag{A.1}$$

Put

$$\Delta = \max_{1\le N<2^{h_d}X} \operatorname{div}(N)^d.$$

By the maximal order of div, $\Delta = X^{O_d(1/\log\log X)}$ for $X \ge 3$. So $\Delta \ll_{d,\delta'} X^{\delta'}$ for every fixed $\delta' > 0$. By Lemma 4.3, a product $\prod_{i\in I} \mathfrak{s}_i^i < 2^{h_d}X$ with $I \subseteq [d]$ determines the roots $(\mathfrak{s}_i)_{i\in I}$ up to Δ choices. The constants below depend only on d and ε_0. They do not depend on λ, the coefficients or the box.

Lemma A.1. *Let $j \ge 2$ and $m \in \mathbb{Z} \setminus \{0\}$. Then*

$$\#\{(x,y) \in \mathbb{N}^2 : x^j - y^j = m\} \le 2(j-1)\operatorname{div}(|m|).$$

Proof. Put $t = x - y$. Then $t \ne 0$, and $t \mid m$ since $x^j - y^j = t\sum_{i<j} x^{j-1-i}y^i$. So t takes at most $2\operatorname{div}(|m|)$ values. For fixed t, $x^j - (x-t)^j$ is a polynomial in x of degree $j-1 \ge 1$ with leading coefficient $jt \ne 0$. So it equals m for at most $j-1$ values of x, and $y = x - t$. □

Lemma A.2 (pair bound)**.** $\mathcal{B}_d \le \Delta \min(AB, AC, BC)$.

Proof. Fix the a- and b-roots: exactly AB choices. The equation in (2.2) fixes c_0N_c, hence N_c. By (A.1), the c-roots take at most Δ values. The pairs (a,c) and (b,c) are the same, since $b_0N_b = c_0N_c - a_0N_a$ and $a_0N_a = c_0N_c - b_0N_b$. □

Lemma A.3 (Fourier bound)**.** *Let $2 \le j,k,\ell \le d$ and put*

$$\Pi_F = \prod_{j\mid i} A_i \prod_{k\mid i} B_i \prod_{\ell\mid i} C_i,$$

the products over $i \le d$. Then

$$\mathcal{B}_d \le (3d)^{1/2}\Delta^{5/2}\,\frac{(ABC)^{2/3}}{\Pi_F^{1/6}} \ll_{\varepsilon_0,d} X^{3\varepsilon_0}\,\frac{(ABC)^{2/3}}{\Pi_F^{1/6}}.$$

Proof. Orthogonality. Write $e(t) = e^{2\pi i t}$. For a side s put

$$\Sigma_s(\alpha) = \sum e(\alpha\, n_{s,0} N_s) \qquad (\alpha \in \mathbb{R}),$$

the sum over all root tuples of s in the windows of the box. The integral

$$\int_0^1 \Sigma_a(\alpha)\Sigma_b(\alpha)\overline{\Sigma_c(\alpha)}\,d\alpha$$

counts the root tuples with $a_0N_a + b_0N_b = c_0N_c$. Dropping the gcd condition, this is at least $\mathcal{B}_d$, and at most $\int_0^1 |\Sigma_a\Sigma_b\Sigma_c|$. By Hölder with exponents $3,3,3$ and Cauchy–Schwarz,

$$\mathcal{B}_d \le \prod_{s=a,b,c}\Big(\int_0^1 |\Sigma_s|^3\Big)^{1/3}, \qquad \int_0^1 |\Sigma_s|^3 \le \Big(\int_0^1 |\Sigma_s|^2\Big)^{1/2}\Big(\int_0^1 |\Sigma_s|^4\Big)^{1/2}. \tag{A.2}$$

We treat side a with j. Sides b and c, with k and ℓ, are the same. Write $\mathbf{a} = (\mathfrak{a}_i)_{i\le d}$ and $N(\mathbf{a}) = N_a$. As $a_0 \ge 1$, $\int_0^1 e(\alpha a_0 m)\,d\alpha = \mathbf{1}_{m=0}$ for $m \in \mathbb{Z}$.

