

Arithmetic reconstruction and error recovery from three quadratic traces

Brice Pouly*

Abstract

We study completely multiplicative sign functions h through their values at positive integers of the forms $n^2 + 1$, $n^2 + 2$ and $n^2 - 2$, with observed indices $1 \leq n \leq N$. First occurrences of prime factors give a canonical information set and a complete, prefix-compatible family of parity relations, each involving at most $\lfloor \log_2 N \rfloor + 3$ readings. These relations yield exact bounded-distance repair, including corrupted information coordinates, in time $N^{O(1)}(4 + \lfloor \log_2 N \rfloor)^t$ for t errors; erasures enter through an explicit rank parameter. We then construct arithmetic redundancy without estimating a quadratic regulator. If $h(p) = -1$ and $K = \log N / \log \max(3, p)$, the three traces contain at least $\exp(\exp(c \log K / \log \log K))$ negative readings for every fixed $0 < c < \log 2$ and sufficiently large K , uniformly in the prime p and all other prime signs. The same number of each sign occurs on one trace between N^α and N , for each fixed $\alpha < 1$. The proof combines short reconstruction certificates, Lehmer divisibility and balanced divisors. Coprime blocks give compact access to these families without factoring large recurrence terms. Under independent reading noise with fixed erasure probability $0 \leq a < 1$ and conditional flip probability $0 \leq b < 1/2$, every source prefix $P = \lfloor \exp((\log N)^\delta) \rfloor$, for fixed $0 < \delta < 1$, is recoverable from $O(P)$ readings with polynomially small failure probability in P and preparation polynomial in the numerical P and $\log N$. A fixed positive erasure rate nevertheless leaves exponentially many assignments of observed large-prime signs. No positive-density inverse for unrestricted sources is asserted.

Contents

1	What can be recovered from quadratic readings?	2
2	A complete arithmetic presentation	6
3	Repair without trusting the pivots	9
4	Replicating a pivot without a regulator	12
5	Balanced divisors and uniform amplification	13
6	Compact families without factoring large recurrence terms	17
7	Direct prime certificates on a prescribed trace	19
8	Recovering true signs under independent reading noise	21
9	How much information remains hidden	26
10	The boundary between reconstruction and a statistical inverse	29
A	Exact elimination and localisation of large factors	30
B	Linear separation under a local prime budget	32
C	A minimum under a cardinality constraint	34
D	Sources close to a moving quadratic character	37
	Computational material and AI assistance	40
	References	41

*Research and manuscript preparation assisted by GPT-6 Astra. Details of the assistance and the scope of the computational checks appear at the end of the article.

1 What can be recovered from quadratic readings?

A completely multiplicative sign function is determined by one sign at each prime. Reading its values along a polynomial does not ordinarily display those signs separately: one observation contains the product of the signs of several prime factors. The question here is whether three particularly simple observation sequences retain enough arithmetic structure to undo that multiplication, and how much of this structure survives incorrect or missing readings.

Throughout the article,

$$\mathcal{D} = \{-1, -2, 2\}, \quad Q_d(n) = n^2 - d,$$

and $\mathcal{M}^\pm$ denotes the set of completely multiplicative functions from $\mathbb{N}_{\geq 1}$ to $\{\pm 1\}$. We observe the labelled set

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

It has $3N - 1$ elements. Labels remain distinct when their integer values coincide; this convention matters both for an adversarial error budget and for independent reading noise. The observation of h is the word $(h(Q_i))_{i \in I_N}$, and the set of all such words is $\mathcal{C}_N$.

Three different tasks arise. A *recognition* procedure decides whether a proposed word belongs to $\mathcal{C}_N$. A *repair* procedure finds a nearby member of $\mathcal{C}_N$. A *recovery* procedure determines a value of the source that actually produced the observations. The first two tasks do not imply the third: several genuine sources may lie within the declared error budget.

1.1 A calculation that produces redundancy

There is a useful way to repeat information without reading the same label twice. From

$$7^2 + 1 = 2 \cdot 5^2$$

we obtain the three identities

$$\begin{aligned} (8^2 + 1)(57^2 + 1) &= 2 \cdot 325^2, \\ (9^2 + 1)(32^2 + 1) &= 2 \cdot 205^2, \\ (12^2 + 1)(17^2 + 1) &= 2 \cdot 145^2. \end{aligned}$$

For every $h \in \mathcal{M}^\pm$, the product of the two readings in any row is $h(2)$. The six labels are distinct, so $h(2) = -1$ forces three negative and three positive readings. Majority vote among the three products recovers $h(2)$ after one incorrect reading. No small-prime signs have been supplied to the observer, and the central reading at 7 is not used by these three certificates.

