

Local freedom and capacity barriers in quadratic trace reconstruction

Brice Pouly

With AI assistance from GPT-6 Astra

Abstract

A completely multiplicative sign function is determined by its values on $n^2 + 1$, $n^2 + 2$, and $n^2 - 2$, but exact determination does not quantify how many readings detect a negative prime sign. We distinguish three losses of information: partial compatibility tests, geometric restrictions on certificates, and fractional relaxation of signed constraints. After fixing a prime head, we describe the exact fibre of a window and the parity constraints joining two windows. For any fixed head and any sequence $H_N = N^{o(1)}$, one table with $o(N)$ negative entries passes every H_N -window test and every two-reading test. A separate finite table passes these tests without any global source. We bound certificate capacity—fractional packing under unit reading loads—for narrow and binary certificates and for low-degree transport libraries whose links cancel odd prime valuations in pairs. A fixed algebraic curve of certificates for a target prime p has at most logarithmic capacity, or capacity at most one when a reading is constant; in the infinite unanchored case its common poles have field $\mathbb{Q}(\sqrt{p})$. Conversely, selected values of $n^2 + 1$ can force linearly many errors while the capacity of all certificates stays bounded. Two internally disjoint pair families compose without loss on their existing readings, whereas sixteen actual values exhibit $\text{Pack} = 3 < \text{Cap} = 4 < \mu = 5$. The selected-sample constructions do not give an upper bound for the minimum on a complete prefix.

Contents

1	What exact observations fail to quantify	2
2	Two counting estimates with moving square classes	6
3	The exact freedom of one window, and the cost of joining two	10
4	One low-weight table passing all the partial tests	13
5	Geometric restrictions on positive certificates	15
6	A fixed algebraic curve has at most logarithmic capacity	20
7	Moving transport libraries: diversity matters more than height	23
8	Capacity can miss most of the forced errors	26
9	Quadratic positivity can retain information that capacity loses	29
10	Two families compose without loss; five need not	31
11	What a quantitative reconstruction argument must still supply	34
A	Full freedom in logarithmic windows	35
B	Every finite word can occur while measured entropy is zero	37
C	The sixteen-reading arithmetic witness	39

1 What exact observations fail to quantify

The identity

$$(3^2 + 2)(9^2 + 2)(1752^2 + 2) = 2 \cdot 37433^2$$

forces the product of three observed signs to equal the sign at the prime two. Indeed, the readings are 11, 83, and $2 \cdot 11 \cdot 83 \cdot 41^2$. Writing x, y for the first two signs and σ for the prescribed sign at two, their sign triple is $(x, y, \sigma xy)$. Each pair can take all four values while the signs at two, three, five, and seven are held fixed, but for $\sigma = -1$ the triple cannot be all positive. A multiplicative relation is information about a joint assignment, not about its separate projections.

The same distinction persists at a much larger scale. There are tables on all three traces up to N with only $o(N)$ negative entries that pass every short-window test and every pair test, each test admitting a genuine multiplicative explanation. These explanations need not agree on the unobserved primes. A different loss of information occurs when an exact product relation is replaced by the inequality “at least one of these readings is negative”. All such inequalities together can have a fractional packing value much smaller than the number of errors imposed on an actual source.

A third, separate restriction appears when certificates must obey a prescribed geometry: exact identities can be plentiful while reusing too few readings to carry much weight. The paper distinguishes partial compatibility, geometrically restricted capacity, and fractional relaxation. Its contribution is to quantify these losses in the same arithmetic observation system, rather than to introduce new general principles of parity or optimisation.

1.1 Sources, labels, and the target minimum

Let $\mathcal{M}_\pm$ be the completely multiplicative functions $h : \mathbb{N}_{\geq 1} \rightarrow \{-1, 1\}$. Set

$$\mathcal{D} = \{-1, -2, 2\}, \quad Q_d(n) = n^2 - d, \quad I_N = \{(n, d) : 1 \leq n \leq N, d \in \mathcal{D}, Q_d(n) > 0\}. \quad (1.1)$$

A label $i = (n, d)$ denotes the reading $Q_i = Q_d(n)$. Equal integer values at different labels remain different readings; $|I_N| = 3N - 1$. For a prime p , define

$$E_N(h) = \sum_{i \in I_N} \mathbf{1}_{h(Q_i)=-1}, \quad m_p(N) = \min_{h \in \mathcal{M}_\pm, h(p)=-1} E_N(h). \quad (1.2)$$

Only finitely many prime signs affect this minimum. All signs other than the prescribed sign at p are free, and a minimising source may change with N .

A *certificate for p* on a labelled sample $A = (A_i)_{i \in I}$ is a nonempty subset $C \subseteq I$ such that

$$\prod_{i \in C} A_i = pz_C^2, \quad z_C \in \mathbb{N}_{\geq 1}. \quad (1.3)$$

Its signs have product -1 whenever $h(p) = -1$. To add the resulting error inequalities without charging a reading more than once, impose

$$\alpha_C \geq 0, \quad \sum_{C \ni i} \alpha_C \leq 1 \quad (i \in I). \quad (1.4)$$

The maximum of $\sum_C \alpha_C$ is the *capacity* $\text{Cap}_p(A)$: a fractional packing value under unit reading loads. The maximum number of disjoint certificates is $\text{Pack}_p(A)$, and the actual minimum is

$$\mu_p(A) = \min_{h(p)=-1} \sum_{i \in I} \mathbf{1}_{h(A_i)=-1}.$$

The elementary inequalities

$$\text{Pack}_p(A) \leq \text{Cap}_p(A) \leq \mu_p(A) \quad (1.5)$$

are the starting point, not equalities to be assumed. Restrictions on the allowed certificates will always be indicated. On the full sample, $\mu_p((Q_i)_{i \in I_N}) = m_p(N)$.

The minimum number of labels meeting every certificate is exactly $\mu_p(A)$, by Proposition 8.1. Thus an integral cover of all certificates retains the true error minimum; it is the fractional relaxation that can lower its value. The fifteen-reading example in Section 8.4 has capacity five but error minimum seven.

For a positive integer a , $\text{core}(a)$ is its squarefree kernel: $a = \text{core}(a) \text{sq}(a)^2$. Thus $\text{core}(a)$ records *odd* valuations, not every prime divisor. Write $[a]$ for its class in $\mathbb{Q}_{>0}^\times / \mathbb{Q}_{>0}^{\times 2}$, viewed additively as a vector space over $\mathbb{F}_2$. A source is precisely a linear character of this space. All unspecified logarithms are natural, and constants in O or $\ll$ depend only on displayed subscripts. We use $N^{o(1)}$ for a positive quantity whose logarithm is $o(\log N)$, or, in an upper-bound statement, one bounded by $O_\delta(N^\delta)$ for every fixed $\delta > 0$.

The exact injectivity of the three infinite traces has a short explanation. For the quotient of two sources with identical traces, the values 2, 3, and 6 first fix the signs at two and three. For every prime $q \geq 5$, at least one $d \in \mathcal{D}$ is a quadratic residue modulo q . A centred root $1 \leq r \leq (q-1)/2$ gives $Q_d(r) = qm$ with $0 < m < q$. The least prime with a nontrivial quotient sign would then contradict the observed sign at r . This descent does not supply a positive proportion of detecting readings.

1.2 Three main conclusions

The first conclusion concerns the difference between a table and a source. Let S be a fixed finite set of primes with prescribed signs κ . A table passes an H -window test if its restriction to that window is the output of some source agreeing with κ on S . It passes a pair test if the same holds for the specified one or two labels, however far apart they lie.

Theorem 1.1 (Simultaneous partial compatibility). *For fixed S, κ and $H_N = N^{o(1)}$, there is a table $w^{(N)} \in \{-1, 1\}^{I_N}$ with $o(N)$ negative entries that passes every H_N -window test contained in I_N and every pair test. The table is the same for all tests; the witnessing source may depend on the test. An explicit table with $N = 4096$ and $H = 2$ has 252 negative entries, passes every such test with $S = \{2, 3, 5, 7\}$ and $\kappa(2) = -1$, but is not the output of any source.*

The general asymptotic assertion does not assert non-realisability for every table it constructs. The finite assertion establishes that additional phenomenon separately. The proof in Section 4 combines an exact local fibre with a uniform count of pairs in a prescribed square class.

This does not conflict with the complete presentation by relations involving at most $\lfloor \log_2 N \rfloor + 3$ readings in *Arithmetic reconstruction and error recovery from three quadratic traces* [22, Theorem 1.1]. A small support cardinality does not bound the diameter of its indices: those relations may join distant readings and need not be among the window or pair tests above.

The second conclusion concerns the geometry of a positive certificate proof. The width of a certificate is $1 + \max_C n - \min_C n$. Uniformly in p ,

$$\begin{aligned} \text{Cap}_p(\text{width} \leq H) &\ll N^{\frac{\log(2H)}{\log(2N)}}, & 1 \leq H \leq N, \\ \text{Cap}_p(\text{size} \leq 2) &\ll_\epsilon N^{2/3+\epsilon}. \end{aligned} \quad (1.6)$$

A fixed algebraic curve of certificates has capacity $O(\log N)$, with a constant depending on the curve, or capacity at most one if one of its readings is constant. For transport libraries whose total algebraic degree is $N^{o(1)}$, the capacity is again $o(N)$, even when their coefficient heights are unrestricted. Here the library must support prime-by-prime cancellation of odd valuations by pairs of linked readings, as defined in Section 7; arbitrary algebraic proof methods are not covered. These are distinct restrictions: increasing the distance between two readings does not circumvent the binary bound, while using many readings in a subpolynomial window does not circumvent the width bound.

The third conclusion is that these upper bounds on capacity must not be read as upper bounds on forced errors.

Theorem 1.2 (Arithmetic gaps and composition). *For every $M \geq 32$, selected distinct values $A_i = n_i^2 + 1$ can satisfy*

$$\mu_2(A) > M/16, \quad 1 \leq \text{Cap}_2(A) < 16.$$

The indices may be required to exceed any prescribed bound, and any finite compatible prime head may be preserved. A separate sample of sixteen explicit values satisfies

$$\text{Pack}_2(A) = 3, \quad \text{Cap}_2(A) = 4, \quad \mu_2(A) = 5.$$

For two square classes $a + b = [p]$, two internally disjoint families of pairs with respective classes a and b , of sizes M_a, M_b , yield at least $\min(M_a, M_b)$ disjoint certificates for p on their existing labels. The sixteen-value sample shows that the analogous lossless principle fails for five families.

Here M counts selected observations, not their largest index. The arithmetic realisation does not preserve density or give a useful height bound in terms of M .

A positive baseline on the complete prefix. The obstructions below do not mean that a negative prime sign is detected only finitely often. The following elementary consequence of injectivity and Pell multiplication gives a useful reference scale, not an optimal lower bound or a new Pell result.

Proposition 1.3 (Logarithmic disjoint packing). *For every fixed prime p , there is $c_p > 0$ such that, for all sufficiently large N ,*

$$\text{Pack}_p((Q_i)_{i \in I_N}) \geq c_p \log N, \quad m_p(N) \geq c_p \log N.$$

Proof. The class $[p]$ lies in the span of the classes of the three traces. Otherwise a linear functional vanishing on that span but taking value one at $[p]$ would define a nontrivial source with all three traces positive, contradicting the injectivity proved above. Choose an inclusion-minimal finite certificate C_0 for p . Its classes $a_i = \text{core}(Q_i) > 1$ are distinct: two equal classes could be removed without changing the target. The inequality $a_i > 1$ follows because none of the positive readings is a square.

Write $n_i^2 - a_i u_i^2 = d_i$. By Pell's theorem, choose an integral unit $\epsilon_i = x_i + y_i \sqrt{a_i} > 1$ of norm one with $x_i, y_i > 0$ [9, Theorem 2.3 and multiplication of solutions]. Define

$$n_{i,k} + u_{i,k} \sqrt{a_i} = (n_i + u_i \sqrt{a_i}) \epsilon_i^k \quad (k \geq 0).$$

These are positive integer solutions with strictly increasing $n_{i,k}$, and $n_{i,k} = \frac{1}{2}(n_i + u_i \sqrt{a_i}) \epsilon_i^k + O_i(\epsilon_i^{-k})$. Thus the number of terms with $n_{i,k} \leq N$ is $\log N / \log \epsilon_i + O_i(1)$. Take the same initial number of terms in every orbit, namely the minimum of these counts. At each rank, one reading from each orbit gives a certificate for p . The certificates are disjoint: an orbit has no repeated index, and different orbits have different square classes and hence cannot share a label. The fixed certificate and units give $\gg_p \log N$ disjoint certificates, proving both claims. $\square$

For $p = 2$, the singletons generated by $n_k + u_k\sqrt{2} = (1 + \sqrt{2})(3 + 2\sqrt{2})^k$ already give

$$m_2(N) \geq \frac{\log N}{\log(3 + 2\sqrt{2})} - O(1).$$

A stronger lower bound for the same unrestricted minimum is proved in [22, Theorem 1.3]:

$$m_p(N) \geq \Phi_c(K), \quad \Phi_c(K) = \exp\left(\exp\left(c \frac{\log K}{\log \log K}\right)\right), \quad K = \frac{\log N}{\log \max(3, p)},$$

for each fixed $0 < c < \log 2$ and sufficiently large K , with a threshold independent of p . At fixed p , this exceeds every fixed power of $\log N$. The conclusion is a lower bound for $m_p(N)$, not a claim of the same bound for direct target- p packing: its proof amplifies a negative pivot without composing all pivot families into certificates for p . Proposition 1.3 retains a separate role as an elementary, self-contained packing bound. The stronger result is cited for comparison and is not used in the proofs below.

1.3 Which objects the bounds concern

Object	Conclusion	Information not supplied
Complete prefix I_N	Exact local fibres; uniform pair counts; low-weight partially compatible tables	A global source producing those tables
A specified certificate class in I_N	An upper bound on its capacity under unit loads	An upper bound on $m_p(N)$
A fixed algebraic curve	A curve-dependent logarithmic capacity bound	Uniformity over moving curves
Selected values $n_i^2 + 1$	Exact realisation of binary models; gaps between packing, capacity, and errors	A comparison with the full prefix at the same height

In particular, none of the counterexamples constructs a source with $E_N(h) = o(N)$ under $h(p) = -1$. Nor does the paper establish the converse target $m_p(N) \geq c_p N$ for fixed p .

1.4 Arithmetic realisation and its classical inputs

The contributions concern the arithmetic observation system, not new general theories of Pell equations, matroid packing, or semidefinite optimisation. Three lines of prior work explain the distinction.

Square classes and integral points. De la Bretèche–Wang–Xu [5] supply the closest arithmetic comparison. Their Proposition 5.1 gives $O_P(\sqrt{N})$ for off-diagonal square products of two values of one fixed quadratic. The bound here is not an improvement of that exponent: it permits a moving target square class and two different types among the three quadratics. The logarithmic count for a single square class is also classical; their remark after Lemma 3.2 and equation (13) include a refinement uniform in that class. Their Lemma 3.1 credits the quadratic-case argument of Chinis–Shala [8, Lemmas 2.4–2.5 and proof] for small counts of exact ratios. We retain short norm proofs to make the uniformities used here explicit.

We apply Evertse–Silverman [13, Theorem 1(b)] in a fixed biquadratic splitting field, Siegel’s geometric restriction in the formulation of [2], and the coefficient-uniform plane-curve bound [7, Theorem 3]. Selberg’s diagonalisation [16, Chapter 13] and fixed-modulus Mertens estimates [3, Theorem 3.3] supply the sieve. None is a new counting method of this paper.

Packing, parity, and positivity. Minimal certificates are exactly the port of a binary matroid with a distinguished target element; see Cornuéjols [10, author’s July 2000 notes, Section 8.3.1, p. 120]. Section 8 gives the precise dictionary between packing, fractional covering, and the true sign minimum. Two-window repair is a classical minimum T -join problem [12]. The positive matrix bounds in Section 9 are the spectral and semidefinite bounds for graph cuts [11, 14], transferred to errors with explicit reading loads. The negative Pell input for arithmetic realisation is a special case of the classical nonresidue-graph criterion discussed by Lemmermeyer [17, Proposition 5.3]; its direct integral proof is retained in Lemma 8.2.