Second moment. $\int_0^1 |\Sigma_a|^2$ counts pairs $(\mathbf{a},\mathbf{a}')$ with $N(\mathbf{a}) = N(\mathbf{a}')$. Choose $\mathbf{a}$ in A ways; then $\mathbf{a}'$ takes at most Δ values. So

$$\int_0^1 |\Sigma_a|^2 \le A\Delta.$$

Fourth moment. Let $J = \{i \le d : j \mid i\}$, so $j \in J$. Split $\mathbf{a} = (\mathbf{a}^\circ, \mathbf{a}^\bullet)$ into the roots with $i \notin J$ and $i \in J$, and put

$$u(\mathbf{a}^\circ) = \prod_{i\notin J}\mathfrak{a}_i^i, \qquad W(\mathbf{a}^\bullet) = \prod_{i\in J}\mathfrak{a}_i^i.$$

The tuple $\mathbf{a}^\circ$ runs over exactly $A^\circ = \prod_{i\notin J} A_i = A/\prod_{j\mid i} A_i$ values. Cauchy–Schwarz over $\mathbf{a}^\circ$ gives

$$|\Sigma_a(\alpha)|^2 \le A^\circ\,\mathcal{T}(\alpha), \qquad \mathcal{T}(\alpha) = \sum_{\mathbf{a}^\circ}\sum_{\mathbf{a}^\bullet,\mathbf{a}'^\bullet} e\big(\alpha a_0\, u(\mathbf{a}^\circ)(W(\mathbf{a}^\bullet) - W(\mathbf{a}'^\bullet))\big) \ge 0.$$

Expand $|\Sigma_a|^2$ over pairs $(\mathbf{a}'',\mathbf{a}''')$ and integrate:

$$\int_0^1 |\Sigma_a|^4 \le A^\circ \int_0^1 \mathcal{T}|\Sigma_a|^2 = A^\circ\,\mathcal{N},$$

Here $\mathcal{N}$ counts the tuples $(\mathbf{a}^\circ,\mathbf{a}^\bullet,\mathbf{a}'^\bullet,\mathbf{a}'',\mathbf{a}''')$ with

$$u(\mathbf{a}^\circ)\big(W(\mathbf{a}^\bullet) - W(\mathbf{a}'^\bullet)\big) = N(\mathbf{a}''') - N(\mathbf{a}''). \tag{A.3}$$

Zero case. If the right side of (A.3) is 0, then $W(\mathbf{a}^\bullet) = W(\mathbf{a}'^\bullet)$. Choose $(\mathbf{a}^\circ,\mathbf{a}^\bullet)$ and $\mathbf{a}''$ in A^2 ways. Then $\mathbf{a}'^\bullet$ and $\mathbf{a}'''$ take at most Δ values each. This gives at most $A^2\Delta^2$ tuples.

Nonzero case. Choose $\mathbf{a}'',\mathbf{a}'''$ in A^2 ways, with right side $m_0 \ne 0$. By (A.1), $|m_0| < 2^{h_d}X$. Each $\mathfrak{a}_i$ with $i \notin J$ divides m_0, so $\mathbf{a}^\circ$ takes at most $\operatorname{div}(|m_0|)^d \le \Delta$ values. Then $m = m_0/u(\mathbf{a}^\circ) \ne 0$ is fixed, and $|m| < 2^{h_d}X$. As $j \mid i$ for $i \in J$,

$$W(\mathbf{a}^\bullet) = x^j, \quad W(\mathbf{a}'^\bullet) = y^j, \qquad x = \prod_{i\in J}\mathfrak{a}_i^{i/j}, \quad y = \prod_{i\in J}\mathfrak{a}_i'^{\,i/j},$$

with $x, y \in \mathbb{N}$ and $x^j - y^j = m$. Lemma A.1 gives at most $2(j-1)\operatorname{div}(|m|) \le 2d\Delta$ pairs (x, y). Since $x \le x^j < 2^{h_d} X$ and $y \le y^j < 2^{h_d} X$, Lemma 4.3 recovers $\mathbf{a}^\bullet$ from x and $\mathbf{a}'^\bullet$ from y, with at most Δ values each. This gives at most $2dA^2\Delta^4$ tuples.