The general identity behind this calculation is

$$\begin{aligned} m^2 - d &= Du^2, & ab &= Du^2, & x &= m + a, & y &= m + b, \\ Q_d(x)Q_d(y) &= D[u(x + y)]^2. \end{aligned} \quad (1.2)$$

Counting divisors alone is not enough: the resulting indices must fit below N , and different certificates must not repeatedly use the same readings. Balanced divisors will pay both costs. Before applying this identity, however, we need a way to express an arbitrary target prime through suitable values D .

1.2 Exact presentation and bounded-distance repair

The choice of three curves ensures that every prime is encountered. For an odd prime q , the product of the Legendre symbols of -1 , -2 and 2 is $(4/q) = 1$, so at least one of the three

quadratics has a root modulo q . The values 2 and 3 are already read at index one. Lemma 2.1 turns this coverage into a positive reading with a smaller cofactor.

Let $\mathcal{P}_N$ be the primes dividing at least one value in (1.1). For each prime q , select the first positive quadratic reading divisible by q . These *pivots* form a canonical information set. Their arithmetic, rather than a generic elimination procedure, controls the size of the relations.

Theorem 1.1 (Complete short presentation). *For $N \geq 2$, there is a prefix-compatible collection of $3N - 1 - |\mathcal{P}_N|$ independent square-product relations on I_N , each involving at most*

$$\ell_N = \lfloor \log_2 N \rfloor + 3$$

labels. A sign word belongs to $\mathcal{C}_N$ if and only if it satisfies these relations. Its pivot values determine all relevant prime signs uniquely. In particular, the noiseless observations determine $h(m)$ for every $m \leq 2N + 1$.

The construction and proof occupy Section 2. The result is more than injectivity of the infinite observation: it supplies all constraints in the original finite prefix. As a consequence, one can repair data without assuming that any of the information coordinates are trustworthy.

Theorem 1.2 (Exact repair). *Given a word on I_N , a nonnegative integer t , and prescribed signs on any subset of $\mathcal{P}_N$, one can decide whether a compatible source differs from the word at at most t labels in time*

$$N^{O(1)}(1 + \ell_N)^t. \quad (1.3)$$

A positive answer supplies a source and its corrections; a negative answer supplies a verifiable finite search tree. With erasures, replace ℓ_N in (1.3) by $(r + 1)\ell_N$, where r is the rank of the erased pivot columns after the equations belonging to erased non-pivots have been removed.

Here polynomial time means polynomial in the numerical length N of the supplied table. Factoring the observed integers, each at most $N^2 + 2$, is included in this bound. The error parameter concerns readings, not negative prime signs. Section 3 also decides which prime signs are forced and when the correct answer is ambiguity.

1.3 A uniform lower bound for an unrestricted source

To quantify the distinction between injectivity and stability, set

$$E_N(h) = \sum_{i \in I_N} \mathbf{1}_{h(Q_i)=-1}, \quad m_p(N) = \min_{\substack{h \in \mathcal{M}^\pm \\ h(p)=-1}} E_N(h). \quad (1.4)$$

All prime signs other than $h(p)$ are free, and the minimising function may change with N . For $K > e$ and $c > 0$, write

$$\Phi_c(K) = \exp\left(\exp\left(c \frac{\log K}{\log \log K}\right)\right). \quad (1.5)$$

Unless a base is displayed, logarithms are natural.

Theorem 1.3 (Uniform separation on a terminal range). *Fix $\alpha < 1$ and $0 < c < \log 2$. There exists $K_0(\alpha, c)$, independent of the prime p , with the following property. Put*

$$B_p = \max(3, p), \quad K = \frac{\log N}{\log B_p}.$$

If $K \geq K_0(\alpha, c)$ and $h \in \mathcal{M}^\pm$ satisfies $h(p) = -1$, then some $d \in \mathcal{D}$ satisfies, for each $v \in \{\pm 1\}$,

$$\#\{N^\alpha < n \leq N : h(Q_d(n)) = v\} \geq \Phi_c(K). \quad (1.6)$$

Consequently $m_p(N) \geq \Phi_c(K)$.