Prior result or mechanism	Scope retained or added here	Use in the paper
One fixed quadratic, square target: $O_P(\sqrt{N})$ [5, Proposition 5.1]	Mixed trace types and arbitrary target class, with the weaker exponent $2/3 + \varepsilon$	Pair constraints in a common table
Exact-ratio counts [5, 8]	Mixed types; a realised link bounds its reduced coefficients	Necessity of library diversity under unit loads
Binary ports, joins, and positive graph forms [10, 12, 14]	Actual prime assignments and quadratic values, with square factors removed exactly	Arithmetic gaps and repair without hidden sign variables
Siegel and coefficient-uniform curve counts [2, 7]	Target-imposed common poles; loads on fixed curves or on paired transport links	Distinct geometric capacity barriers

What the arithmetic realisations establish. The same low-weight table works for all the specified tests, rather than selecting a different table for each test. The fixed-curve theorem forces the field $\mathbb{Q}(\sqrt{p})$ at the common poles before converting integrality into a load bound. The selected-sample realisation preserves every allowed prime assignment and the entire certificate family. Finally, composing two matchings keeps the existing labels and their height. These are the assertions to distinguish from the classical mechanisms above; they do not claim a general improvement in those mechanisms.

Reading route. Section 2 supplies the two counting estimates used repeatedly. Sections 3–4 explain local freedom and simultaneous partial compatibility. Sections 5–7 quantify geometric restrictions on certificates. Sections 8–10 show what capacity misses and where composition succeeds or fails. The graph examples and rational centres are supporting illustrations, not additional main themes. The appendices retain two complementary distinctions: full rank in logarithmic windows, and a single source with every finite word at positive frequency but zero measured entropy.

2 Two counting estimates with moving square classes

A private prime gives an exact local degree of freedom. Before using that observation, we need to count the readings for which no such prime is available. We also need to count pairs that remain dependent after a prime head is fixed. The two estimates below answer these different questions; neither assumes anything about the signs of a source.

2.1 A square class has only logarithmically many representatives

The logarithmic dependence comes from classical norm equations; compare also [5, remark after Lemma 3.2 and equation (13)]. The proof below isolates an absolute spacing bound sufficient for all our moving square classes. Put $\lambda_0 = (3 + \sqrt{5})/2$, and let $\tau(k)$ denote the number of positive divisors of k .

Lemma 2.1 (Uniform norm count). *If $a \geq 2$ is squarefree, $K \neq 0$ is an integer, and $M > 1$, the number of pairs $X \geq 0, Y \geq 1$ satisfying*

$$X^2 - aY^2 = K, \quad 1 < X + Y\sqrt{a} \leq M$$

is at most $\tau(|K|)(1 + \log M / \log \lambda_0)$. For $a = 1$ and $K \neq 0$, the number is at most $2\tau(|K|)$.

Proof. The principal ideal generated by $\alpha = X + Y\sqrt{a}$ in the full ring of integers of $\mathbb{Q}(\sqrt{a})$ has norm $|K|$. There are at most $\tau(|K|)$ integral ideals of this norm. Indeed, a split prime occurring to exponent e has $e + 1$ possible distributions between its two prime ideals; an inert or ramified prime has at most one. These ideal and norm facts are classical; see [20, Chapters 3–5].

Two positive generators $\alpha_2 > \alpha_1$ of the same ideal and the same signed norm have quotient a unit $u > 1$ of norm one. Its conjugate is $u^{-1} > 0$, so its integral trace is at least three. Hence $u \geq \lambda_0$. The generators of each ideal are multiplicatively separated in $(1, M]$, which proves the count. For $a = 1$, factor $(X - Y)(X + Y) = K$. $\square$

For a squarefree $a \geq 1$, write

$$R_a(N) = \#\{i \in I_N : \text{core}(Q_i) = a\}.$$

No positive $Q_d(n)$ is a square: each lies strictly between the adjacent squares on the relevant side of n^2 . Thus $R_1(N) = 0$. Applying Lemma 2.1 to $n^2 - au^2 = d$ gives the explicit uniform estimate

$$R_a(N) \leq 5 \left(1 + \frac{\log(2N + 1)}{\log \lambda_0} \right). \quad (2.1)$$

The factor five is $\sum_{d \in \mathcal{D}} \tau(|d|)$. No regulator or class number is being bounded uniformly in a .

2.2 All pairs in a prescribed square class

Theorem 2.2 (Uniform pair count). *For every fixed $\varepsilon > 0$, uniformly in $N \geq 2$ and squarefree $a \geq 1$,*

$$T_a(N) := \#\{\{i, j\} \subset I_N : i \neq j, \text{core}(Q_i Q_j) = a\} \ll_{\varepsilon} N^{2/3+\varepsilon}.$$

The diagonal in labels is excluded, but distinct labels of equal integer value are retained.

Proof. We first control large square parts. If $1 \leq U \leq N^{2/3}$, then

$$B_N(U) := \#\{i : \text{sq}(Q_i) > U\} \ll \left(\frac{N}{U} + N^{2/3} \right) \log(2N). \quad (2.2)$$

To see this, put $V = \lceil N^{2/3} \rceil$. For $U < u \leq V$, the condition $u^2 \mid Q_d(n)$ has no solutions if u is even, since the valuation at two is at most one. For odd u , simple roots lift, and there are at most $2^{\omega(u)} \leq \tau(u)$ roots modulo u^2 . Summing the congruence counts gives

$$\sum_{U < u \leq V} \tau(u)(N/u^2 + 1) \ll N \log(2U)/U + V \log(2V).$$

Here $\sum_{u \leq t} \tau(u) \leq t(1 + \log t)$ and a dyadic decomposition suffice. If $\text{sq}(Q_i) > V$, then $\text{core}(Q_i) \ll N^{2/3}$, and (2.1) pays for all these classes. This proves (2.2).

Now choose $U = \lfloor N^{1/3} \rfloor$. Once the square class of one member of a pair is fixed, the other's class is fixed as well: it is $\text{core}(a \text{core}(Q_i))$. By (2.1), a reading has $O(\log(2N))$ partners in this target class. Pairs meeting the large-square-part set therefore contribute

$$O(B_N(U) \log(2N)) \ll N^{2/3} \log^2(2N).$$

For the remaining pairs write

$$n^2 - d = rbu^2, \quad m^2 - e = rcv^2, \quad bc = a,$$

where rb, rc are squarefree, $(b, c) = 1$, and $u, v \leq U$. Eliminating r gives

$$X^2 - aY^2 = K, \quad X = bum, \quad Y = vn, \quad K = b^2eu^2 - adv^2. \quad (2.3)$$

There are at most $\tau(a)$ choices of (b, c) . If $a > 1$, $K = 0$ admits no positive solution. If $a = 1$ and $K = 0$, then $eu^2 = dv^2$. The distinct same-sign elements of $\mathcal{D}$ have a nonsquare ratio, so $d = e$, $u = v$, and then $n = m$. This is the excluded diagonal.

A represented class satisfies $a \leq (N^2 + 2)^2$. Crude bounds $X + Y\sqrt{a} \leq 6N^6$ and $|K| \leq 40N^{10}$ now suffice. For every fixed $\eta > 0$, $\tau(k) \ll_\eta k^\eta$: for large primes q , $e + 1 \leq 2^e \leq q^{\eta e}$, and the remaining finite set of primes contributes a constant. Lemma 2.1, including its factorised case, consequently gives $O_\varepsilon(N^\varepsilon)$ solutions per choice after reducing the auxiliary exponent. Summing over nine choices of d, e , U^2 choices of u, v , and $\tau(a)$ choices of b proves the result. $\square$

The threshold $N^{1/3}$ balances the square-part tail against the two free square factors. It is not an optimality claim for pair counting.

2.3 A sieve for the absence of an odd prime factor

For $Y \geq 2$ and a prime p , let

$$A_d(T; Y, p) = \{1 \leq n \leq T : Q_d(n) > 0, v_q(Q_d(n)) \text{ is even for every } q > Y, q \neq p\}.$$

Let $\mathcal{P}_d^{\text{ex}}$ be the odd primes congruent to $5, 3, 7$ modulo eight when $d = -1, -2, 2$, respectively. Define $A_d^{\text{ex}}(T; Y, p)$ by imposing the same parity condition only for $q \in \mathcal{P}_d^{\text{ex}}$.

Theorem 2.3 (Uniform odd-factor sieve). *Uniformly in $T \geq 3$, $Y \geq 2$, p , and $d \in \mathcal{D}$,*

$$|A_d(T; Y, p)| \ll T \min \left(1, \frac{\log(2Y)}{\log(2T)} \right), \quad (2.4)$$

$$|A_d^{\text{ex}}(T; Y, p)| \ll T \min \left(1, \sqrt{\frac{\log(2Y)}{\log(2T)}} \right). \quad (2.5)$$

For every positive integer M , the number of readings $i \in I_N$ with $\text{core}(Q_i) \mid \text{rad}(pM)$ is at most

$$CN \min \left(1, \frac{\log(2 + \log(2M))}{\log(2N)} \right). \quad (2.6)$$

For a fixed M , the sharper bound $O(2^{\omega(M)} \log(2N))$ also holds, uniformly in p .

Proof. We give the finite sieve and its error term, since its uniformity is consumed later by moving widths and moving rule libraries. Sieve over odd splitting primes for Q_d , or over $\mathcal{P}_d^{\text{ex}}$, in $Y < q \leq z$, omitting p . The forbidden event is $v_q(Q_d(n)) = 1$. Each of the two roots modulo q has $q - 1$ lifts with precisely this valuation, so its density is

$$g(q) = \frac{2(q-1)}{q^2}, \quad \rho(q) = 2(q-1).$$

For squarefree m supported on the sieving primes, set $g(m) = \prod_{q|m} g(q)$ and $\rho(m) = m^2 g(m)$. The Chinese remainder theorem gives

$$\sum_{\substack{n \leq T \\ Q_d(n) > 0}} \prod_{q|m} \mathbf{1}_{v_q(Q_d(n))=1} = Tg(m) + r_m, \quad |r_m| \leq \rho(m).$$

For $m = 1$ the possible missing value $Q_2(1) < 0$ costs at most one. For $m > 1$ it is not in a forbidden class.

Put $t(q) = g(q)/(1 - g(q))$, extend multiplicatively on squarefree integers in this prime set, and define

$$G(z) = \sum_{m \leq z} t(m), \quad \lambda_m = \frac{\mu(m)t(m)}{g(m)G(z)} \sum_{\substack{r \leq z/m \\ (r,m)=1}} t(r) \quad (m \leq z).$$

Set $\lambda_m = 0$ otherwise. The classical Selberg diagonalisation [16, Section 13.2] here reads

$$\lambda_1 = 1, \quad |\lambda_m| \leq 2^{\omega(m)}, \quad \sum_{a,b \leq z} \lambda_a \lambda_b g([a,b]) = G(z)^{-1}. \quad (2.7)$$

For completeness, if $y_r = \sum_{r|m} \lambda_m g(m)$, Möbius inversion gives $y_r = \mu(r)t(r)/G(z)$. The identity $g([a,b]) = g(a)g(b) \sum_{r|(a,b)} 1/t(r)$ transforms the quadratic form into $\sum_r y_r^2/t(r) = 1/G(z)$. Also $t(m)/g(m) = \prod_{q|m} (1 - g(q))^{-1} \leq 2^{\omega(m)}$, which proves the weight bound.

A sifted integer makes the weighted sum exactly one. Squaring and using (2.7) therefore bounds its count by

$$\frac{T}{G(z)} + \sum_{a,b \leq z} |\lambda_a \lambda_b| \rho([a,b]) \leq \frac{T}{G(z)} + z^4(1 + \log z)^6. \quad (2.8)$$

Indeed, $\rho([a,b]) \leq [a,b]2^{\omega([a,b])}$, $[a,b] \leq z^2$, and $\sum_{m \leq z} 4^{\omega(m)} \leq z(1 + \log z)^3$ on squarefree integers. Sifting only valuation one enlarges the exceptional set; higher odd valuations do not invalidate this upper bound.

Let $\theta = 1$ for all splitting primes and $\theta = 1/2$ for the exclusive class. Fixed-modulus Mertens estimates [3, Theorem 3.3] and $g(q) = 2/q + O(q^{-2})$ give, uniformly for $x \geq Y \geq 2$,

$$\prod_{\substack{Y < q \leq x \\ q \text{ in the sieve, } q \neq p}} (1 + t(q)) \asymp \left(\frac{\log x}{\log Y} \right)^\theta, \quad \sum_{q \leq x} g(q) \log q \ll \log(2x). \quad (2.9)$$

The splitting primes have density $1/2$ among primes, and an exclusive class has density $1/4$, always at modulus eight. Removing one prime changes the product by a bounded factor independent of that prime.

Take $x = z^a$ for a sufficiently small fixed $a > 0$. Choose each available prime up to x independently with probability $g(q)$ and let R be their product. Then $\mathbb{E} \log R \leq \frac{1}{4} \log z$, so $\mathbb{P}(R \leq z) \geq 3/4$. The probability of a squarefree product m is $t(m)/\prod(1 + t(q))$. Consequently

$$G(z) \gg (\log z / \log(2Y))^\theta \quad (Y \leq x).$$

If $Y > x$, use $G(z) \geq 1$ and the trivial count. With $z = T^{1/8}$, the error in (2.8) is $O(T^{1/2} \log^6(2T))$, absorbed by both claimed bounds for large T . The bounded range is absorbed in the absolute constant.

For (2.6), take $Y = \max(3, \log(2M))$ and omit also the primes dividing M . The omission beyond Y changes the Euler product by only a bounded factor, since

$$\sum_{\substack{q|M \\ q > Y}} \frac{1}{q} \leq \frac{\log M}{Y \log Y} \ll 1.$$

Repeat the dimension-one argument; if Y is too large, the trivial bound applies. Finally, for fixed M there are at most $2^{\omega(M)+1}$ square classes supported on pM , and (2.1) proves the last assertion. $\square$

The probability space in this proof is only a device for lower-bounding a finite Euler sum. No source signs have been randomised.

3 The exact freedom of one window, and the cost of joining two

An unusually large prime factor is useful only if its valuation is odd and it is not shared by another reading in the experiment. A resultant makes the second condition automatic inside a sufficiently short window. The first condition cannot be discarded.

3.1 Private odd factors and an exact fibre

For an interval of H consecutive indices starting at u , let $W(u, H)$ consist of its positive labelled readings. Set

$$\Delta_H = (H^2 + 4)^2, \quad B_Y(W) = \{i \in W : P^+(\text{core}(Q_i)) \leq Y\},$$

where $P^+(1) = 1$. The complement $G_Y(W) = W \setminus B_Y(W)$ will supply the free coordinates.

Lemma 3.1 (A common divisor pays for the separation). *For distinct typed shifts (t, d) and (s, e) , a common prime divisor of $(u + t)^2 - d$ and $(u + s)^2 - e$ divides the nonzero integer*

$$R_{d,e}(t - s) = (t - s)^4 - 2(d + e)(t - s)^2 + (d - e)^2.$$

Moreover $|R_{d,e}(v)| \leq (v^2 + 4)^2$.

Proof. The displayed integer is the resultant of the two monic quadratics. They are irreducible over $\mathbb{Q}$, and equality of the monic polynomials would force equality of their typed shifts. They are therefore coprime. The resultant vanishes modulo any common prime divisor. The bound follows from $|d|, |e| \leq 2$. $\square$

Theorem 3.2 (Exact window fibre). *Fix all prime signs $\kappa(q)$ for $q \leq Y$, where $Y \geq \Delta_H$. The possible words $w \in \{-1, 1\}^{W(u, H)}$ are exactly those satisfying*

$$w_i = \kappa(\text{core}(Q_i)) \quad (i \in B_Y(W)). \quad (3.1)$$

All other coordinates are jointly free. In particular, the fibre has cardinality $2^{|W| - |B_Y(W)|}$, equal to $2^{3H - |B_Y(W)|}$ when $u \geq 2$.