Hence $\mathcal{N} \le 3dA^2\Delta^4$ and

$$\int_0^1 |\Sigma_a|^4 \le 3d\,\Delta^4\,\frac{A^3}{\prod_{j|i} A_i}.$$

Combination. By (A.2),

$$\int_0^1 |\Sigma_a|^3 \le (3d)^{1/2}\Delta^{5/2}\,\frac{A^2}{\left(\prod_{j|i} A_i\right)^{1/2}}.$$

Multiply the three sides and take the cube root. Finally $\Delta^{5/2} \ll_{\varepsilon_0,d} X^{3\varepsilon_0}$. □

Take $\log_X$, multiply by 6, keep only $i \le 6$ and choose $j, k, \ell \in \{2, 3, 5\}$. Since all coordinates are nonnegative, this gives the 27 rows of (2.12), each raised by $18\varepsilon_0 + O_{\varepsilon_0,d}(1/\log X)$.

For the geometry bound we import the following lattice-point count, in the form used in the proof of [2, Proposition 4.1].

Theorem C ([7, Lemma 3])**.** *Let a', b', c' be nonzero integers with $\gcd(a', b', c') = 1$, and let $H_a, H_b, H_c \ge 1$. The number of $(x, y, z) \in \mathbb{Z}^3$ with $\gcd(x, y, z) = 1$, $a'x + b'y = c'z$ and $|x| \le H_a$, $|y| \le H_b$, $|z| \le H_c$ is*

$$\ll 1 + \frac{H_a H_b H_c}{\max\{|a'|H_a, |b'|H_b, |c'|H_c\}},$$

with an absolute implied constant C_{HB}.

Lemma A.4 (geometry bound)**.** *Let $I, I', I'' \subseteq [d]$ and put*

$$\Pi_1 = \prod_{i\in I} A_i \prod_{i\in I'} B_i \prod_{i\in I''} C_i, \qquad \Pi_2 = \prod_{i\in I} A_i^{i-1} \prod_{i\in I'} B_i^{i-1} \prod_{i\in I''} C_i^{i-1}.$$

Then

$$\mathcal{B}_d \le C_{\mathrm{HB}}\,\Delta^3\Big(\frac{ABC}{\Pi_1} + 2^{3h_d} X^{-1+\varepsilon_0/2}\,ABC\,\Pi_2\Big).$$

Proof. Variables. For a tuple counted by $\mathcal{B}_d$ put

$$a' = a_0 \prod_{i\notin I} \mathfrak{a}_i^i, \quad b' = b_0 \prod_{i\notin I'} \mathfrak{b}_i^i, \quad c' = c_0 \prod_{i\notin I''} \mathfrak{c}_i^i,$$
$$x = \prod_{i\in I} \mathfrak{a}_i^i, \qquad y = \prod_{i\in I'} \mathfrak{b}_i^i, \qquad z = \prod_{i\in I''} \mathfrak{c}_i^i.$$

Then $a'x + b'y = c'z$ and $a', b', c' \ge 1$. The integers a', b', c' divide the three side values, and so do x, y, z. The side values are pairwise coprime by Lemma 2.1. So $\gcd(a', b', c') = 1$ and $\gcd(x, y, z) = 1$.

Heights. Put

$$H_a = 2^{h_d} \prod_{i\in I} A_i^i, \qquad H_b = 2^{h_d} \prod_{i\in I'} B_i^i, \qquad H_c = 2^{h_d} \prod_{i\in I''} C_i^i.$$

These are at least 1. Since $\mathfrak{a}_i < 2A_i$, $0 < x < H_a$; likewise $y < H_b$ and $z < H_c$. As $c_0 \ge 1$ and $\mathfrak{c}_i \ge C_i$,

$$c'H_c \ge \prod_{i\notin I''} C_i^i \prod_{i\in I''} C_i^i = \prod_{i\le d} C_i^i \ge X^{1-\varepsilon_0/2}$$

by (2.4).