The trace d in this statement can depend on h . The underlying families of integer identities do not. For two arbitrary sources f, g with $f(p) \neq g(p)$, apply the theorem to $h = fg$: it gives the same lower bound for their disagreements on one trace, together with the same number of agreements.

A short reconstruction certificate writes $h(p)$ as a product of pivot readings. At least one pivot is negative. Each pivot has an explicit norm-one unit of height controlled by p , even when its squarefree part is a large composite integer. Lehmer divisibility supplies many coprime factors of a later recurrence term; balanced divisors then produce many disjoint pairs carrying the sign of that pivot. Selecting one negative pivot avoids a loss from summing overlapping families. Section 5 makes this argument uniform in p and pays the height of every reading.

At fixed p , the lower bound exceeds every fixed power of $\log N$ and is smaller than every positive power of N . This describes the *bound*, not the actual order of $m_p(N)$. In particular, (1.6) does not establish a positive-density inverse from vanishing error proportions.

1.4 Noise, compact computation and the information that remains missing

Arithmetic redundancy has a statistical consequence even though the source is arbitrary. Under independent erasures and sign flips attached to labels, the amplified pairs recover all prime signs through

$$P = \left\lfloor \exp((\log N)^\delta) \right\rfloor, \quad 0 < \delta < 1 \text{ fixed},$$

with failure probability at most P^{-A-1} for any fixed $A \geq 1$. Corollary 8.2 uses $O(P)$ distinct readings and preparation polynomial in the numerical P and $\log N$. It corrects each pivot using pair products before performing the triangular reconstruction; overlaps between different pivot families are paid by a union bound.

Section 8 retains two complementary routes. Elementary replication has an explicit finite height bound, gives a simultaneous prefix $\exp(c_1 \sqrt{\log N})$, and recovers a separately requested prime as large as $\exp(c_2 \log N / \log \log N)$ with $O(\log N)$ readings. Direct Pell repetitions retain a smaller prime range for which both queries and preparation are polylogarithmic in N . Table 1 distinguishes these costs and quantifiers.

These recoveries cannot identify every prime sign appearing in the observations. With a fixed positive erasure rate, even an oracle revealing all signs at primes at most $2N$ leaves an exponential number of compatible assignments at the larger primes. Section 9 gives the exact finite fibre and a corresponding statistical obstruction in the presence of flips. Section 6 treats a different cost: enormous families of certificates can have compact, polynomially accessible descriptions without requiring factorisation of enormous Lehmer terms. A compact description is not a collected table of readings.

1.5 Related work and the organisation of the proofs

The arithmetic results most relevant here concern first prime appearances, repeated square classes, and signs at quadratic arguments. Everest, Stevens, Tamsett and Ward [7, Lemma 4.1

and Proposition 4.2] relate primitive prime divisors of $n^2 + \beta$ to the inequality $q > 2n$, outside the initial exceptional terms. Their Theorem 5.1 also gives the large-factor counting input used in Section 9; Lemma 9.1 is a specialisation, with its logarithmic-mass proof included. The extra property in Theorem 2.4 is a *complete* independent presentation of the three-trace prefix, compatible with enlargement and with logarithmic row width. First appearances alone do not state that conclusion.

Pell repetition of a represented square class already appears in the study of multiplicative signs. Borwein, Choi and Ganguli [4, Theorem 2.2] show how a solution of a quadratic equation $F(n) = \ell m^2$ generates infinitely many positive solutions under their hypotheses. This is an arithmetic mechanism, and so repeats the value of any completely multiplicative sign function, not only Liouville. Our use in Section 4 starts from a pivot whose own explicit unit gives a uniform height bound; Section 5 adds enough internally disjoint pairs to obtain Theorem 1.3.

For the particular source λ , Srinivasan [14, Theorem 1.3] proves infinitely many sign changes on $n^2 + d$ for every nonzero integer d . Theorem 1.3 instead concerns the minimum over all sources with only $h(p) = -1$ prescribed, including sources and target primes varying with N . Thus the issue is uniform quantitative separation, not the first qualitative occurrence of both Liouville signs. A nearby but different use of square-product equations is the work of de la Bretèche, Wang and Xu [6]: their counts yield limit laws for random multiplicative functions. Here the source is arbitrary, the separation theorem is deterministic, and in Section 8 randomness enters only through reading errors.