Proof. A reading in $B_Y(W)$ depends only on the prescribed head, so (3.1) is necessary. Every other reading has an odd prime factor $q > Y$. By Lemma 3.1, this prime divides no other reading in the window, even to an even valuation. Choose one such prime for each free reading. These primes are distinct and can be flipped independently to realise any requested assignment. This also proves the statement for a window containing $n = 1$, with the nonpositive reading omitted. $\square$

The theorem fixes the whole prime head before the word is requested. It is not a statement that a typical source happens to give independent signs. With independent fair signs on the remaining primes, however, its free coordinates do indeed have the uniform joint law, conditionally on the head.

Proposition 3.3 (Optimal repair inside one window). *Let h_0 agree with the fixed head, and let w satisfy (3.1). Let $J = \{i \in G_Y(W) : w_i \neq h_0(Q_i)\}$. For $i \in J$ let q_i^* be the largest prime of odd valuation in Q_i . For every $\sigma > 0$,*

$$\min_{\substack{h|_{q \leq Y} = h_0|_{q \leq Y} \\ h(Q_i) = w_i \quad (i \in W)}} \sum_{q: h(q) \neq h_0(q)} q^{-\sigma} = \sum_{i \in J} (q_i^*)^{-\sigma}.$$

The smallest number of flipped primes is $|J|$. For an arbitrary requested word, the smallest residual Hamming error is its number of mismatches on $B_Y(W)$.

Proof. The sets of odd prime factors above Y belonging to different readings are disjoint. A changed free coordinate requires an odd, hence nonempty, set of flips in its own set. Its cheapest choice is the largest such prime. These choices affect no other reading, so all the individual lower bounds are attained together. Head-determined coordinates cannot be repaired, and every other coordinate can. $\square$

The cost is at most $3H/Y^\sigma$, but a bound on the number of ordinary prime divisors would not prove this statement. For example,

$$1393^2 + 1 = 2 \cdot 985^2 = 2 \cdot 5^2 \cdot 197^2.$$

At $H = 1$ and $Y = 25$, the large prime 197 supplies no freedom: the reading is determined by the sign at two.

3.2 How much of a window is forced?

Corollary 3.4 (Average exceptional fraction). *For $X \geq 3$, $1 \leq H \leq X$, and $Y \geq \Delta_H$,*

$$\frac{1}{X} \sum_{X \leq u < 2X} \frac{|B_Y(W(u, H))|}{H} \ll \min \left(1, \frac{\log(2Y)}{\log(2X)} \right).$$

Thus if $H = X^{o(1)}$ and $\log Y = o(\log X)$, all but $o(X)$ origins have $o(H)$ forced coordinates, in the usual quantitative sense obtained from Markov's inequality.

Proof. Each positive labelled reading with index below $3X$ belongs to at most H of the windows. The count of such readings with no odd prime factor above Y is bounded by (2.4); exempting an extra prime can only enlarge it. Divide the resulting bound by XH . $\square$

For example, $H = \lfloor \exp(\sqrt{\log X}) \rfloor$ and $Y = \Delta_H$ give $|B_Y(W)| \ll H(\log X)^{-1/4}$ outside $O(X(\log X)^{-1/4})$ origins. Every compatible repair on such a window has harmonic cost below $3/H^3$. The source may depend on the origin and the requested word. No simultaneous global assignment follows from this estimate.

3.3 Joining windows introduces parity, even without a cycle

Consider two disjoint H -windows, and fix all prime signs through $Y \geq \Delta_H$. A prime above Y can have odd valuation at most once in each window. Construct a multigraph with the readings as vertices and one additional vertex $*$. A prime of odd valuation in exactly two readings gives an edge between them; a prime occurring oddly in exactly one reading gives an edge from it to $*$. Primes with no odd occurrence are irrelevant. A *closed component* is a connected component not containing $*$; isolated reading vertices count as closed components.

For a closed component C , define $k_C = \text{core}(\prod_{i \in C} Q_i)$. Every prime factor of k_C is at most Y .

Theorem 3.5 (Exact gluing criterion). *A word on the union W of the two windows extends to a source with the fixed head if and only if*

$$\prod_{i \in C} w_i = \kappa(k_C) \quad \text{for every closed component } C. \quad (3.2)$$

If there are c closed components, the fibre has size $2^{|W|-c}$. Its Hamming distance from an arbitrary word is exactly the number of violated equations in (3.2). In particular, deleting one reading from each closed component is necessary and sufficient to leave all remaining coordinates jointly free.

Proof. Relative to a reference assignment of tail signs, flipping a prime toggles the endpoints of its edge, with the coordinate at $*$ discarded. The incidence vectors of a connected graph over $\mathbb{F}_2$ span the even-weight vectors on its vertices. A spanning tree proves this directly by removing leaves. For a component containing $*$, discarding that coordinate leaves the full space on its reading vertices. For a closed component, the only restriction is its total parity. These restrictions are disjoint and yield exactly (3.2).

A violated component needs at least one changed coordinate, and changing one coordinate in each violated component suffices. If no coordinate is deleted from a closed component, its parity restriction persists; deleting one makes its projection unrestricted. $\square$

A component can be a tree and still be closed. Consequently, counting cycles alone does not describe the obstruction to gluing.

Example 3.6 (Two free triples that do not glue freely). Take the windows $n = 9$ and $n = 175$, each of width one, and $Y = 25$. Their readings are

$$(82, 83, 79), \quad (30626, 30627, 30623),$$

with $30626 = 2 \cdot 15313$, $30627 = 3^2 \cdot 41 \cdot 83$, and $30623 = 113 \cdot 271$. Each triple is free after the head is fixed. In the union, however, the vertices 82, 30627, 83 form a closed path with edge primes 41, 83. Its relation is

$$82 \cdot 30627 \cdot 83 = 2 \cdot 10209^2.$$

When $\kappa(2) = -1$, at least one of these three readings is negative. The full six-reading fibre has size 32, although every pair projection is free. Flipping the signs at 82 and 30627 relative to a compatible word costs exactly $1/41$ in harmonic distance; flipping only the first is incompatible with the same head.

The numerical assertions in this example are checked by the accompanying verifier. Their explanation is the closed-path parity, not the computation.

3.4 The exact weighted repair problem

The optimisation mechanism is the classical minimum T -join and its reduction to matching in the shortest-path metric [12]; see also [10, Chapter 2]. The arithmetic assertion is that this minimum equals the cost of changing the actual tail-prime signs. Give the edge belonging to a prime q the cost $q^{-\sigma}$, for fixed $\sigma > 0$. Relative to a reference source, let J be the reading coordinates to be toggled. Put $T = J$ if $|J|$ is even, and $T = J \cup \{*\}$ otherwise.

Proposition 3.7 (Repair as a minimum join). *A repair exists if and only if J has even cardinality in every closed component. Its least prime cost is the minimum total edge cost of a subgraph whose odd-degree vertices are exactly T .*

Proof. Flipping primes is exactly selecting edges modulo two, so the incidence equation gives both necessity and sufficiency. Positive costs make any extraneous cycle removable. Pairing the odd vertices along paths in a feasible subgraph bounds its cost below by a minimum pairing in the shortest-path metric, separately in each component. Conversely, the symmetric difference of shortest paths for a pairing has the required odd vertices and costs no more than the sum of their lengths. This proves the equality with the minimum join formulation. $\square$

This is a finite weighted optimisation identity, not a claim about exact numerical comparison of arbitrary irrational weights. For $\sigma = 1$ all costs are rational. With three or more windows, a tail prime may meet three readings; the columns are then hyperedges, and the graph formula no longer applies. For instance, 41 divides $9^2 + 1$, $11^2 + 2$, and $17^2 - 2$.

4 One low-weight table passing all the partial tests

Local freedom by itself allows a different word at every origin. We now keep *one table* and satisfy all the window and pair tests at once. The construction uses square classes to make the pair conditions consistent, then makes a large prime head trivial to make the window conditions consistent. It does not impose all higher-order multiplicative relations.

4.1 Pair compatibility has an exact description

Fix a finite prime set S and its signs κ . For $i \in I_N$, set

$$r_i = \prod_{\substack{q \notin S \\ v_q(Q_i) \text{ odd}}} q, \quad a_i = \prod_{q \in S} \kappa(q)^{v_q(Q_i)}.$$

Two nonzero vectors over $\mathbb{F}_2$ are independent exactly when they are distinct. It follows that a table passes every one- and two-reading test if and only if

$$w_i = a_i z_{r_i}, \quad z_1 = 1, \quad (4.1)$$

where one arbitrary sign z_r is chosen for each nontrivial exterior class. This is a common assignment to classes, not necessarily a character on their span. A relation among three different classes can still fail.

The same observation gives a useful deletion statement. Write $R_r^{(S)} = \#\{i : r_i = r\}$. The smallest number of deletions that leaves every one- and two-reading projection free outside S is

$$b_S(N) = R_1^{(S)} + \sum_{r>1} (R_r^{(S)} - 1)_+ \ll_{\varepsilon} 2^{|S|} N^{2/3+\varepsilon}. \quad (4.2)$$

Indeed, delete every trivial exterior class and all but one representative of every other class. Necessity is immediate. For the bound, a trivial class has full square class supported on S , while a pair of equal exterior classes has product class supported on S . There are at most $2^{|S|}$ such full classes, and $r-1 \leq \binom{r}{2}$. Apply (2.1) and Theorem 2.2. This bound is independent of the heights of the primes in S .

4.2 Choosing the orientations of the classes

Theorem 4.1 (Quantitative common-table construction). *Let $N \geq 2$, $1 \leq H \leq N$, and let S have s elements. Prescribe κ on S . If*

$$Y \geq \max(2, \max S, \Delta_H),$$

with $\max \emptyset = 1$, a finite algorithm produces a table w passing every H -window test and every pair test, with

$$\#\{i : w_i = -1\} \ll N \min \left(1, \frac{\log(2Y)}{\log(2N)} \right) + C_{\varepsilon} 2^s N^{2/3+\varepsilon} \quad (4.3)$$

for every fixed $\varepsilon > 0$. Each test uses sources agreeing with the same prescribed head on S .

Proof. Extend the head to all primes through Y by assigning $+1$ to primes not in S . The set

$$B_Y = \{i \in I_N : P^+(\text{core}(Q_i)) \leq Y\}$$

is a union of exterior classes, because every prime of S is at most Y .

Use (4.1). For classes in B_Y set $z_r = 1$, including $r = 1$. On every other class choose z_r so that the number of negative values $a_i z_r$ is as small as possible, breaking ties by either fixed convention. The pair tests hold by construction. In each window the only coordinates forced by the enlarged head are those in B_Y , and they have exactly the required sign a_i . Theorem 3.2 supplies a source for that window.

The negative entries in B_Y number at most $|B_Y|$, bounded by (2.4). On a remaining exterior class, if the two head phases occur R_+ and R_- times, the contribution is $\min(R_+, R_-) \leq R_+ R_-$. Each oppositely phased pair in the same exterior class has its full product class supported on S , with character value -1 . There are at most 2^s possible full classes. Summing Theorem 2.2 over them bounds all these minority contributions by the second term in (4.3).

All steps are finite: factor the readings, group their exterior classes, and choose their orientations. No efficient asymptotic factorisation algorithm is needed for the existence statement. $\square$

For fixed S , $H = N^{o(1)}$, and $Y = \max(2, \max S, \Delta_H)$, choose a fixed $\varepsilon < 1/3$ to get weight $o(N)$. This proves the asymptotic part of Theorem 1.1. More generally, a moving head still works if $s \leq (1/3 - \eta) \log_2 N$ for fixed $\eta > 0$, $\log Y = o(\log N)$, and $0 < \varepsilon < \eta$.

There is a direct limitation on proof systems using only these tests. Any inequality that is a valid consequence of precisely their feasible-set constraints must hold at the table in Theorem 4.1. It cannot force a linear Hamming weight on all such tables. Allowing higher-degree algebraic consequences of the *same* constraints does not remove an actual feasible point. This observation does not concern a system with additional prime variables and global relations that the table fails. In particular, the complete relations of [22, Theorem 1.1] may have logarithmic support cardinality without lying in any of the short windows tested here.

4.3 An explicit failure of global realisability

For $N = 4096$, $H = 2$, $S = \{2, 3, 5, 7\}$, $\kappa(2) = -1$ and the other head signs positive, take $Y = 64 = \Delta_2$. The construction above, with positive orientation in ties, gives

Quantity	Value
Readings	12287
Exterior classes	11930
Head-determined readings	177
Negative head-determined readings	103
Other negative readings	149
Total negative readings	252

There are 140 nonfixed classes with both head phases. The negative counts on $n^2 + 1, n^2 + 2, n^2 - 2$ are respectively 90, 94, 68. The verifier tests all 4095 windows by binary linear algebra and all pair constraints by the exact exterior-class criterion.

The entries at $3^2 + 2 = 11$, $9^2 + 2 = 83$, and $1752^2 + 2 = 2 \cdot 11 \cdot 83 \cdot 41^2$ are all positive. Their product is $2 \cdot 37433^2$, so any global source producing those entries would be positive at two. But the table's reading $1^2 + 1 = 2$ is negative. Thus the table has no global multiplicative source, even without an externally imposed head.

This is a finite witness of incompatible global explanations. The asymptotic construction gives a possibly different table for each N and does not claim that every resulting table is globally impossible. Neither assertion supplies a source attaining $m_2(N) = o(N)$.

4.4 Two complete traces still leave most individual readings ambiguous

Locality is not the only way to discard information. Even when two traces are known at *every* index, the third retains many undetermined coordinates. The following fibre description is the trace part of [23, Lemma 2.1], applied to the quotient of two sources. We retain its short proof; the subsequent counting and rank bounds quantify what remains undetermined after a prime head is also fixed.

Proposition 4.2 (Exact fibre after two full traces). *Fix $d \in \mathcal{D}$. Two sources agree on all positive values of Q_e , $e \neq d$, if and only if they agree at every prime outside $\mathcal{P}_d^{\text{ex}}$. The prime signs in $\mathcal{P}_d^{\text{ex}}$ are arbitrary.*

Proof. An exclusive prime divides no value of the two retained quadratics, so changing its sign has no effect. Conversely, apply the quotient argument from Section 1. The retained readings fix two, and also three whenever three is visible. If $q \geq 5$ is the least visible prime with negative quotient sign, a centred root on a retained trace gives $Q_e(r) = qm$, $0 < m < q$. Every prime divisor of m is visible on that same trace or is two, hence already has positive quotient sign. This contradicts the observed value. The visibility table modulo eight leaves exactly the exclusive class invisible. $\square$

Suppose these full traces, all prime signs through Y , and the sign at p are known from a genuine source. The sign at an omitted reading $Q_d(n)$ is determined exactly when $n \in A_d^{\text{ex}}(N; Y, p)$. A single unprescribed exclusive prime of odd valuation can otherwise be flipped. By (2.5), at most

$$CN\sqrt{\log(2Y)/\log(2N)}$$

readings are individually determined. For $Y = N^{o(1)}$, this is $o(N)$.

Individual ambiguity does not imply joint freedom of all remaining coordinates. One unconditional joint lower bound is

$$\#\{\text{possible omitted trace words through } N\} \geq 2^{\#\{Y < q \leq 2N+1: q \in \mathcal{P}_d^{\text{ex}}, q \neq p\}}.$$

For each prime in this set, a centred root supplies a row with pivot q and all other prime factors smaller than q . The resulting rows are triangular and independent after projection outside the known head. The exponent is $(1/2 + o(1))N/\log N$ when $Y = N^{o(1)}$, by the prime number theorem in the fixed progression [21, (27.12.8)]. This is a rank lower bound, not a claim of $2^{N-o(N)}$ independent readings.

5 Geometric restrictions on positive certificates

The preceding arguments describe possible words. The same arithmetic estimates also limit proofs that add the elementary inequalities supplied by certificates. The essential step is to identify a common set of readings that must carry their loads, rather than to count a large number of descriptions of the same identities.