Count. Fix the complementary roots $\mathfrak{a}_i$ ($i \notin I$), $\mathfrak{b}_i$ ($i \notin I'$) and $\mathfrak{c}_i$ ($i \notin I''$): exactly ABC/Π_1 choices. They fix a', b', c'. By Theorem C, the number of (x, y, z) is at most

$$C_{\mathrm{HB}}\Big(1 + \frac{H_a H_b H_c}{c' H_c}\Big) \le C_{\mathrm{HB}}\Big(1 + 2^{3h_d} X^{-1+\varepsilon_0/2} \prod_{i\in I} A_i^i \prod_{i\in I'} B_i^i \prod_{i\in I''} C_i^i\Big).$$

Each of x, y, z is less than $2^{h_d} X$. So it fixes its selected roots up to Δ values. Multiply, and use

$$\frac{ABC}{\Pi_1} \prod_{i\in I} A_i^i \prod_{i\in I'} B_i^i \prod_{i\in I''} C_i^i = ABC\,\Pi_2. \qquad \square$$

Corollary A.5. *For $I, I', I'' \subseteq [d]$,*

$$\mathcal{B}_d \ll_{\varepsilon_0,d} \frac{X^{\lambda+4\varepsilon_0}}{\Pi_1} + X^{\lambda-1+6\varepsilon_0}\,\Pi_2.$$

Proof. By (2.4), $ABC \le X^{\lambda+3\varepsilon_0/4}$, and $\Delta^3 \ll_{\varepsilon_0,d} X^{\varepsilon_0/4}$. Lemma A.4 gives

$$\mathcal{B}_d \ll_{\varepsilon_0,d} \frac{X^{\lambda+\varepsilon_0}}{\Pi_1} + X^{\lambda-1+3\varepsilon_0/2}\,\Pi_2,$$

which is stronger, as $X \ge 1$. $\square$

This is [2, Proposition 4.1] in our convention, with the same exponents. Lemmas A.2–A.4 use the windows, (2.2), $n_{s,0} \ge 1$ and the λ-free constraints of (2.4). Corollary A.5 also uses $ABC \le X^{\lambda+3\varepsilon_0/4}$. At scale Y with $\lambda := \mu$ they give the entries of Table 12.1 for (2.11), (2.12) and (G1)–(G13).

Appendix B. The thirteen min-disjunctions

We work at scale X with exponent λ; Lemma 12.2 uses the same derivation at scale Y with μ. Put $p_i = a_i + b_i + c_i$, $L = a + b + c$. Each row is Corollary A.5 for one triple $I, I', I'' \subseteq [6]$. A sum of two terms is at most twice the larger, so

$$D \le \max(\lambda + 4\varepsilon_0 - P, \lambda + 6\varepsilon_0 - Q) + O_{\varepsilon_0,d}(1/\log X),$$

where $P = \sum_{i\in I} a_i + \sum_{i\in I'} b_i + \sum_{i\in I''} c_i$ and $Q = 1 - \sum_{i\in I}(i-1)a_i - \sum_{i\in I'}(i-1)b_i - \sum_{i\in I''}(i-1)c_i$. With $C_{\varepsilon_0,d}$ the constant of Corollary A.5, the constant and the factor 2 cost $\log(2C_{\varepsilon_0,d})/\log X = O_{\varepsilon_0,d}(1/\log X)$. By the lower bound in (2.4) and (2.5),

$$2^{-O_d(1)} X^{\lambda} \le \prod_{j\le d} A_j B_j C_j = X^L, \qquad \lambda \le L + O_{\varepsilon_0,d}(1/\log X).$$

Hence $\min(P, Q) \le L - D + 6\varepsilon_0 + O_{\varepsilon_0,d}(1/\log X)$. The certificate uses the limiting form below, free of ε_0; the slack $6\varepsilon_0 + O_{\varepsilon_0,d}(1/\log X)$ is charged in Lemma 12.2 and Table 12.1. The choices, from the proof of [2, Theorem 1.3]:

row 1 :	$I = I' = I'' = \{1, 2, 4\}$;
rows 2–4 :	$I = I' = \{1, 2\},\ I'' = \{1, 2, 3\}$ and permutations;
rows 5–7 :	$I = \{1, 2\},\ I' = I'' = \{1, 2, 3\}$ and permutations;
rows 8–10 :	$I = I' = \{1, 2\},\ I'' = \{1, 3\}$ and permutations;
rows 11–13 :	$I = \{1, 2\},\ I' = I'' = \{1, 3\}$ and permutations.