Systematic parity checks and distance-based error correction belong to classical coding theory [9]; bounded branching on a violated constraint and repetition voting are standard operations. The concentration estimate is Hoeffding’s [10], with its required specialisation proved below. These operations consume the short arithmetic presentation and the height-controlled repetitions; they do not supply them. The norm equations use Lagrange’s theorem and, only in the direct prime-class route, the analytic class number formula; see Conrad [5] and Sutherland [15]. The primitive-divisor input is [3, Theorem 1.4]; the real-pair result of Carmichael–Ward, recorded there as Theorem A, already suffices. We keep the conservative threshold thirty throughout. The gcd refinement in the compact construction lies in the classical subject studied by Bernstein [2]; no complexity bound from that paper is imported.

The two central arithmetic statements are the complete short presentation in the original prefix and the regulator-free amplification uniform in the target prime. Certified repair, noisy recovery and the information bounds describe consequences and limitations of this structure. They are not claims to a general nearest-codeword algorithm or to a positive-rate code for all multiplicative sources.

The appendices are complementary, not inputs to Theorem 1.3. Appendix A eliminates the largest factors exactly before localising the remaining conflict. Appendix B uses smooth quadratic values in fixed progressions, through [16, Definition 2.8 and Proposition 2.10], to obtain linear bounds for mobile sources under a local harmonic budget. Its relation to the fixed-source pretentious theorem [16, Theorem 2.9] is explained there, with admissibility retained. Appendices C–D give controlled prime-complexity and moving-character classes, using the stated Kubilius input of Gorodetsky [8, Theorem 2.3] and a mixed Weil bound [11, Lemma 3.1]. None of these structural assumptions is inferred from a small unrestricted error count.

Reading routes. For exact reconstruction, follow Sections 2–3. The uniform separation proof runs from Section 4 to Section 5; Section 7 instead fixes the trace from the target prime. For noisy observations, Section 6 supplies compact access and Sections 8–9 compare recovery with hidden information.

2 A complete arithmetic presentation

The first task is to expose every prime sign using readings that are already in the supplied prefix. A root modulo a prime gives a small cofactor; ordering these roots by their first occurrence makes the resulting reconstruction triangular.

2.1 First occurrences introduce one prime at a time

For a prime q , let $\nu(q)$ be the least positive index at which q divides a positive $Q_d(n)$. Let $b(q)$ denote the corresponding label, called the pivot of q . The exceptional initial pivots are

$$b(2) = (1, -1), \quad b(3) = (1, -2).$$

We write $D_q = Q_{b(q)} = qc_q$, so that $c_2 = c_3 = 1$.

The relation between first appearances of a prime in a quadratic sequence and a centred root is classical; see [7, Lemma 4.1 and Proposition 4.2] for a single sequence $n^2 + \beta$ outside its initial exceptions. The following three-trace formulation also tracks when the cofactor primes have appeared, which is needed for a presentation contained in the same finite prefix.

Lemma 2.1 (Small cofactors at first occurrence). *Every prime has a pivot. For $q \geq 5$, its type is unique, and*

$$2\nu(q) < q, \quad D_q = qc_q, \quad 1 \leq c_q < q/4. \quad (2.1)$$

The valuation of q in D_q is one. Every prime factor of c_q has appeared at a strictly smaller index than $\nu(q)$, and a label is the pivot of at most one prime.

Proof. The product of the three Legendre symbols is

$$\left(\frac{-1}{q}\right) \left(\frac{-2}{q}\right) \left(\frac{2}{q}\right) = \left(\frac{4}{q}\right) = 1.$$

At least one symbol is $+1$. Its centred root $1 \leq r \leq (q-1)/2$ gives a nonzero multiple $r^2 - d$ of q . This multiple is positive: the only negative value possible is -1 , which is not divisible by q . At the first occurrence,

$$0 < D_q \leq (q-1)^2/4 + 2 < q^2/4.$$

This proves (2.1) and the assertion about the valuation.

Put $n = \nu(q) \geq 2$. Since $q \geq 2n + 1$,

$$c_q \leq \frac{n^2 + 2}{2n + 1} < n.$$

A prime factor r of c_q is less than n . Its own centred-root argument, or the initial pivots when $r = 2, 3$, places its first occurrence before n . Two new primes at this label would each exceed $2n$ and have product greater than $n^2 + 2$, which is impossible. Finally, two types at the same index have values differing by 1, 3 or 4, so cannot both be divisible by $q \geq 5$. $\square$

Set $\mathcal{B}_N = \{b(q) : q \in \mathcal{P}_N\}$. Order the relevant primes increasingly. The valuation matrix of the D_q is triangular with diagonal entries one, over $\mathbb{Z}$ and hence over $\mathbb{F}_2$. In particular, the pivot readings may be assigned arbitrarily. They determine a unique assignment on $\mathcal{P}_N$ through

$$h(q) = w_{b(q)} h(c_q). \quad (2.2)$$

Signs outside $\mathcal{P}_N$ are unrestricted and do not affect the observed word. This is the precise information-set property used below.