5.1 Width and cardinality are different restrictions

Theorem 5.1 (All sizes, bounded width). *For every admissible weighted family of certificates for p in I_N with width at most H , where $1 \leq H \leq N$,*

$$\sum_C |C| \alpha_C \ll N \frac{\log(2H)}{\log(2N)}. \quad (5.1)$$

The constant is absolute, uniformly in p . In particular, a width $H = N^{o(1)}$ gives capacity $o(N)$ with no bound on certificate size.

Proof. Put $Y = \Delta_H$. A prime $q > Y$ divides at most one reading in a certificate, by Lemma 3.1. If $q \neq p$, its valuation there must therefore be even. Every reading of every certificate lies in the common set

$$\{(n, d) \in I_N : n \in A_d(N; Y, p)\}.$$

Sum the unit-load inequalities over this set and apply (2.4). Since $\log(2\Delta_H) \ll \log(2H)$, the result follows. $\square$

For a probability law Π_N on certificates with $\Pi_N\{C : i \in C\} \leq K/N$ for every label, scaling by N/K shows that

$$\Pi_N\{\text{width}(C) \leq H\} \ll K \frac{\log(2H)}{\log(2N)}.$$

Thus any such diffuse law places asymptotically negligible mass on subpolynomial widths. This is a necessary condition on a law, not a construction of one.

Binary certificates have a stronger obstruction that does not restrict width:

$$\text{Cap}_p(\text{size} \leq 2) \leq R_p(N) + T_p(N) \ll_\epsilon N^{2/3+\epsilon}. \quad (5.2)$$

There is also an exact finite formula. The involution $\tau_p(a) = \text{core}(pa)$ has no fixed point. Apart from the orbit $\{1, p\}$, the certificates between the classes a and $\tau_p(a)$ form complete bipartite graphs. Since $R_1 = 0$,

$$\text{Cap}_p(\text{size} \leq 2) = R_p(N) + \sum_{\{a, \tau_p(a)\} \neq \{1, p\}} \min(R_a(N), R_{\tau_p(a)}(N)), \quad (5.3)$$

with one summand per orbit. The smaller side bounds the edge mass and can be fully matched. Deleting that side, and all class- p singletons, is also the least deletion that destroys every binary certificate. This integer optimum remains only a lower bound for $m_p(N)$.

5.2 A trace used only once must meet a sieve exception

The supplementary laws of quadratic reciprocity give the visibility table

$q \bmod 8$	$q \mid n^2 + 1$ possible	$q \mid n^2 + 2$ possible	$q \mid n^2 - 2$ possible
1	yes	yes	yes
3	no	yes	no
5	yes	no	no
7	no	no	yes

An exclusive prime is exclusive to a *trace*, not necessarily to a single reading on it.

Theorem 5.2 (A singly represented trace). *Under unit loads, the total weight of certificates in which at least one trace is represented exactly once satisfies*

$$\sum_{C: \exists d, |C \cap Q_d|=1} \alpha_C \ll \frac{N}{\sqrt{\log(2N)}},$$

uniformly in p , with no bound on the total size or width of a certificate.

Proof. If (n, d) is the only label of its trace in a certificate, each exclusive prime $q \neq p$ must have even valuation in $Q_d(n)$. Thus $n \in A_d^{\text{ex}}(N; 2, p)$. Every certificate under consideration meets the union of these three exceptional sets. Summing the loads on that union bounds the total mass by its size, and (2.5) applies. $\square$

In particular, all mixed triplets and all certificates of size at most five using all three traces have sublinear total capacity. The theorem does not exclude triplets contained in one trace, nor does it prove that six readings suffice for a positive density.

A six-reading example explains the boundary of the argument:

Trace	Index	Reading
$n^2 + 1$	2	5
$n^2 + 1$	13	$170 = 2 \cdot 5 \cdot 17$
$n^2 + 2$	1	3
$n^2 + 2$	11	$123 = 3 \cdot 41$
$n^2 - 2$	11	$119 = 7 \cdot 17$
$n^2 - 2$	17	$287 = 7 \cdot 41$

Their product is $2 \cdot 73185^2$. The exclusive primes 5, 3, 7 cancel within their respective traces, and 17, 41 join the pairs. Outside two the six square classes have rank five: the coordinates 5, 3, 7 force equal coefficients within each pair, and 17, 41 force equality between pairs. Hence the full set is the only nonempty relation, and its target is two. There is no proper square or target-two subrelation.

5.3 A separate fixed-size improvement

The width bound is uniform over all sizes. When the size is fixed, integral-point bounds give a different estimate that can be stronger at polynomial widths.

Theorem 5.3 (Bounded size and width). *For every fixed $k \geq 2$ and $\varepsilon > 0$, uniformly in p , $N \geq 2$, and $1 \leq H \leq N$,*

$$\text{Cap}_p(\text{size} \leq k, \text{width} \leq H) \ll_{k, \varepsilon} \log(2N) + (H + 1)^{k-1+\varepsilon}.$$

Thus widths $H \leq N^\theta$ have capacity $o(N)$ whenever $\theta < 1/(k-1)$. For each fixed width H , the capacity of all certificates in that width is $O_H(\log(2N))$, uniformly in p .

Proof. An anchored shape with $r \geq 2$ readings gives

$$F(T) = \prod_{j=1}^r ((T + t_j)^2 - d_j), \quad 0 \leq t_j < H,$$

with distinct typed shifts and at least one $t_j = 0$. This polynomial is separable and all its roots lie in the fixed field $K_0 = \mathbb{Q}(i, \sqrt{2})$. Its discriminant satisfies

$$\Delta_F = \prod_j 4d_j \prod_{i < j} R_{d_i, d_j} (t_i - t_j)^2, \quad 0 < |\Delta_F| \leq 8^r (H^2 + 4)^{2r(r-1)}. \quad (5.4)$$

We specify the imported integral-point bound. Evertse–Silverman [13, Theorem 1(b)] bounds the number of $x \in R_S$ for which a separable polynomial $f(x)$ is a nonzero square in a number field K . With $m = [K : \mathbb{Q}]$, $s = |S|$, and an extension L/K of degree M containing three roots, their bound is

$$7^{M(4m+9s)} 4^{\kappa_2(L)},$$

provided f has degree at least three, has coefficients in the ring of S -integers R_S , and its discriminant is an S -unit. Here $\kappa_2(L)$ is the dimension of the two-torsion in the class group. Take $K = \mathbb{Q}$, $L = K_0$, $f = pF$, and S to consist of the infinite place and all primes dividing $p\Delta_F$. The discriminant of pF is $p^{4r-2}\Delta_F$, so every hypothesis holds. A solution $F(x) = pz^2$ gives $pF(x) = (pz)^2$. We obtain

$$\#\{x \in \mathbb{Z} : F(x) = pz^2 \text{ for some } z \neq 0\} \leq A_0 B_0^{\omega(p\Delta_F)}, \quad (5.5)$$

where $A_0 = 7^{52} 4^{\kappa_2(K_0)}$ and $B_0 = 7^{36}$ are absolute. We only use finiteness of the class group of the fixed field; no uncomputed assertion that its two-torsion vanishes is needed.

For fixed $k, r \leq k$, the divisor-type bound $B_0^{\omega(m)} \ll_\xi |m|^\xi$ and (5.4) make (5.5) $O_{k,\varepsilon}((H+1)^\varepsilon)$, uniformly in p , because $\omega(p) = 1$. The number of anchored shapes is at most

$$3 \binom{3H-1}{r-1} \ll_k (H+1)^{r-1}.$$

Sum over $2 \leq r \leq k$. Singletons contribute $R_p(N) = O(\log(2N))$. Each certificate weight is at most one. For fixed H , take $k = 3H$, since no width- H certificate has more labels. $\square$

The fixed-field mechanism is closely related to the application in [5, Lemma 3.3]. The discriminant calculation and the explicit localisation above are what allow the shifts, width, and target prime to move in this statement. The size k is fixed before the limit.

5.4 Rational centres require many denominators

One may try to make many same-trace pairs by using solutions of a norm equation as centres. The norm equation alone omits an integrality condition on its divisors.

Proposition 5.4 (Exact rational-centre correspondence). *If $x < y \leq N$ and $Q_d(x)Q_d(y) = pz^2$ with positive readings, set*

$$g = \gcd(x+y, xy+d), \quad a = (xy+d)/g, \quad b = (x+y)/g, \quad c = z/g.$$

Then $a \geq 0$, $b, c \geq 1$ are pairwise coprime integers, $p \nmid b$, and

$$a^2 - pc^2 = db^2, \quad a < Nb. \quad (5.6)$$

The integers $r = bx - a$ and $s = by - a$ satisfy

$$0 < r < s, \quad rs = pc^2, \quad r \equiv s \equiv -a \pmod{b}, \quad x = (a+r)/b, \quad y = (a+s)/b. \quad (5.7)$$

Conversely, a primitive point of (5.6) and a divisor $r < s = pc^2/r$ with $r \equiv -a \pmod{b}$ and $a+s \leq bN$ give exactly one such pair.

Proof. The identity $(xy+d)^2 - d(x+y)^2 = Q_d(x)Q_d(y) = pz^2$ shows $g \mid z$ by prime valuations, including at p . This proves integrality and the norm relation. The coprimality follows from $(a, b) = 1$: a common prime of b, c would divide a , while a common prime of a, c would force a square divisor of d . Similarly $p \mid b$ would force $p \mid a$.

Since $g \mid Q_d(x), Q_d(y)$, we have $r = Q_d(x)/g$ and $s = Q_d(y)/g$, which proves (5.7). Conversely $(pc, b) = 1$, so the norm relation and the congruence for r force that for s . The resulting integers x, y satisfy $a(x+y) = b(xy+d)$. Thus $t = (x+y)/b$ is integral and $Q_d(x) = rt$, $Q_d(y) = st$, yielding product $p(ct)^2$ and the specified reduced centre. Uniqueness follows from the definitions. The possible zero centre is not lost: $p = 2$, $d = -2$, $(x, y) = (1, 2)$ gives $(a, b, c) = (0, 1, 1)$. $\square$

Theorem 5.5 (Denominator diversity). *For any set $\mathcal{B} \subseteq \{1, \dots, 2N\}$, the number of same-trace pairs for p whose reduced centre has denominator in $\mathcal{B}$ is*

$$T_{p,d}(N; \mathcal{B}) \ll_{\varepsilon} |\mathcal{B}| N^{\varepsilon}$$

for every fixed $\varepsilon > 0$, uniformly in p, d . The same upper bound holds for their capacity. If all these denominators use a common set of $o(\log N)$ primes, their number and capacity are $N^{o(1)}$.

Proof. For a fixed denominator $b \leq 2N$, (5.6) has norm db^2 and

$$1 < a + c\sqrt{p} \leq 6N^2, \quad pc^2 \leq 6N^4.$$

Lemma 2.1 counts at most $\tau(|d|b^2)(1 + \log(6N^2)/\log \lambda_0)$ centres. Each supplies at most $\tau(pc^2)/2$ unordered divisor pairs, even before the congruence and height tests. The elementary divisor bound, with a sufficiently small fixed exponent, proves the first assertion after summing over b .

If a common prime set has s elements, a denominator at most $2N$ has an exponent vector of sum at most $L = \lfloor \log_2(2N) \rfloor$. There are at most $\binom{L+s}{s}$ such vectors. When $s = o(\log N)$, the logarithm of this binomial coefficient is $o(\log N)$. Apply the first assertion with any fixed positive exponent and then let that exponent be arbitrarily small. $\square$

The special case $\mathcal{B} = \{1\}$ includes the entire integer-centre construction

$$m^2 - d = pu^2, \quad ab = pu^2, \quad x = m + a, \quad y = m + b, \quad Q_d(x)Q_d(y) = p[u(x + y)]^2.$$

Its union over all integer centres is still $N^{o(1)}$. Adding more divisors to the same type of centre cannot give a fixed power of N . The theorem is not a bound of that order on all pairs with unrestricted denominators; for those, Theorem 2.2 gives the separate $N^{2/3+\varepsilon}$ estimate.

The divisor test is substantial. The primitive point

$$23^2 - 2 \cdot 17^2 = -7^2$$

has no divisor of $2 \cdot 17^2$ congruent to $-23 \equiv 5 \pmod{7}$, hence produces no integer pair at any height. With the same denominator, $(a, b, c) = (103, 7, 73)$ does give the pair $(15, 776)$. More generally, for even $t \geq 28$,

$$a = t^2 + 2t - 1, \quad b = t^2 - 2t - 1, \quad c = t^2 + 1$$

are primitive solutions of $a^2 - 2c^2 = -b^2$, with $1 < a/b < 7/6$. No centre $(xy - 1)/(x + y)$ of positive integers $x < y$ lies in this interval: $x = 1$ gives a value below one; $x = 2$ gives one at $y = 3$ and at least $7/6$ afterwards; $x \geq 3$ gives at least $11/7$. Thus $\gg \sqrt{B}$ distinct denominators $b \leq B$ support these norm points but no associated pair. The elementary norm identities and coprimality follow by expansion and $(t, b) = 1$.

Once admissible pairs really are counted, their loads cost little. For a fixed reading, its partner has a fixed square class, so (2.1) gives $O(\log N)$ partners. A greedy matching extracts $\gg T/\log N$ disjoint pairs from any T distinct pairs. It is the count with both the divisor congruence and the height restriction, not the number of points on the norm conic, that would feed this conclusion.

5.5 A universal polynomial identity needs a fixed anchor

Suppose $R_i \in \mathbb{Q}[T]$ and

$$\prod_i (R_i(T)^2 - d_i) = pZ(T)^2 \neq 0,$$

where every constant R_i is an admissible positive integer index. If C is the product of the constant readings, comparison of leading coefficients gives $C/p \in \mathbb{Q}^{\times 2}$. Since C is a positive integer, $C = pz_0^2$ for an integer z_0 . In particular at least one reading is constant. All emitted certificates share its label, so their capacity is at most one. The same leading-monomial argument works for polynomial identities in several parameters.

For example,

$$(T^2 + 1)((T + 1)^2 + 1) = (T^2 + T + 1)^2 + 1.$$

Adjoining the constant reading $1^2 + 1 = 2$ gives on the order of $\sqrt{N}$ four-reading certificates, but their capacity is exactly one once any of them is present. This statement concerns an identity in the polynomial ring, not arbitrary integral points on its associated variety.

6 A fixed algebraic curve has at most logarithmic capacity

The preceding anchor argument assumes a polynomial identity. We now allow arbitrary rational points on a fixed algebraic curve, with no chosen parametrisation. Integrality of the reading indices, rather than the appearance of a convenient formula, determines the restriction.

Fix p , r , and $d_1, \dots, d_r \in \mathcal{D}$, and let C be a geometrically integral affine curve over $\mathbb{Q}$ contained in

$$\prod_{j=1}^r (X_j^2 - d_j) = pZ^2. \quad (6.1)$$

A rational point is admissible at height N if the X_j are integers in $[1, N]$, all readings are positive, and their labels (X_j, d_j) are distinct. The corresponding rational Z is automatically integral: a rational square with a denominator dividing a prime cannot have a nontrivial square denominator. Repeated emissions of one certificate are merged.

Theorem 6.1 (Fixed-curve barrier). *If some X_j is constant on C , the capacity of the emitted certificates is at most one. Otherwise the number of emitted certificates, and hence their capacity, is $O_C(\log(2N))$.*

If infinitely many admissible points exist in the second case, the projective normalisation of C is $\mathbb{P}_{\mathbb{Q}}^1$. Its points at infinity are exactly two conjugate points with residue field $\mathbb{Q}(\sqrt{p})$, and each is a pole of every X_j .

The constant depends on the fixed curve, its coordinate functions, and the target. It is not uniform over a sequence of curves chosen as N grows.

The step from integrality to finitely many denominator norms uses the following elementary form of Bézout's identity.