Written out:

(G1)	$P_1 = p_1 + p_2 + p_4,$	$Q_1 = 1 - p_2 - 3p_4$
(G2)	$P_2 = p_1 + p_2 + a_3,$	$Q_2 = 1 - p_2 - 2a_3$
(G3)	$P_3 = p_1 + p_2 + b_3,$	$Q_3 = 1 - p_2 - 2b_3$
(G4)	$P_4 = p_1 + p_2 + c_3,$	$Q_4 = 1 - p_2 - 2c_3$
(G5)	$P_5 = p_1 + p_2 + a_3 + b_3,$	$Q_5 = 1 - p_2 - 2a_3 - 2b_3$
(G6)	$P_6 = p_1 + p_2 + b_3 + c_3,$	$Q_6 = 1 - p_2 - 2b_3 - 2c_3$
(G7)	$P_7 = p_1 + p_2 + c_3 + a_3,$	$Q_7 = 1 - p_2 - 2c_3 - 2a_3$
(G8)	$P_8 = p_1 + a_3 + b_2 + c_2,$	$Q_8 = 1 - 2a_3 - b_2 - c_2$
(G9)	$P_9 = p_1 + b_3 + a_2 + c_2,$	$Q_9 = 1 - 2b_3 - a_2 - c_2$
(G10)	$P_{10} = p_1 + c_3 + a_2 + b_2,$	$Q_{10} = 1 - 2c_3 - a_2 - b_2$
(G11)	$P_{11} = p_1 + a_2 + b_3 + c_3,$	$Q_{11} = 1 - a_2 - 2b_3 - 2c_3$
(G12)	$P_{12} = p_1 + b_2 + a_3 + c_3,$	$Q_{12} = 1 - b_2 - 2a_3 - 2c_3$
(G13)	$P_{13} = p_1 + c_2 + a_3 + b_3,$	$Q_{13} = 1 - c_2 - 2a_3 - 2b_3$

and each row is used as the disjunction $D \le L - P_j$ or $D \le L - Q_j$.

Appendix C. Computer checks

The paper comes with external files. They are the certificate report of Theorem 2 and the checking programs of Table C.2. The rows, witness (11.7), and verification procedures are specified in the text. All arithmetic is exact. No checking program imports a numerical package or an LP solver.

C.1. **The report.** The file `final-report.raw.json.xz` decompresses to the report. `normalize_completed_report.py` recomputes its derived trie statistics; on this report its output equals its input byte for byte. The report is one JSON object with fields `target` (`"20/37"`), `system`, `search_flags`, `complete`, `stats`, `certificates`, `survivors`, `open_stack` and `elapsed_s`. The lists `survivors` and `open_stack` are empty. Each certificate has exactly four fields.

- `kind`: always `"upper"`.
- `path`: the list of arm labels from the root to the leaf.
- `terms`: a list of `[row-label,"p/q"]`, multipliers positive.
- `rhs`: the value $\sum_i \eta_i b_i$.

The paths form the trie of Theorem 2. A label names one row or arm of $\mathcal{S}$ (Table C.1). The verifier rebuilds each row from its label and reads no stored coefficient vector. The metadata string `system` also contains the label `DET`. It names a row family outside $\mathcal{S}$. The verifier builds no row from it, and no path or multiplier in this certificate uses such a row.

program	what it checks
`verify_tree_report_clean.py`	Standard library only. Strict JSON, duplicate keys rejected; target, system string and flags. At each leaf: every label well formed and in $\mathcal{S}$; every term a linear row, a row $-x_k \le 0$, or an arm on the path; (11.4) exactly, that is $\sum_i \eta_i g_i = e_D$ and $\sum_i \eta_i b_i \le 20/37$; the declared `rhs`. The trie: paths distinct and prefix-free; the children of each internal node are exactly the arms of one clause, (6.5) included at any depth. It recomputes Tables 11.2 and 11.3 and Λ_U. It rejects 46 corrupted reports, among them a missing arm, a missing (6.5) arm, a tampered multiplier, a row outside its path, a forbidden POW3(a) descriptor and a prefix leaf.
`verify_tree_report.py`	a second replay of (11.4) and of the node counts
`verify_witness_clean.py`	x^* against every clause of $\mathcal{S}$ (Table 11.4); it rejects 19 corrupted constructors
`audit_clause_compiler.py`, `compiler_differential_used.py`	every row used by the certificate, and every POW3 and grouped descriptor, rebuilt by the search program's compiler and compared with the verifier's row