2.2 A short descent in square classes

For $a \geq 1$, define

$$\text{core}(a) = \prod_{q: v_q(a) \text{ odd}} q.$$

This is the squarefree kernel, not the product of all distinct prime divisors. Suppose the prime factors of a belong to $\mathcal{P}_N$. Start at $a_0 = \text{core}(a)$. If the current value is greater than one, take its largest prime factor q , record $b(q)$, and replace it by

$$a_{j+1} = \text{core}\left(\frac{a_j}{q} c_q\right). \quad (2.3)$$

For $q \geq 5$, the essential gain is

$$a_{j+1} \leq (a_j/q) c_q < a_j/4. \quad (2.4)$$

The largest prime strictly decreases. The recorded labels therefore form a set, denoted $B(a)$, rather than a multiset.

Proposition 2.2 (Short reconstruction certificates). *If $a_0 > 1$, the descent gives*

$$|B(a)| \leq \lfloor \log_4 a_0 \rfloor + 2, \quad a_0 \prod_{j \in B(a)} Q_j \text{ is a square.} \quad (2.5)$$

For $a_0 = 1$, take $B(a) = \emptyset$. In particular, for a prime $p \in \mathcal{P}_N$,

$$\prod_{j \in B(p)} Q_j = p z_p^2, \quad s_p := |B(p)| \leq \min(\lfloor \log_4 p \rfloor + 2, \lfloor \log_2 p \rfloor), \quad (2.6)$$

with an integer $z_p \geq 1$.

Proof. Every step in (2.3) multiplies the current square class by the class of $D_q = q c_q$ and cancels its largest prime coordinate. The alternative bound $|B(a)| \leq \lfloor \log_2 \text{core}(a) \rfloor$ follows by induction from (2.4): the terminal values 1, 2, 3, 6 require 0, 1, 1, 2 steps, respectively, each at most its binary logarithm. After $k > 0$ steps with $q \geq 5$, the remaining positive integer is less than $a_0/4^k$. Thus there are at most $\lfloor \log_4 a_0 \rfloor$ such steps. At most two terminal steps remove the primes 2 and 3. At termination the square class is trivial. For a prime target, the product in (2.6) has the parity vector of p ; division by p therefore leaves a positive integer square. $\square$

The reduction by a factor greater than four explains the logarithmic relation length. Its use of square classes is specific to signs; it must not be substituted without change into a statement about arbitrary complex phases.

Remark 2.3 (Noiseless recovery beyond the index range). Every prime $p \leq 2N + 1$ has its pivot in I_N , so (2.2) determines every $h(m)$ with $m \leq 2N + 1$. More generally, for a completely multiplicative function valued in an abelian group, each integer $a \geq 2$ has a rational identity

$$a = \prod_{d,r} (r^2 - d)^{e_{d,r}}, \quad \sum_{d,r} |e_{d,r}| \leq \lfloor \log_2 a \rfloor, \quad r \leq \lfloor a/2 \rfloor.$$

Indeed, use $p = D_p/c_p$ at a prime and concatenate already constructed identities for the prime factors of c_p ; the cost is at most $1 + \log_2 c_p < \log_2 p$. Products handle composite a , while 2 and 3 have one-term identities. Thus the three infinite traces determine such a source as well. The observations used for a prefix of index N can be integers of size $N^2 + 2$; this is not recovery from smaller integer arguments.

2.3 All relations, inside the original prefix

For a non-pivot label $i \in I_N \setminus \mathcal{B}_N$, put

$$C_i = \{i\} \cup B(Q_i). \quad (2.7)$$

The union is disjoint. Its other labels are pivots occurring strictly before i : a prime dividing Q_i either already appeared or would make i its pivot; subsequent cofactor descent goes backwards again. The product over C_i is a square.