Lemma 6.2 (A fixed gcd for primitive evaluations). *Let $A, B \in \mathbb{Z}[U, V]$ be nonzero homogeneous forms of the same positive degree, with no common zero in $\mathbb{P}^1(\mathbb{Q})$. There is a nonzero integer D , depending only on the two forms, such that*

$$\gcd(A(a, b), B(a, b)) \mid D \quad (\gcd(a, b) = 1).$$

Proof. On the chart $V = 1$, the two coprime polynomials admit an integral Bézout identity with constant right side $R_0 \neq 0$, after clearing denominators. Homogenisation shows that their evaluated gcd divides $R_0 b^m$ for some fixed m . The chart $U = 1$ similarly gives divisibility by $R_{\infty} a^{m'}$, with $R_{\infty} \neq 0$. For every prime, at least one of a, b is a unit. The corresponding identity bounds the gcd valuation by that of R_0 or R_{∞} . Hence $D = |R_0 R_{\infty}|$ works, including the primitive pairs with a zero coordinate. $\square$

The proof follows four steps. Infinitely many integral readings force the nonconstant coordinates towards common poles. The certificate identity then determines the quadratic field of those poles. Integrality bounds the norms of the rational parameter's denominators, leaving finitely many unit orbits and hence only logarithmically many possibilities at the given height. The geometric restriction alone would not supply the count.

Proof of Theorem 6.1. A constant admissible coordinate supplies a fixed label in every certificate, so its unit load proves the first assertion. Assume now that every X_j is nonconstant. Finitely many admissible points cause no difficulty, and we may assume there are infinitely many.

Pass to the smooth projective normalisation $\overline{C}$. Only finitely many singular points are lost. Its relevant boundary is the union of the poles of the coordinate functions X_j, Z ; by (6.1), Z cannot have a pole unless an X_j does. The integral points lift to S -integral points on a fixed model of the normalisation, with a fixed finite set S accounting for denominators. The necessary part of Siegel's theorem says that infinitely many such points force genus zero and at most two geometric boundary points; see the formulation in [2, Introduction and Theorem 1.2]. A nonsingular rational point then identifies $\overline{C}$ with $\mathbb{P}_{\mathbb{Q}}^1$.

Choose an infinite sequence of admissible points and a convergent subsequence in the compact real projective line. Let its limit be A . If a nonconstant X_j were regular at A , its integer values along the sequence would converge, hence be eventually constant. A nonconstant rational function has finite fibres, a contradiction. Thus every X_j has a pole at A . The rational function

$$R = Z / \prod_j X_j$$

satisfies

$$pR^2 = \prod_j (1 - d_j/X_j^2).$$

It is regular and nonzero at A , with $pR(A)^2 = 1$. The residue field at this algebraic boundary point therefore contains $\mathbb{Q}(\sqrt{p})$. There are at most two geometric boundary points in all, so they must be exactly the two conjugates of A , with that residue field. Rationality of each X_j makes its pole set invariant under conjugation; hence each has poles at both points.

Choose a rational coordinate t on $\mathbb{P}^1$ whose infinity is not a boundary point. The boundary is defined by an irreducible quadratic

$$F(t) = a_0 t^2 + b_0 t + c_0 \in \mathbb{Z}[t], \quad b_0^2 - 4a_0 c_0 = ps_0^2,$$

with s_0 a nonzero integer. One nonconstant coordinate has the form

$$X_j(t) = \frac{G(t)}{cF(t)^k}, \quad k \geq 1, \quad \deg G \leq 2k, \quad (G, F) = 1,$$

for a nonzero integer c and an integral polynomial G . Let F_h, G_h be the homogeneous forms, of degrees two and $2k$ respectively. The forms F_h^k, G_h have no common geometric zero on $\mathbb{P}^1$. Lemma 6.2 therefore gives a fixed nonzero integer D such that

$$\gcd(F_h(a, b)^k, G_h(a, b)) \mid D \quad \text{whenever } (a, b) = 1. \quad (6.2)$$

An integral value $X_j(a/b)$ implies $F_h(a, b)^k \mid G_h(a, b)$. Thus (6.2) bounds $|F_h(a, b)|$ by a fixed constant. It is nonzero, since F is irreducible. Also, compactness on $\max(|a|, |b|) = 1$ and the absence of common zeros give

$$\max(|F_h(a, b)|^k, |G_h(a, b)|) \gg_C \max(|a|, |b|)^{2k}.$$

Because $|X_j| \leq N$, the left side is $O_C(N+1)$. Therefore $|a|, |b| \ll_C (N+1)^{1/(2k)}$.

There are only finitely many nonzero integers $h = F_h(a, b)$ to consider. For each, complete the square:

$$(2a_0a + b_0b)^2 - p(s_0b)^2 = 4a_0h. \quad (6.3)$$

The coordinates in this fixed, nonzero norm equation are polynomially bounded in N . Lemma 2.1, applied after taking their absolute values, bounds their number by $O_C(\log(2N))$; zero coordinates contribute only a finite number. The map from (a, b) to these coordinates has finite fixed multiplicity. This bounds the rational parameters and proves the theorem. $\square$

6.1 Sharpness, abundance, and shared loads

The logarithmic order occurs for genuine unanchored pairs. On the Pell curve

$$y^2 - 2x^2 = 1, \quad y_k + x_k\sqrt{2} = (3 + 2\sqrt{2})^k,$$

we have $Q_{-1}(y_k) = 2Q_{-1}(x_k)$. The x_k are even, the y_k odd, and both sequences strictly increase, so all pairs are disjoint. Their capacity through height N is

$$\frac{\log N}{\log(3 + 2\sqrt{2})} + O(1).$$

One rational parametrisation is $x = 2t/(t^2 - 2)$, $y = (t^2 + 2)/(t^2 - 2)$; its two poles are exactly the conjugate points predicted by the theorem.

Even Zariski density does not control loads. Let

$$a_i + u_i\sqrt{5} = (2 + \sqrt{5})^{2i+1}, \quad b_j + v_j\sqrt{10} = (3 + \sqrt{10})^{2j+1}.$$

Then $a_i^2 + 1 = 5u_i^2$, $b_j^2 + 1 = 10v_j^2$, and every cross-pair is a certificate for two. The products of these two infinite Pell sets are Zariski dense in the product of the two norm conics: an infinite subset of an integral curve is dense, and a polynomial vanishing on the product vanishes successively on each factor. There are on the order of $\log^2 N$ cross-pairs through height N , but their capacity is exactly the smaller of the two vertex counts, hence only of order $\log N$. In detail, those counts are

$$\frac{\log N}{\log(9 + 4\sqrt{5})} + O(1), \quad \frac{\log N}{\log(19 + 6\sqrt{10})} + O(1).$$

This is a complete bipartite matching calculation, not a lack of rational points.

A finite collection of fixed rational recipes, even allowing rational rather than just integral parameter values, also has capacity $O(\log N)$. Adjoin Z with (6.1) and split into its finitely many curve components; components not geometrically integral have only finitely many rational points outside their intersections with conjugates. Apply Theorem 6.1 to the others. This corollary bounds the certificates emitted by the recipes, not every possible certificate that might be formed by recombining their readings.

Finally, the nonsquare target is essential. The identity

$$(4x^3 + 3x)^2 + 1 = (x^2 + 1)(4x^2 + 1)^2$$

gives polynomially many pairs with square product. By restricting to $x \leq cN^{1/3}$ and greedily discarding overlaps, one obtains $\gg N^{1/3}$ disjoint pairs. These are relations of target class one, not error-forcing certificates for a prime. The boundary-field argument correctly distinguishes the two situations.

7 Moving transport libraries: diversity matters more than height

A fixed-curve bound does not address a growing library of rules. We now allow the coefficients and the rules themselves to depend on N . The price will be measured by the diversity and total degree of the library, not by an untracked constant attached to each curve.

7.1 What it means to transport a parity

A typed link is a pair of distinct labels $(n, d), (m, e)$ allowed by a specified relation between n and m . A certificate is *supported by the library* if, for every prime $q \neq p$, the readings in that certificate where q occurs to odd valuation can be paired along allowed links. The pairing may depend on q .

This condition is stronger than the fact that each prime occurs an even number of times, which every certificate already satisfies. It describes proofs that cancel these parities using the chosen links. The bounds below apply to this definition, not to every conceivable use of an algebraic relation.

7.2 Affine rules force a finite prime alphabet

Consider a rule $an = bm + c$, with integer coefficients of absolute value at most A , not both a, b zero. A common prime divisor of $n^2 - d$ and $m^2 - e$ must divide

$$R = (a^2d + b^2e - c^2)^2 - 4a^2b^2de, \quad |R| \leq 33A^4. \quad (7.1)$$

This follows by eliminating n, m from their quadratic congruences and the linear relation. If $R = 0$ and $ab \neq 0$, the biquadratic-field independence of $\sqrt{d}, \sqrt{e}$ shows that $d = e$, $c = 0$, and $a = \pm b$. The only positive-index possibility is the forbidden identical label. If one coefficient is zero, $R = 0$ would require an integer square to equal a nonsquare rational multiple of that coefficient's square, again impossible for a nontrivial rule. Thus rules with $R = 0$ have no admissible link relevant here.

Let M be the least common multiple of all nonzero resultants in a library, with $M = 1$ for an empty list. A library-supported certificate has $\text{core}(Q_i) \mid \text{rad}(pM)$ at each of its readings: every other odd prime must be paired along a link and hence divides that link's resultant. Theorem 2.3 and the unit loads give

$$\sum_C |C| \alpha_C \ll N \min \left(1, \frac{\log(2 + K \log(2A))}{\log(2N)} \right) \quad (7.2)$$

for K affine rules of height at most A . For a fixed library the sharper bound is $O_{\mathcal{L}}(\log(2N))$, uniformly in p .

For example, suppose each certificate lies in the union of two H -windows with the *same* gap G for the entire family. All within- and between-window pairings can be represented by $O(H)$ typed translations of height $O(N)$, even when G is macroscopic. Formula (7.2) is $o(N)$ if $H = N^{o(1)}$. The statement would not follow if every certificate could select a new arbitrary gap without paying for that additional diversity.

7.3 Polynomial rules of unrestricted coefficient height

Let a library consist of nonzero nonconstant polynomials $F(X, Y) \in \mathbb{Q}[X, Y]$, each with an ordered pair of trace types. Factor them over $\mathbb{Q}$ and remove duplicate components for the

same type. Let ℓ be the number of linear components and let $d_j \geq 2$ be the degrees of the nonlinear components. Define

$$\mathfrak{D} = \max \left(1, \ell + \sum_j d_j \right).$$

The coefficient heights are not bounded.

Theorem 7.1 (Algebraic-library barrier). *For a library-supported weighted family in I_N , uniformly in p , the rules, and their coefficients,*

$$\sum_C |C| \alpha_C \ll N \min \left(1, \frac{\log(2 + \ell \log(2N))}{\log(2N)} \right) + \mathfrak{D} \sqrt{N} \log(2N) + \mathfrak{D}^4. \quad (7.3)$$

The left side is also at most $3N - 1$. Consequently $\mathfrak{D} = N^{o(1)}$ gives capacity $o(N)$. If there are no rich linear components in the proof below, the first term may be replaced by $O(\log(2N))$.

Proof. Call a line *rich* if it has at least two distinct integer points in $[1, N]^2$. A primitive equation $an + bm = c$ for such a line can be chosen with $|a|, |b| \leq N$ and $|c| \leq N^2$: subtract two points, divide their coordinate differences by their gcd, and substitute one point. Hence its nonzero resultant is at most $41N^8$. A line that is not rich supplies at most one pair. Put all endpoints of these latter links into a set Z .

For a nonlinear irreducible plane component of degree $d \geq 2$, the coefficient-uniform estimate of Castryck–Cluckers–Dittmann–Nguyen [7, Theorem 3] is

$$\#(C(\mathbb{Z}) \cap [-N, N]^2) \leq C_0 d^3 N^{1/d} (\log(2N) + d), \quad (7.4)$$

with an absolute constant C_0 . Its hypotheses are integrality over $\mathbb{Q}$ and the displayed degree; no bound on coefficient height is required. Put the endpoints of all these links into Z as well. Then

$$|Z| \leq 2\ell + 2C_0 \sum_j d_j^3 N^{1/d_j} (\log(2N) + d_j).$$

Summing the degree costs. Assume first $N \geq e^2$. For $2 \leq d \leq \log N$, the derivative of $3 \log d + (\log N)/d$ changes sign only from negative to positive. Its maximum on this interval is therefore at an endpoint, giving

$$d^3 N^{1/d} \leq \max\{8\sqrt{N}, e(\log N)^3\} \ll \sqrt{N}.$$

Also $\log(2N) + d \ll \log(2N)$ in this range. There are at most $\mathfrak{D}$ components, so their total contribution is $O(\mathfrak{D} \sqrt{N} \log(2N))$. For $d > \log N$, we have $N^{1/d} < e$ and $\log(2N) + d \ll d$, so the contribution is $O(d^4)$. Since

$$\sum_j d_j^4 \leq \left(\sum_j d_j \right)^4 \leq \mathfrak{D}^4,$$

we obtain $|Z| \ll \mathfrak{D} \sqrt{N} \log(2N) + \mathfrak{D}^4$. The bounded range $2 \leq N < e^2$ and the term 2ℓ are absorbed by the same absolute constant.

Let M be the least common multiple of the nonzero resultants of the rich lines. Then $\log(2M) \ll 1 + \ell \log(2N)$. Outside Z , an odd prime $q \neq p$ used by a supported certificate must be carried along a rich line and thus divides M . Such readings lie in the finite-alphabet set of (2.6). Sum the loads separately on this set and on Z to obtain (7.3). With no rich line, $M = 1$, so (2.1) gives the final refinement. $\square$

The proof separates two possibilities that a large coefficient could conceal. A line with only one integer point is charged to an exceptional endpoint set. A line with two points admits a small primitive equation determined by those points. Thus coefficient height cannot be used as uncharged diversity.

A nonlinear rule may share large prime factors without having many links. For instance, $m = n^2 - n + 1$ satisfies $m^2 + 1 = (n^2 + 1)((n - 1)^2 + 1)$ but has only $O(\sqrt{N})$ pairs with both indices at most N . Conversely,

$$\prod_{t=-N+1}^{N-1} (Y - X - t) = 0$$

allows every pair in the box; its degree $2N - 1$ pays for that freedom. A bound for plane curves cannot be applied without further argument to a higher-dimensional relation with an existentially quantified extra variable.

7.4 Exact cofactor ratios require almost linearly many rules

For one fixed quadratic, the small count for an exact-ratio rule already appears in [5, Lemma 3.1], which draws on the quadratic part of [8, Lemmas 2.4–2.5 and proof]. The point below is the mixed-type formulation and its conversion into a necessary diversity bound for an entire library. A particularly rigid rule is

$$bQ_d(n) = aQ_e(m), \quad a, b \geq 1, \quad (a, b) = 1.$$

Proposition 7.2 (Exact-ratio libraries). *A single such rule has $O_\eta(N^\eta)$ admissible links for every fixed $\eta > 0$, uniformly in a, b, d, e . A library of K exact-ratio rules supporting certificates under the preceding parity-pairing definition satisfies*

$$\sum_C |C| \alpha_C \ll_\eta K N^\eta + \log(2N).$$

A linear mass therefore requires $K \geq N^{1-o(1)}$ in the precise sense that $K \gg_\eta N^{1-\eta}$ for each fixed $\eta > 0$ along such a family.

Proof. If any link exists, reduction of the ratio implies $a, b \leq N^2 + 2$. Eliminating the cofactor gives

$$(bn)^2 - abm^2 = b(bd - ae) = K_0.$$

If $K_0 = 0$, positivity of the indices gives $bn^2 = am^2$ and $bd = ae$. The only square ratio between elements of $\mathcal{D}$ is the identical one, forcing the identical label; there is no admissible link. Otherwise $|K_0| \ll N^4$, and $bn + m\sqrt{ab} \ll N^3$. Remove the square part of ab and use Lemma 2.1, including its factorised case, followed by the divisor bound. This proves the link count.

Every reading of a supported certificate either belongs to one of these links or has no odd prime factor except possibly p . The latter readings have square class p and number $O(\log(2N))$; square class one does not occur. Count the endpoints of the K link sets and sum their unit loads. $\square$

The exponent η is fixed before N tends to infinity. The final necessary condition does not result from substituting a varying $\eta(N)$ into an untracked constant.