The driver runs these programs and writes their output:

`run_verification.sh` $\longrightarrow$ `FROZEN_VERIFICATION.stdout`.

Soundness uses the displayed row definitions and the label map in Table C.1. It also uses the exact Farkas identities at every leaf and the admissibility and trie checks of the first program. The compiler differential also compares the verifier's row builder with the search compiler. The coefficient formulas and derivations in Sections 2–B identify those rows with the system $\mathcal{S}$.

Table C.1 gives the labels. Here $s \in \{a, b, c\}$; σ is the modulus or powered side; (y, z) is as in Section 5. A set $T \subseteq \{1, \dots, 6, \text{tail}\}$ is written as the integer $\sum_{t \in T} 2^{t-1}$, with the tail counted as $t = 7$. Free sets R_y, R_z are written likewise, in $[1, 63]$ or 0. Slots are written `a1`, …, `c6`.

TABLE C.1. Verifier labels and their sources.

verifier label	row or arm
`L`	(2.8)
`roots<=s`, `rad-s`	(2.9), (2.10)
`tail7-s`, `val-s`	$v_s \geq 7\tau_s$, $\sum_{i\leq 6} is_i + v_s \leq 1$ of (3.1)
`pair-xy`	(2.11)
`fourier-s-j`, $j = 0, 1, 2$; `fourier-sum`	the rows $f_s \geq s_2 + s_4 + s_6$, $s_3 + s_6$, s_5; the last row of (11.2)
`HB3`	(7.1)
`ARCH:a<=c`, `ARCH:b<=c`	(6.4)
`ARCH:max-a`, `ARCH:max-b`	the arms of (6.5)
`G0`; `G1-s`; `G2-st`; `G3-s`; `G4-s`;	(G1); (G2)–(G4); (G5)–(G7), $st = ab, bc, ca$;
suffix `:0`, `:1`	(G8)–(G10); (G11)–(G13); the P arm, the Q arm
`SP:e:y:z:k:0`, `:1`	The field k equals the spacing exponent ℓ; the two arms of (8.5)
`UN:`σ`:`R_y`:`R_z`:`T`:00`, `:10`	$D \leq \mathsf{A}_{\mathrm{cut}}$, $D \leq \mathsf{A}_{\mathrm{cut}} + \mathsf{B}_{\mathrm{cut}}$ of (11.3)
`CS4:`σ`:`T`:`$\mathcal{H}$`:W`, `:h2`	the two arms of (10.6); T is the integer mask above, and $\mathcal{H}$ is the four comma-separated, lexicographically sorted held slots
`PS:`σ`:`T`:half`, `:2W3`	the two arms of (10.7)
`POW3`σ`:`J`:S`, `:avg`	$D \leq E_{\mathfrak{D}}$, $D \leq \frac{1}{2}(E_{\mathfrak{D}} + R_\sigma)$ of (9.23)
`GROUP12c:...`	the three arms of (9.24); after `c1c2sq+` come three
`GROUP12a:c1c2sq+...`	canonical singleton slots separated by `+`
`GROUP12b:c1c2sq+...`	
suffix `:S`, `:avg`, `:gate`	
`GROUP1212a:b1b2sq+c1c2sq+...`	the four arms of (9.25); after the two fixed squared
`GROUP1212b:a1a2sq+c1c2sq+...`	groups come two canonical singleton slots
suffix `:S`, `:avg`, `:gate-`s	separated by `+`
`nonneg:x`	$-x \leq 0$

TABLE C.2. SHA-256 of the files this paper depends on.