8 Capacity can miss most of the forced errors

Every certificate gives an odd-parity constraint on actual signs. Replacing it by a positive covering inequality forgets part of that constraint. We first identify the resulting optimisation problem exactly, then realise large gaps using quadratic readings rather than an abstract binary matrix alone.

8.1 The integral obstruction and its fractional relaxation

Represent the square classes of a finite sample by rows $v_i \in \mathbb{F}_2^d$, and the target by a nonzero vector t . Then

$$\mu_t = \min_{x: t \cdot x = 1} \text{wt}((v_i \cdot x)_i), \quad C \text{ is a certificate} \iff \sum_{i \in C} v_i = t. \quad (8.1)$$

Add a distinguished element e , represented by t , to the binary matroid represented by the vectors v_i (viewed as columns). An inclusion-minimal certificate C is exactly a set for which $C \cup \{e\}$ is a circuit containing e . Indeed, a zero-sum proper subset of C could be removed, and a target-sum proper subset would contradict minimality. The converse is the same argument in reverse. Thus the minimal certificates form the *port at e* of this binary matroid, in the terminology of Cornuéjols [10, author's July 2000 notes, Section 8.3.1, p. 120].

Every certificate contains a minimal one. Replacing it by that subset preserves its weight and cannot increase any load; it also preserves disjointness in an integral packing. Hitting all minimal certificates is equivalent to hitting all certificates. Writing ν, ν^* for integral and fractional packing and τ, τ^* for integral and fractional covering of this port, the dictionary is

$$\text{Pack} = \nu, \quad \text{Cap} = \nu^* = \tau^*, \quad \mu = \tau.$$

The middle equality is finite linear programming duality. The following standard separation argument proves the last equality directly in our sign notation.

Proposition 8.1 (Integral-cover interpretation). *The minimum μ_t equals the smallest cardinality of a subset B of readings that meets every certificate for t .*

Proof. The negative readings of an assignment with $t \cdot x = 1$ meet every certificate. Conversely, if B meets every certificate, t is not in the span of the rows outside B . A linear functional can therefore vanish on that span and equal one on t . Its negative readings are contained in B . $\square$

Thus all certificate inequalities with an integral cover retain the true minimum. Passing to the fractional cover, equivalently to the capacity by finite linear programming duality, is the relaxation at issue. The arithmetic constructions below exhibit its gap with the full family of certificates; Section 8.4 makes the distinction explicit through an identity of signed products.

8.2 Realising odd binary rows on $n^2 + 1$

The criterion used here is classical. Lemmermeyer's nonresidue-graph formulation [17, Section 5, Proposition 5.3] gives a norm-minus-one unit when every nontrivial bipartition of the prime-discriminant graph has an odd cross-degree. Our nonresidue conditions give a complete graph on an odd number of vertices, which has that property. When 2 occurs, its prime-discriminant vertex is 8, not 2; for each odd $q \equiv 5 \pmod{8}$, the relevant symbols $(8/q)$ and $(q/2)$ are both -1 . We keep the elementary proof below to obtain the integral equation in precisely our conventions, rather than infer integrality from a statement about units in a maximal order.

Lemma 8.2 (Classical odd nonresidue criterion, specialised). *Let $q_0 = 2$, and choose distinct primes $q_1, \dots, q_{d-1} \equiv 5 \pmod{8}$ with $\left(\frac{q_i}{q_j}\right) = -1$ for $i \neq j$, $i, j \geq 1$. Every product a of an odd number of distinct primes from this list admits positive integers n, u with*

$$n^2 - au^2 = -1.$$

Such solutions give arbitrarily large, distinct n .

Proof. The quadratic reciprocity law makes the pairwise nonresidue requirements symmetric, since all odd primes are 1 modulo four; also $\left(\frac{2}{q_j}\right) = \left(\frac{-2}{q_j}\right) = -1$ and $\left(\frac{-1}{q_j}\right) = 1$. The number a is congruent to five modulo eight if it is odd, and to two modulo eight otherwise.

Take the solution $X, Y > 0$ of $X^2 - aY^2 = 1$ with least X , whose existence is Lagrange's theorem [9, Theorem 2.3]. Reduction modulo eight gives X odd and Y even. The consecutive coprime integers $(X-1)/2$ and $(X+1)/2$, of product $a(Y/2)^2$, have the form br^2 and cs^2 with $bc = a$. Thus

$$cs^2 - br^2 = 1.$$

If $b, c > 1$, one contains an even number of the selected prime factors and the other an odd number. The even part contains an odd prime ℓ . Every prime in the other part is a nonresidue modulo ℓ , including two when present. Reducing the displayed equation modulo ℓ , and using $\left(\frac{-1}{\ell}\right) = 1$, would make the odd part a residue, a contradiction. Thus $b = 1$ or $c = 1$. If $c = 1$, then $s^2 - ar^2 = 1$ is a positive Pell solution with $s < X$, contradicting minimality. Therefore $b = 1$, giving $r^2 - as^2 = -1$.

Odd powers of $r + s\sqrt{a}$ have norm -1 , positive integral coefficients, and unbounded first coordinate. $\square$

The required prime list can be chosen beyond any finite forbidden set. At each step choose nonresidue classes modulo the previous odd primes and the class five modulo eight; the Chinese remainder theorem and Dirichlet's theorem [21, Section 27.12] supply a new prime in the combined progression. Quadratic reciprocity supplies the reverse requirements.

Corollary 8.3 (Arithmetic realisation). *Any finite collection of odd-weight vectors in $\mathbb{F}_2^d$, with target e_0 , can be realised as the square classes of distinct readings $n_i^2 + 1$ by sending e_j to $[q_j]$, with $q_0 = 2$. The indices may exceed any prescribed bound. A finite prime head with sign -1 at two may be fixed arbitrarily; choose all other q_j outside that head.*

All binary assignments with target sign -1 remain available. Hence the realisation preserves the complete certificate hypergraph, its packing and capacity, and the true minimum of errors.

Proof. Apply Lemma 8.2 to each row product, and use successively larger odd powers to make the indices distinct and above the prescribed bound. The resulting readings are exactly the row products times squares. Distinct primes give independent square classes. The square factors do not affect signs, including those at protected primes. $\square$

This is an existence construction with a finite search description. It has no claimed polynomial height bound in the number of rows, and no claimed efficient reduction in their bit size.

8.3 Bounded capacity and a linear error minimum

Theorem 8.4 (Arbitrarily large arithmetic gaps). *For every $M \geq 32$, every finite prime head κ with $\kappa(2) = -1$, and every prescribed lower bound for the indices, there exist M distinct*

readings $A_i = n_i^2 + 1$ above that bound such that

$$\mu_2(A) > M/16, \quad 1 \leq \text{Cap}_2(A) < 16.$$

These values of the invariants are unchanged by restricting sources to the prescribed head.

Proof. Put $d = \lfloor M/2 \rfloor$, $t = \lfloor M/16 \rfloor$, and choose the rows independently and uniformly from the odd-weight affine hyperplane of $\mathbb{F}_2^d$. For $x_0 = 1$, the all-ones vector x produces M negative readings. Every other such x gives independent fair row evaluations. Writing $B(M, t) = \sum_{j=0}^t \binom{M}{j}$, the probability that some such assignment has weight at most t is bounded by

$$2^{d-1-M} B(M, t).$$

A sum of an even number of odd rows cannot equal e_0 . A nonempty odd subset of rows sums uniformly over the odd affine hyperplane, so the probability that some certificate has size at most t is at most

$$2^{1-d} B(M, t).$$

The binary entropy bound gives $B(M, t) \leq 2^{MH_2(1/16)} < 2^{3M/8}$. The sum of the two failure probabilities is at most $(9/2)2^{-M/8} < 1$ for $M \geq 32$. There is therefore a matrix with minimum greater than t and no certificate of size at most t .

It has a certificate: otherwise separation of e_0 from the row span would give an assignment of weight zero. Thus its capacity is at least one. Summing the unit loads gives

$$(t+1) \sum_C \alpha_C \leq \sum_C |C| \alpha_C \leq M,$$

so the capacity is at most $M/(t+1) < 16$, while the minimum is at least $t+1 > M/16$. Corollary 8.3 transfers this entire finite model to the required readings and head. $\square$

The probability argument selects a finite matrix, not a random multiplicative source in the conclusion. Large integrality gaps are a familiar combinatorial phenomenon; the point here is their realisation on a single quadratic trace with all actual source assignments preserved.

8.4 A fifteen-reading model in which signed multiplication does more

The classical binary character model on a four-dimensional vector space makes the lost information visible without an optimisation solver. Its role here is its exact realisation by the subsequent quadratic values, not a new abstract coding construction. In $\mathbb{F}_2^5$, let W be the even-weight subspace, of dimension four, and take the fifteen rows

$$v_t = e_0 + t, \quad 0 \neq t \in W.$$

No row is the target, and every certificate has odd size, hence at least three. For distinct nonzero t, u , the triple $\{t, u, t+u\}$ is a certificate. There are 35 such triples, each vertex lies in seven, and giving each weight $1/7$ gives capacity five. The size lower bound gives the reverse inequality $\text{Cap} \leq 15/3 = 5$.

For an actual source with target sign -1 , write its reading signs as $Z_t = -\chi(t)$, where χ is a character of W . A nontrivial character is positive on seven of the fifteen nonzero vectors and negative on eight. Thus the error minimum is seven, attained by any nontrivial character; the trivial character gives fifteen errors. Equivalently, with $S = \sum_{t \neq 0} Z_t$,

$$Z_t Z_u = -Z_{t+u} \quad (t \neq u), \quad S^2 = 15 - 14S. \quad (8.2)$$

Hence $S = 1$ or -15 , and the number of errors is seven or fifteen.

Corollary 8.3 makes this model arithmetic. An explicit realisation with basis primes $2, 5, 13, 37, 557$ is included in `data/fifteen_readings.csv`; each identity $n_i^2 + 1 = a_i u_i^2$ is checked exactly. Equation (8.2) uses the signs of the products, not only the inequalities saying that each target triple contains an error. It explains how seven errors can be forced while the capacity of *all* certificates is five.

9 Quadratic positivity can retain information that capacity loses

The previous example used a signed quadratic identity. Graphs give a reusable form of that mechanism, and show that it can coexist with the absence of information in many small observation sets.

9.1 Graph cuts realised by quadratic readings

Let $G = (V, E)$ be a finite simple graph. Choose the prime 2 and one prime q_v for each vertex v as in Lemma 8.2. Realise each edge uv by a distinct reading

$$A_{uv} = n_{uv}^2 + 1 = 2q_u q_v b_{uv}^2.$$

For $h(2) = -1$, put $s_v = h(q_v)$. The edge reading is $Z_{uv} = -s_u s_v$, and therefore

$$\mu_2(A) = |E| - \text{MaxCut}(G) = \min_{s \in \{-1, 1\}^V} \frac{1}{4} \sum_{uv \in E} (s_u + s_v)^2. \quad (9.1)$$

An edge subset is a target-two certificate exactly when it is Eulerian and has odd cardinality: every vertex prime cancels, while two remains odd. Every such subgraph contains an odd cycle. Replacing a certificate by an odd cycle contained in it cannot increase a load. Consequently

$$\text{Cap}_2(A) = \text{fractional packing value of the odd cycles of } G. \quad (9.2)$$

These equalities use all source assignments and all certificates on the sample.

The matrix inequality behind graph cuts is classical: see Delorme–Poljak [11] and the semidefinite primal–dual formulations in Goemans–Williamson [14, Section 4]. We use its equivalent form for monochromatic edges, with an additional budget on the multiplicative readings. In particular, the following weighted inequality does not require independent vertex signs. Suppose positive integers a_v and labelled readings $Q_{i(e)}$ satisfy

$$Q_{i(e)} t_e^2 = p a_u a_v r_e^2 \quad (e = uv).$$

Give edges weights $w_e \geq 0$ with $\sum_{e: i(e)=i} w_e \leq 1$ for every reading. Let $Q_w = D_w + A_w$ be the weighted signless Laplacian. If $Q_w - \text{diag}(b_v)$ is positive semidefinite, then for every $h(p) = -1$,

$$E_N(h) \geq \frac{1}{4} \sum_v b_v, \quad (9.3)$$

provided the readings lie in I_N . Indeed, with $s_v = h(a_v)$, the weighted error sum is $\frac{1}{4} s^T Q_w s$, while $s_v^2 = 1$. Shared prime factors between the a_v do not affect this argument. Formula (9.3) is a sufficient input for a proof on a prefix; no family of that strength on the full prefix is constructed here.

9.2 Bounded-degree samples with a growing gap

For a d -regular graph whose least adjacency eigenvalue is at least $-\rho$, (9.1) gives

$$\mu_2(A) \geq \frac{|V|(d - \rho)}{4} = \frac{|E|}{2} \left(1 - \frac{\rho}{d}\right).$$

If the girth is g , then every certificate has at least g edges, so $\text{Cap}_2(A) \leq |E|/g$.

The classical nonbipartite six-regular Ramanujan graphs provide an infinite family with

$$g > \frac{2}{3} \log_5 |V|, \quad \lambda_{\min} \geq -2\sqrt{5}.$$

We use the *starting graph* of Alon–Ganguly–Srivastava [1, beginning of Section 3], where this input is explicitly attributed to the Lubotzky–Phillips–Sarnak construction [18]. Their subsequently modified graph is not the input here. With $M = 3|V|$ edges, arithmetic realisation gives

$$\mu_2(A) \geq \frac{3 - \sqrt{5}}{6} M > \frac{M}{12}, \quad 1 \leq \text{Cap}_2(A) < \frac{3M}{2 \log_5(M/3)}. \quad (9.4)$$

Each free prime occurs in exactly six reading classes. The numerical inequality can also be witnessed rationally: if A_G is the adjacency matrix, then $A_G + 5I$ is positive definite, and

$$\frac{1}{4} s^T (6I + A_G) s = \frac{M}{12} + \frac{1}{4} s^T (A_G + 5I) s.$$

A rational LDL^T decomposition of the positive definite rational matrix gives a finite sum-of-squares certificate. This is degree two in the *prime sign variables*, not a degree-two consequence in unconstrained reading signs.

9.3 Why forest observations do not see the target sign

Take the vertex signs independently and fairly, and consider either target sign $\sigma = h(2)$. The readings on edges are $\sigma s_u s_v$. On every forest these readings are independent and fair under either value of σ : choose a root sign in each component, and the edge signs then determine all other vertex signs bijectively.

It follows that fewer than g distinct edge readings cannot distinguish the two target signs, even when each queried edge is chosen from the preceding answers. At every step the queried set is a forest, and the next new edge is conditionally fair under both hypotheses. Re-reading an edge gives the same sign, not fresh randomness. This local indistinguishability is compatible with (9.4); the latter uses the entire graph's prime-sign structure.

9.4 A finite graph with exact capacity and exact error minimum

The Hoffman–Singleton graph supplies a compact exact example. Use vertices $P_{i,j}$ and $Q_{i,j}$ for $i, j \in \mathbb{F}_5$. Join $P_{i,j}$ to $P_{i,j+1}$, $Q_{i,j}$ to $Q_{i,j+2}$, and $P_{i,j}$ to $Q_{k,ik+j}$ for all k . Edges are undirected. This is the usual pentagon–pentagram construction [6].

It has 50 vertices and 175 edges. If A is its adjacency matrix and J the all-ones matrix, direct counting gives

$$A^2 = 6I - A + J.$$

Set $C = 5A + 15I - J$. Then $C^2 = 25C$ and $C\mathbf{1} = 0$. For every sign vector s ,

$$\frac{1}{4} s^T (7I + A) s = 50 + \frac{\|Cs\|^2}{500} + \frac{(\sum_v s_v)^2}{20}. \quad (9.5)$$

Assigning $+1$ to every P -vertex and -1 to every Q -vertex attains fifty monochromatic edges, so the graph's actual error minimum is fifty.

The matrix identity says that adjacent vertices have no common neighbour and distinct nonadjacent vertices have exactly one. Thus there are no triangles or quadrilaterals. For an edge uv , each of the $6 \cdot 6$ choices $a \in N(u) \setminus \{v\}$ and $b \in N(v) \setminus \{u\}$ has a unique common neighbour c , giving a pentagon u, a, c, b, v . Conversely every pentagon through uv arises this way. Each edge therefore belongs to 36 pentagons, and the total number is $175 \cdot 36/5 = 1260$. Weight $1/36$ on every pentagon gives an odd-cycle packing of mass 35. Every odd cycle has length at least five, so the total load gives the reverse bound $175/5 = 35$. Thus its arithmetic realisations satisfy

$$\text{Cap}_2(A) = 35 < \mu_2(A) = 50.$$

The accompanying finite verifier constructs the graph, enumerates its pentagons, and checks both matrix identities in integer arithmetic. The transfer to 175 distinct integer readings is the existence result of Corollary 8.3; a list of those 175 potentially enormous indices is not supplied or claimed to have been generated.

10 Two families compose without loss; five need not

One can force errors by first writing the target prime class as a sum of several pivot classes. If the target sign is negative, at least one pivot is negative, and a disjoint family for that pivot already forces its full error count. Converting *all* the pivot families into direct certificates for the target is a stronger requirement. We now separate these two operations.

10.1 A lossless theorem for two families

Theorem 10.1 (Two-family composition). *Let a, b be square classes with $a + b = t \neq 0$. On a common labelled sample, let $\mathcal{A}$ be a family of M_a internally disjoint pairs of class a , and $\mathcal{B}$ a family of M_b internally disjoint pairs of class b . The families may overlap each other. Their existing labels contain at least $\min(M_a, M_b)$ disjoint certificates of class t , each of size two or four.*

The construction uses only a traversal of the two listed matchings. It introduces no new reading and does not increase the largest index when the sample is arithmetic.

Proof. Truncate both families to the same size $M = \min(M_a, M_b)$. Their union is an edge-coloured graph of maximum degree two. The colours alternate along every component. There is no edge in both families, because $a \neq b$.

Two endpoints at distance two along a component have class $a + b = t$. An alternating cycle has length divisible by four: summing all its edge classes gives $(\text{length}/2)t = 0$. Partition each consecutive block of four vertices into its two distance-two pairs. A cycle with $4k$ edges thus gives $2k$ disjoint target pairs.

For a path with L edges, partition successive blocks of four vertices in the same way. The four residue classes give the following outputs:

L	Target pairs already obtained	Unused data
$4k$	$2k$	one vertex
$4k + 1$	$2k$	one edge of the majority colour
$4k + 2$	$2k + 1$	one vertex
$4k + 3$	$2k + 2$	none

For $L = 4k + 2$, the last three vertices contribute their distance-two pair. Let b_a, b_b count the paths of length 1 modulo four whose majority colours are a, b , and let g_a, g_b count those of length 3 modulo four. Equality of the two total colour counts gives

$$b_a + g_a = b_b + g_b.$$

The target pairs already obtained number

$$M + \frac{g_a + g_b - b_a - b_b}{2}.$$

Pair a reserved a -edge with a reserved b -edge. Their four vertices form a target certificate; reserved edges lie in distinct components and are disjoint from all previous outputs. This adds $\min(b_a, b_b)$ certificates. The new total is

$$M + \min(g_a, g_b) \geq M.$$

All steps inspect each listed edge a bounded number of times. $\square$

The size-four output cannot simply be suppressed. The four readings at indices 5, 57, 4, 13 of $n^2 + 1$ are 26, 3250, 17, 170. The first pair has class five, the second class ten, and their product has class two. No proper subset has class two; the direct output must use all four readings. The theorem consequently cannot be iterated by treating its output as another family of pairs.

10.2 Sixteen readings with three different invariants

Start with independent classes $a, e_1, \dots, e_5$ and target $t = e_1 + \dots + e_5$. Use the sixteen readings indexed by subsets $S \subseteq \{1, \dots, 5\}$ of size at most two, with class

$$v_S = a + \sum_{j \in S} e_j. \quad (10.1)$$

For each i , there are five disjoint pairs of class e_i :

$$\{\emptyset, \{i\}\}, \quad \{\{j\}, \{i, j\}\} \quad (j \neq i).$$

If $h(t) = -1$, at least one $h(e_i)$ is negative, so its five pairs force at least five errors. The assignment $h(a) = +1$ and $h(e_i) = -1$ for every i attains exactly five, namely the singleton vertices. Thus $\mu_t = 5$.

Every target certificate has even cardinality, because its a -coordinate must cancel. It has no size-two instance, since the symmetric difference of two sets of size at most two cannot be all five indices. Hence its size is at least four, giving $\text{Cap}_t \leq 16/4 = 4$.

The reverse bound has a symmetric fractional witness. The target quartets fall into three types according to their subset sizes:

Sizes	Number	Weight per quartet
(0, 1, 2, 2)	15	1/15
(1, 1, 1, 2)	10	1/20
(1, 2, 2, 2)	50	1/20

The first type partitions the five indices into a singleton and two pairs; the second chooses three singletons and their complementary pair. For the third, fix its singleton i . Its three pair-edges must have odd degree at the other four indices and even degree at i . They are either

a three-edge star on the other four vertices (four choices), or a two-edge path centred at i and a disjoint edge (six choices). This gives ten quartets per singleton.

The empty vertex has load $15/15 = 1$. A singleton has loads $3/15$, $6/20$, and $10/20$, again summing to one. A pair vertex has loads $3/15$, $1/20$, and $15/20$; the last count follows either directly or by symmetry from $50 \cdot 3/10 = 15$. All loads are one, and the total weight is four. Therefore $\text{Cap}_t = 4$.

Three disjoint certificates are

$$\begin{aligned} &\{\emptyset, 1, 23, 45\}, \\ &\{2, 3, 4, 15\}, \\ &\{5, 12, 13, 14\}, \end{aligned}$$

where strings denote subsets. Four disjoint certificates would each have size four and partition all sixteen readings. But the sum of all sixteen classes is t : each e_i occurs five times and a occurs sixteen times. The sum of four target certificates would instead be $4t = 0$. Thus $\text{Pack}_t = 3$.

Theorem 10.2 (Five-family obstruction on actual readings). *There are sixteen distinct values $n_S^2 + 1$, all with $n_S < 10^{35}$, and five internally disjoint families of five pairs each, whose target classes sum to $[2]$, such that*

$$\text{Pack}_2 = 3 < \text{Cap}_2 = 4 < \mu_2 = 5.$$

All three invariants use the full family of certificates on the sixteen labels.

Proof. Use the independent prime basis $2, 5, 13, 17, 29, 37$ and set

$$a = [58], \quad (e_1, e_2, e_3, e_4, e_5) = ([754], [1073], [3770], [18241], [170]).$$

Their sum is $[2]$. Independence follows, for example, from the reverse expressions

$$[2] = \sum_i e_i, \quad [5] = e_1 + e_3, \quad [13] = a + e_1, \quad [17] = e_2 + e_4, \quad [29] = a + [2], \quad [37] = e_2 + [29].$$

Appendix C gives explicit positive integers n_S, u_S and squarefree c_S with $n_S^2 + 1 = c_S u_S^2$ and $[c_S] = v_S$. The indices are distinct and below the stated bound. This realises exactly the model (10.1), so all three values just proved carry over. The source negative precisely at $2, 13, 29$ among these six basis primes attains the five-error minimum. $\square$

The numerical witness can be checked entirely by integer multiplication, binary elimination, and rational load sums. No numerical linear-programming tolerance is required.

One may replicate every square class R times at distinct indices by odd powers of its negative-Pell solution. Every source then has exactly R copies of its old errors, giving $\mu_2 = 5R$. Lifting the quartet weights uniformly over all choices of copies gives capacity $4R$, and the size-four lower bound gives the reverse inequality. There are five pair families of size $5R$, and at least $3R$ disjoint direct certificates. We do not assert that the integral packing is exactly $3R$ after replication.

The obstruction does not classify three or four pair families, nor special families with additional arithmetic structure. It also leaves the five-error conclusion intact: one negative pivot supplies its own five disjoint pairs. For the same reason it is compatible with [22, Theorem 1.3 and Section 5]. That amplification selects a negative pivot and uses its family; it does not require simultaneous conversion of all pivot families into direct certificates for the target prime.

11 What a quantitative reconstruction argument must still supply

The obstructions proved here refer to three different operations. Restricting a table to windows or pairs can lose global multiplicative coherence. Restricting certificates to a narrow geometry or a small transport library can lose capacity. Replacing an integral cover by its fractional relaxation can lose part of the true error minimum even when *every* certificate is available.

The first operation is measured by the common-table construction, not by separate examples at different windows. The second is measured by unit loads on actual labels, not by the number of formal identities. The third is witnessed by real quadratic values, but on selected samples whose heights are not controlled by their cardinality. These distinctions explain why none of the negative results is a construction with $m_p(N) = o(N)$.

They also leave several precise possibilities open. A proof of a polynomial or linear lower bound for $m_p(N)$ could use genuinely global relations that the partially compatible tables fail. It could construct a sufficiently diverse nonlocal family with its loads paid at the original height. Or it could exploit positivity on actual prime signs, as in (9.3), rather than insist that certificate capacity equal the minimum. The selected graph samples show that the last mechanism can be stronger; they do not supply its missing full-prefix arithmetic input.

For composition, the two-family theorem gives a height-preserving positive result. The five-family example shows why that result is not a general associativity principle. Determining what additional structure permits further lossless composition is a separate question from improving the growth rate of $m_p(N)$.

Finite data and reproducibility. The reproducibility bundle is supplied inside the published source archive on Zenodo, <https://doi.org/10.5281/zenodo.23319030>. It contains the manuscript sources, frozen bibliography, standard-library Python checks, and reference CSV/JSON files. After extracting the ZIP, run

```
python3 checks/reproduce.py
```

This command rebuilds the finite data in an isolated temporary directory, compares all generated files byte for byte with the reference data, and runs the additional finite checks of the logarithmic baseline. It does not overwrite the supplied reference files. The expected principal outputs are:

Instance	Expected exact checks
Table with $N = 4096$, $H = 2$	12 287 readings, 252 negatives, 4 095 feasible windows; every pair covered by the exterior-class criterion
Fifteen quadratic readings	1 024 target subsets; $\text{Cap} = 5$, $\mu = 7$
Sixteen quadratic readings	1 024 target subsets, 75 quartets; $\text{Pack} = 3$, $\text{Cap} = 4$, $\mu = 5$
Hoffman–Singleton graph	50 vertices, 175 edges, 1 260 pentagons; $\text{Cap} = 35$, $\mu = 50$

The small gluing and centre examples are checked as well. For the graph, only the graph and matrix witnesses are generated, not its 175 Pell indices. Neither these tests nor the baseline checks prove asymptotic estimates. The archive manifest identifies this data revision and its files; SHA-256 hashes and reproduction commands are included in the published bundle.

AI assistance and responsibility. GPT-6 Astra assisted the research development, calculations, proof drafting, source consultation, and preparation of the original manuscript and

checker. GPT-6 Astra Pro assisted the reviews and revisions, including bibliographic cross-checks, proof exposition, and reproducibility packaging. The revision history is recorded in the source archive. The supplied reviews are AI reports, not human mathematical endorsements. The finite checker has been rerun for this edition; no Lean formalisation or independent human verification is claimed. The author is responsible for the submitted manuscript. Computational agreement concerns only the explicit finite objects and does not certify originality or the external theorems used in the proofs.

A Full freedom in logarithmic windows

The mesoscopic fibre theorem identifies exactly which coordinates remain forced after a large head is fixed. With a smaller head and a logarithmic number of readings, a different argument can show that *all* coordinates are free at almost every origin. This is not a consequence of the average exceptional-fraction bound, which permits a small nonzero number of forced coordinates.

Let $\mathcal{T}$ be a set of m distinct typed shifts (t, d) , with $0 \leq t \leq N$ and $d \in \mathcal{D}$. Let S contain s primes of arbitrary heights, and let

$$v_{t,d}^S(n) = (v_q((n+t)^2 - d) \bmod 2)_{q \notin S}.$$

Theorem A.1 (A growing full-rank window). *For all sufficiently large N , uniformly when $m + s \leq \log_2 N$,*

$$\#\{2 \leq n \leq N : \text{rank}_{\mathbb{F}_2}(v_{t,d}^S(n))_{(t,d) \in \mathcal{T}} < m\} \ll (m+1)^2 2^{m+s} \sqrt{N} \log(2N).$$

In particular, if $3L + s \leq (1/2 - \eta) \log_2 N$ for a fixed $0 < \eta < 1/2$, the three traces in an L -window are jointly free after fixing the signs on S , except at $O_\eta(N^{1-\eta} \log^3(2N))$ origins $2 \leq n \leq N$. The windows may extend to $N + L - 1$.

Proof. We use Heath-Brown's square-sieve principle [15]: a second moment of quadratic symbols detects a square class. The bounds below keep track of the varying number of factors and the protected prime set. A dependence on $r \geq 1$ selected rows means

$$F(n) = az^2, \quad F(T) = \prod_{j=1}^r ((T + t_j)^2 - d_j),$$

where a is squarefree and supported on S . We first prove uniformly in the selected shifts and in a that

$$\#\{2 \leq n \leq N : F(n) = az^2\} \ll (r+1)^2 \sqrt{N} \log(2N). \quad (\text{A.1})$$

Let $Q = \lceil \sqrt{N} \rceil$ and take as probes the primes $Q < \ell \leq 2Q$ that are outside S and do not divide $\text{disc } F$. From (5.4), with shift differences at most N , the number of excluded primes in this interval is $O(r^2 + s)$. The prime number theorem [21, (27.12.5)] therefore gives a probe set $\mathcal{P}$ with

$$M = |\mathcal{P}| \gg \sqrt{N} / \log(2N), \quad M \geq 20r,$$

for all sufficiently large N , uniformly in $r + s \leq \log_2 N$.

For any n under consideration, $F(n) \leq (5N^2)^r$, so at most $10r$ probes divide $F(n)$. Put $T(n) = \sum_{\ell \in \mathcal{P}} \left(\frac{aF(n)}{\ell} \right)$. If $F(n) = az^2$, every nonzero symbol is one and $T(n) \geq M/2$. Writing Z for the count in (A.1),

$$ZM^2/4 \leq \sum_{n=2}^N T(n)^2.$$

The diagonal contributes at most MN . For distinct probes ℓ, q , every complete Fourier coefficient of $\left(\frac{F(n)}{\ell}\right)\left(\frac{F(n)}{q}\right)$ modulo ℓq factors by the Chinese remainder theorem. The mixed character-sum estimate [19, Lemma 3.1 of the cited arXiv edition] gives

$$\left| \sum_{x \bmod \ell} \left(\frac{F(x)}{\ell}\right) e^{2\pi i u x / \ell} \right| \leq 2(2r+1)\sqrt{\ell} \quad (u \in \mathbb{Z}).$$

Its hypotheses hold because F is separable modulo ℓ , hence is not a square over the algebraic closure, and the multiplicative character is nonprincipal of order two. The additive coefficient $u = 0$ is allowed by this same hypothesis. Thus the product coefficient is $O((r+1)^2\sqrt{\ell q})$.