file	SHA-256
`MANIFEST.sha256` (20/37 package)	`7ba2202c473e0204baf7752a8fd41923`
	`82111ca4cd189a6db584e3912a3bcf43`
`final-report.raw.json.xz`	`f0412ad682389d463d410b96737144e6`
	`65afba13ef26c29f64c7a13f128e24e0`
report (decompressed, normalized)	`9cf43afd90bb683897290c18a9ebfb58`
	`697d0baafe8c9d2c6ae6ff71e8f5e2f7`
`normalize_completed_report.py`	`f38667a2fe45bda186c0ef0ae827f11c`
	`8c68cfac0976da043f7eba59bbd9c701`
`verify_tree_report_clean.py`	`9c301c46a2561e2d3c7c27a2c258186d`
	`66703d89a52f86d74c2f1e6604ad2d0d`
`verify_tree_report.py`	`d7abb356e4098127e775c4f003ef4bd8`
	`2660cbd734547154ab5f8b3f1b394f4a`
`verify_witness_clean.py`	`b795b735b3ec81177b57f6402b746d26`
	`2b5fae0a102eadc5f6b07777b9944cf3`
`audit_clause_compiler.py`	`ea40e6d7cbac17b5a2662b31e4d2b96a`
	`2ee3a1805ae137892d947311d15df929`
`compiler_differential_used.py`	`39ece2ea82da2cd5e221624707de6f0b`
	`4d5e7cd18a6599b3e53f02452f9072e3`
`run_verification.sh`	`dacd0fe7868341f22c4ed5b94a284492`
	`df3c8c45dc4f9da578800ba8b0db215b`
`FROZEN_VERIFICATION.stdout`	`3c7494813ddb89721817b77f48bdac05`
	`5f9bef2f298b3ca7291799e4565df947`

Statements and declarations

Competing interests. The author has no competing interests.

Funding. No funding was received for this work.

Data availability. The certificates, the checking programs of Appendix C and their outputs accompany this paper. Their SHA-256 values are in Table C.2.

References

[1] C. Bernert, *The exceptional set in the abc conjecture*, preprint (2025), arXiv:2506.13364v1.

[2] C. Bernert, T. Browning, J. D. Lichtman, and J. Teräväinen, *Bounds on the exceptional set in the abc conjecture*, to appear in C. R. Math.; arXiv:2410.12234v2, revised 9 May 2026.

[3] T. Browning, J. D. Lichtman, and J. Teräväinen, *Bounds on the exceptional set in the abc conjecture*, preprint (2024), arXiv:2410.12234v1; earlier version of [2].

[4] Todd Cochrane and Sanying Shi, *The congruence* $x_1x_2 \equiv x_3x_4 \pmod m$ *and mean values of character sums*, J. Number Theory **130** (2010), no. 3, 767–785, https://doi.org/10.1016/j.jnt.2009.08.006.

[5] N. G. de Bruijn, *On the number of integers* $\leq x$ *whose prime factors divide* n, Illinois J. Math. **6** (1962), 137–141, https://doi.org/10.1215/ijm/1255631814.

[6] O. Gorodetsky, K. Matomäki, M. Radziwiłł, and B. Rodgers, *On the variance of squarefree integers in short intervals and arithmetic progressions*, Geom. Funct. Anal. **31** (2021), 111–149, https://doi.org/10.1007/s00039-021-00557-5.

[7] D. R. Heath-Brown, *Diophantine approximation with square-free numbers*, Math. Z. **187** (1984), 335–344, https://doi.org/10.1007/BF01161951.

[8] D. R. Heath-Brown, *Counting square-full solutions to* $x + y = z$, preprint (2026), arXiv:2601.07817v1.

[9] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, 2nd ed., Grad. Texts in Math. **84**, Springer, New York, 1990, https://doi.org/10.1007/978-1-4757-2103-4.

[10] D. M. Kane, *On the number of ABC solutions with restricted radical sizes*, J. Number Theory **154** (2015), 32–43, https://doi.org/10.1016/j.jnt.2014.09.021.

[11] R. Li, *On the exceptional set in the abc conjecture*, preprint (2025), arXiv:2507.02885v1.

Independent Researcher, Columbia, Maryland, USA
Email address: ryzfsu@gmail.com