Completing the interval. Put $m_0 = \ell q$ and $b(x) = \left(\frac{F(x)}{\ell}\right)\left(\frac{F(x)}{q}\right)$, a periodic function modulo m_0 . Write $e_{m_0}(x) = \exp(2\pi i x / m_0)$ and $\hat{b}(u) = \sum_{x \bmod m_0} b(x) e_{m_0}(ux)$. Fourier inversion gives the exact identity

$$\sum_{n=2}^N b(n) = \frac{1}{m_0} \sum_{u \bmod m_0} \hat{b}(u) \sum_{n=2}^N e_{m_0}(-un).$$

Here $N < m_0 \ll N$. For $1 \leq u < m_0$, the geometric-sum bound is

$$\left| \sum_{n=2}^N e_{m_0}(-un) \right| \leq \min \left(N, \frac{1}{2\|u/m_0\|_{\mathbb{R}/\mathbb{Z}}} \right).$$

Consequently the sum of these bounds, divided by m_0 , is at most $\sum_{1 \leq u \leq m_0/2} 1/u + O(1) \ll \log(2m_0)$. The zero frequency contributes $(N-1)/m_0 \leq 1$ to the same normalised sum; it is not omitted. Combining this with $\max_u |\hat{b}(u)| \ll (r+1)^2\sqrt{m_0}$, and then restoring the two constant symbols involving a , gives

$$\left| \sum_{n=2}^N \left(\frac{aF(n)}{\ell}\right) \left(\frac{aF(n)}{q}\right) \right| \ll (r+1)^2\sqrt{N} \log(2N).$$

The factors involving a have modulus one because probes avoid S ; their size does not depend on the heights of those primes. Dividing the second-moment bound by M^2 proves (A.1).

There are 2^s choices of a and at most $2^m - 1$ nonempty row subsets. Sum (A.1) over them to obtain the theorem. A full row rank means that the columns outside S span every requested difference word. Choosing m independent columns realises any such difference by at most m prime flips. $\square$

For fixed L and S , a stronger but nonuniform conclusion is available:

$$\#\{2 \leq n \leq X : \text{rank}(v_{j,d}^S(n)) < 3L\} = O_{L,S}(\log(2X)). \quad (\text{A.2})$$

Indeed, products of at least two distinct shifted quadratics are separable of degree at least four. For each of the finitely many products and square classes supported on S , the Evertse–Silverman argument (5.5), with that class in place of p , gives finitely many integer solutions. Single-row dependences are norm equations, counted logarithmically by Lemma 2.1. Beyond the finite set supporting a multirow dependence, there cannot be two zero rows, since their sum would itself be a multirow dependence. The rank is then $3L$ or $3L-1$. No numerical last exceptional origin is extracted from this argument.

The full-rank assertions concern the set of good origins independently of the initial source and the requested word. They do not choose a single source realising arbitrary words at all those origins simultaneously.

B Every finite word can occur while measured entropy is zero

A further consequence of fixed-window freedom separates the richness of a language from the amount of statistical information in its frequencies. This construction produces one global source, unlike the separate window witnesses used earlier; it does not produce a nearly positive source.

Let $\beta_2(n) = (-1)^{v_2(n)}$, let $\mathcal{A} = \{-1, 1\}^3$, and write

$$a_h(n) = (h(n^2 + 1), h(n^2 + 2), h(n^2 - 2)), \quad n \geq 2.$$

Theorem B.1 (A full language with zero measured entropy). *For every $\varepsilon > 0$ and $B_0 \geq 2$, there is a set of primes $\Gamma \subset (B_0, \infty)$ and a single source*

$$h(n) = \beta_2(n)(-1)^{\sum_{q \in \Gamma} v_q(n)}$$

such that

$$\sum_{q \in \Gamma} q^{-1/2} < \varepsilon, \quad \sum_{q \in \Gamma} q^{-t} < \infty \quad \text{for every } t > 0.$$

Every finite word over $\mathcal{A}$ has a positive natural frequency in a_h , and its logarithmic frequency is the same. The empirical stationary measure is ergodic, has rational discrete spectrum, and has entropy zero. Its support is nevertheless the full shift, whose topological entropy is $\log 8$. Each individual trace has mean zero; in particular $E_N(h) = (3/2 + o(1))N$.

Proof. We first record a uniform continuity bound. For any two sources f, g , the fraction of origins $2 \leq n \leq X + 1$ where their words of width L differ is at most

$$C_L \sum_{q: f(q) \neq g(q)} q^{-1/2}, \quad C_L = 3L(2L + 6). \quad (\text{B.1})$$

A disagreement requires a changed prime dividing one of the $3L$ readings. An odd prime has at most two roots modulo q , so meets at most $2X/q + 2$ origins per reading. If it meets any, then $q \leq (X + L)^2 + 2 \leq (L + 2)^2 X^2$, and $2/q + 2/X \leq (2L + 6)/\sqrt{q}$. The prime two satisfies the same upper bound. Union over the primes and readings proves (B.1).

A source with finitely many negative primes gives a rationally almost periodic sequence: truncate the valuations of those primes at a large exponent to obtain a periodic approximation, with disagreement density tending to zero. Simple roots modulo odd prime powers have density at most $2/q^k$; the valuation at two in these traces is already zero or one. Every finite word then has a frequency. If a word of width L occurs at r , it persists on the progression modulo

$$W = \prod_{q \text{ negative}} q^{1 + \max_{0 \leq j < L, d \in \mathcal{D}} v_q(Q_d(r+j))},$$

so its frequency is at least $1/W$.

Enumerate all nonempty finite words as w_j , of lengths L_j . Starting from $h_0 = \beta_2$, choose a positive rational $b_0 < \varepsilon/2$ and let $\sigma_j = \min(1/2, 1/j)$. At stage j , choose B_j larger than B_0 , all previously changed primes, and all the integer readings in previously planted words, and large enough that

$$3L_j B_j^{-\sigma_j} \leq b_{j-1}/2.$$

Use (A.2) with all primes through B_j protected to find an origin where the $3L_j$ rows have full rank. Flip at most $3L_j$ primes above B_j to plant w_j . These are new primes, previously positive, so the negative support grows by a finite set F_j . Its cost satisfies

$$\sum_{q \in F_j} q^{-1/2} \leq \sum_{q \in F_j} q^{-\sigma_j} \leq b_{j-1}/2.$$

Let W_j be the progression modulus for the newly planted word in the finite-support source h_j , and reserve

$$b_j = \min(b_{j-1}/2, 1/(2C_{L_j}W_j)).$$

All these decisions use only already constructed finite data. Searching for the next full-rank origin terminates by (A.2), without any asserted practical bound.

The union $\Gamma = \bigcup_j F_j$ defines one source. Later changes cannot alter a previously planted word at its original location, because their primes exceed all its values. More importantly, their total half-power cost after stage j is at most b_j . For every fixed $t > 0$, eventually $\sigma_j \leq t$, so the same summable stage bounds prove $\sum_{\Gamma} q^{-t} < \infty$. The total half-power cost is at most $b_0 < \varepsilon$.

By (B.1), a_h is a limit in disagreement density of finite-support, hence periodically approximable, sequences. Periodic approximation makes the frequency of every fixed word a Cauchy limit. Its logarithmic frequency agrees by summation by parts. For the word w_j , the tail can remove a density at most $C_{L_j}b_j$, leaving

$$\nu_h(w_j) \geq 1/W_j - C_{L_j}b_j \geq 1/(2W_j) > 0.$$

The word frequencies are not uniform in j and are not equal to 8^{-L_j} .

Each finite-support h_j is negative at two and at finitely many odd primes. In a periodic valuation truncation, the odd-prime conditions are independent of the parity of the index by the Chinese remainder theorem. The sign supplied by two alternates on each trace, so each trace mean is zero. Remove the truncation and then use (B.1) to pass to h .

The structural conclusion is the classical theorem on rationally almost periodic sequences [4, Theorem 1.7]: their empirical measure is ergodic with rational discrete spectrum. In this example the reason can also be seen directly. On the profinite integers with Haar measure, translation by one is ergodic with rational discrete spectrum. For each fixed shift, $\sum_{q \in \Gamma} 2/q < \infty$ makes the odd-prime correction a well-defined measurable product almost everywhere. It codes a factor of this rotation. Finite-support Chinese-remainder calculations and (B.1) identify its cylinder laws with the empirical frequencies just constructed.

Here is a direct entropy bound. If a periodic sequence of period T approximates a_h in disagreement density at most $\delta < 1/2$, take a stationary limiting coupling with its phase. A block of length m is specified by the phase, its error positions, and at most seven alternative symbols at each error. With base-two entropy,

$$H_\mu(a(0), \dots, a(m-1)) \leq \log_2 T + m(H_2(\delta) + \delta \log_2 7).$$

Divide by m , let m tend to infinity, and then let δ decrease to zero. This proves zero measured entropy. Every one of the 8^m words has positive frequency, so the language is the full shift and its topological entropy is $\log 8$. $\square$

The distinction between topological and measured entropy in rationally almost periodic systems is classical; see also [4, Section 3.1]. The construction above realises it simultaneously on these three traces with a protected head and a support summable in every positive power.

The dependence can be visible already at distance one. The density Δ_d where $h(Q_d(n))$ differs from $\beta_2(Q_d(n))$ satisfies

$$\Delta_d \leq \sum_{q \in \Gamma} \frac{\rho_d(q)}{q+1} \leq 2 \sum_{q \in \Gamma} \frac{1}{q} < 2\varepsilon,$$

where $\rho_d(q)$ is the number of roots of Q_d modulo q . The local factor $\rho_d(q)/(q+1)$ is obtained by summing the odd valuation probabilities of the simple roots. The finite-support formula

passes to Γ using (B.1), not an uncontrolled infinite sum of congruence errors. Since each β_2 trace alternates,

$$\lim_{X \rightarrow \infty} \frac{1}{X} \sum_{n=2}^{X+1} h(Q_d(n))h(Q_d(n+1)) \leq -1 + 4\Delta_d < -1 + 8\varepsilon.$$

Thus positive frequencies for every word, even with balanced one-coordinate marginals, do not imply independent or Bernoulli statistics.

C The sixteen-reading arithmetic witness

The row labels refer to the subsets used in Section 10.2. The two tables give $n_S^2 + 1 = c_S u_S^2$ exactly. Splitting the indices and square factors into separate tables keeps the integers legible.

S	c_S	n_S
$\emptyset$	58	99
1	13	18
2	74	43
3	65	8
4	1258	114669
5	2465	34208
12	13949	505872859718
13	290	17
14	237133	37467803169731567258356998326647518
15	2210	47
23	69745	8539575550866247307711088
24	986	157
25	3145	1344783432
34	1185665	918139433921728
35	442	21
45	185	68

S	u_S
$\emptyset$	13
1	5
2	5
3	1
4	3233
5	689
12	4283214685
13	1
14	76941780537374507308269877334405
15	1
23	32335512290115324082601
24	5
25	23979605
34	843194258497
35	1
45	5

The exact verifier finds 1024 target-two subsets, of sizes 4, 6, 8, 10, 12, 16, in numbers 75, 216, 435, 232, 65, 1 respectively. These counts are an additional finite check; the proofs of $\text{Pack} = 3$, $\text{Cap} = 4$, and $\mu = 5$ in Section 10.2 do not require exhaustive enumeration. The CSV file includes the same square factors and classes, and the fractional packing file lists all 75 quartets with their rational weights.

References

- [1] N. Alon, S. Ganguly, and N. Srivastava. *High-girth near-Ramanujan graphs with localized eigenvectors*. arXiv:1908.03694v1, 2019. Input: the unmodified starting graph at the beginning of Section 3, attributed there to Lubotzky–Phillips–Sarnak.
- [2] P. Alvanos, Y. Bilu, and D. Poulakis. Characterizing algebraic curves with infinitely many integral points. *International Journal of Number Theory* **5**(4) (2009), 585–590. doi:10.1142/S1793042109002274. Locators: arXiv:0907.2097v1, introduction and Theorem 1.2.
- [3] M. Bardestani and T. Freiberg. *Mertens’s theorem for splitting primes and more (A concise and adaptable proof of Hardy)*. arXiv:1309.7482v1, 2013. Theorem 3.3; only fixed-modulus progressions are used.
- [4] V. Bergelson, J. Kułaga-Przymus, M. Lemańczyk, and F. K. Richter. Rationally almost periodic sequences, polynomial multiple recurrence and symbolic dynamics. *Ergodic Theory and Dynamical Systems* **39**(9) (2019), 2332–2383. doi:10.1017/etds.2017.130. Locators: arXiv:1611.08392v2, Theorem 1.7 and Section 3.1.
- [5] R. de la Bretèche, V. Y. Wang, and M. W. Xu. *Random Multiplicative Functions and Making Squares from Polynomial Values*. arXiv:2607.06398v1, 2026. Lemmas 3.1–3.4, equation (13), and Proposition 5.1.
- [6] A. E. Brouwer. *Hoffman–Singleton graph*. Author’s graph notes, pentagon–pentagram construction; accessed 27 September 2026.
- [7] W. Castryck, R. Cluckers, P. Dittmann, and K. H. Nguyen. The dimension growth conjecture, polynomial in the degree and without logarithmic factors. *Algebra & Number Theory* **14**(8) (2020), 2261–2294. doi:10.2140/ant.2020.14.2261. Locator: Theorem 3 of arXiv:1904.13109v1.
- [8] J. Chinis and B. Shala. Random Chowla’s conjecture for Rademacher multiplicative functions. *Transactions of the American Mathematical Society* **378** (2025), 8025–8053. doi:10.1090/tran/9457. Locators: arXiv:2409.05952v2, Lemmas 2.4–2.5 and proof.
- [9] K. Conrad. *Pell’s Equation, I*. Author’s notes, Theorem 2.3 and multiplication of solutions; accessed 27 September 2026.
- [10] G. Cornuéjols. *Combinatorial Optimization: Packing and Covering*. CBMS-NSF Regional Conference Series in Applied Mathematics 74, SIAM, 2001. doi:10.1137/1.9780898717105. The port definition is in the author’s July 2000 notes, Section 8.3.1, p. 120; this locator refers to those notes, not the SIAM pagination.
- [11] C. Delorme and S. Poljak. Laplacian eigenvalues and the maximum cut problem. *Mathematical Programming* **62** (1993), 557–574. doi:10.1007/BF01585184.
- [12] J. Edmonds and E. L. Johnson. Matching, Euler tours and the Chinese postman. *Mathematical Programming* **5** (1973), 88–124. doi:10.1007/BF01580113. Author-institution record.
- [13] J.-H. Evertse and J. H. Silverman. Uniform bounds for the number of solutions to $Y^n = f(X)$. *Mathematical Proceedings of the Cambridge Philosophical Society* **100**(2) (1986), 237–248. doi:10.1017/S0305004100066068. Theorem 1(b); original text in the CWI repository.

- [14] M. X. Goemans and D. P. Williamson. Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming. *Journal of the ACM* **42**(6) (1995), 1115–1145. doi:10.1145/227683.227684. Author’s copy, Section 4, especially Sections 4.2–4.3.
- [15] D. R. Heath-Brown. The square sieve and consecutive square-free numbers. *Mathematische Annalen* **266**(3) (1984), 251–259. doi:10.1007/BF01475576.
- [16] K. S. Kedlaya. *Notes on analytic number theory*. Chapter 13: The Selberg sieve, especially Theorem 13.1 and (13.2.3). Author’s online notes; accessed 27 September 2026.
- [17] F. Lemmermeyer. *Higher Descent on Pell Conics. I. From Legendre to Selmer*. arXiv:math/0311309, 2003. Section 5, Proposition 5.3.
- [18] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica* **8** (1988), 261–277. doi:10.1007/BF02126799. The specialised starting-graph statement is located in [1, Section 3].
- [19] L. Mérai, I. E. Shparlinski, and A. Winterhof. Character sums over sparse elements of finite fields. *Bulletin of the London Mathematical Society* **56**(4) (2024), 1488–1510. doi:10.1112/blms.13008. Input: Lemma 3.1 of arXiv:2211.08452v1.
- [20] J. S. Milne. *Algebraic Number Theory*. Version 3.08, 19 July 2020. Chapters 3–5, especially Propositions 4.1–4.2.
- [21] National Institute of Standards and Technology. *Digital Library of Mathematical Functions*. Section 27.12: Asymptotic formulas—primes, equations (27.12.5) and (27.12.8), and the preceding statement of Dirichlet’s theorem. Accessed 27 September 2026.
- [22] B. Pouly. *Arithmetic reconstruction and error recovery from three quadratic traces*. Zenodo, 2026. doi:10.5281/zenodo.23317860. Theorems 1.1 and 1.3, and Section 5.
- [23] B. Pouly. *Selective normality and algebraic rigidity of multiplicative traces*. Zenodo, 2026. doi:10.5281/zenodo.23318326. Lemma 2.1.