Theorem 2.4 (Canonical parity presentation). *For $N \geq 2$, the sets C_i satisfy*

$$|C_i| \leq \lfloor \log_4(N^2 + 2) \rfloor + 3 = \lfloor \log_2 N \rfloor + 3 = \ell_N. \quad (2.8)$$

A word $w \in \{\pm 1\}^{I_N}$ is realised by a source if and only if

$$\prod_{j \in C_i} w_j = 1 \quad (i \in I_N \setminus \mathcal{B}_N). \quad (2.9)$$

These $3N - 1 - |\mathcal{P}_N|$ relations are independent and generate all parity relations among the readings. They are unchanged when the prefix is enlarged.

Proof. Proposition 2.2 gives the inequality in (2.8). To check the equality of integer parts, write $2^k \leq N < 2^{k+1}$. Then $4^k \leq N^2 + 2 < 4^{k+1}$, since $N \leq 2^{k+1} - 1$ and $N \geq 2$.

Every genuine word satisfies the square-product identities. Conversely, preserve the proposed pivot signs and reconstruct prime signs using (2.2). This gives a genuine source, after any assignment outside $\mathcal{P}_N$. Equation (2.9) forces each non-pivot value to equal the value of that source. Every check contains its own non-pivot and no other non-pivot, so the checks are independent. The valuation matrix has rank $|\mathcal{P}_N|$ because of its pivot submatrix; hence its relation space has dimension $3N - 1 - |\mathcal{P}_N|$. Independence with this cardinality proves completeness. First occurrences and the deterministic descent do not depend on a later horizon, proving prefix compatibility. $\square$

In bits, with 1 representing a negative sign and the pivots placed first, the matrix of these checks is

$$H_N = (A_N \mid I), \quad C_N = \ker H_N. \quad (2.10)$$

An abstract information set gives a systematic matrix, but does not by itself give the arithmetic width bound (2.8). Conversely, a short row bound says nothing about how many rows contain a small-prime pivot.

Example 2.5 (A relation crossing two traces). The four labelled values

$$Q_{-1}(5) = 2 \cdot 13, \quad Q_2(12) = 2 \cdot 71, \quad Q_{-1}(86) = 13 \cdot 569, \quad Q_2(201) = 71 \cdot 569$$

have product $1\,050\,374^2$. Their four signs must therefore multiply to $+1$. This example illustrates what a relation tests: the repeated prime factors disappear, even though no individual reading reveals all its prime signs. It does not show that four-reading checks generate every relation at every horizon; Theorem 2.4 supplies the complete family with its logarithmic bound.

2.4 Prescribed prime values, and a repair with fixed pivots

To prescribe $h(q) = \kappa(q)$ for $q \in S \subseteq \mathcal{P}_N$, add

$$\prod_{j \in B(q)} w_j = \kappa(q). \quad (2.11)$$

These rows have weight at most $\ell_N - 1$ and use only pivots. Primes prescribed outside $\mathcal{P}_N$ can simply be assigned after reconstruction; processing an explicit list of them has its own input-length cost.

A useful consequence is an exact local-to-global assertion: if every set of at most ℓ_N labels is separately realisable by a source satisfying κ , then the whole word is realisable by one such source. Apply this assumption to each support in (2.9) and (2.11), then use completeness. The small sets may contain widely separated indices. This is not a statement about short consecutive windows.

For an arbitrary word, preserve all pivots, reconstruct the source, and call its full word $\hat{w}$. If $V_N(w)$ is the number of violated checks in (2.9), then

$$d_H(w, \hat{w}) = V_N(w), \quad \text{dist}_H(w, \mathcal{C}_N) \leq V_N(w). \quad (2.12)$$

Each check determines exactly its own non-pivot value. Thus this repair is optimal among words preserving the pivots, but need not be globally nearest. If a word is at distance at least $\varepsilon|I_N|$ from $\mathcal{C}_N$, a uniformly chosen check rejects it with probability at least ε and uses at most ℓ_N readings. If there are no checks, there are no words at positive distance. This is a consistency test; it does not lower-bound the distance of every source with $h(p) = -1$ from the constant word.

3 Repair without trusting the pivots

The fixed-pivot repair can magnify an error in a heavily used pivot into many altered non-pivot readings. To find a nearest source, one must allow those pivots to change. The complete short presentation makes an exact search possible without guessing every relevant prime sign.

3.1 Branching on a violated relation

Add any prime constraints (2.11) to the systematic matrix and write the resulting affine system as

$$Hx = b.$$

It has $O(N)$ rows and columns, with row weight at most ℓ_N . For the received bit word w , let $s = Hw + b$. A correction is a vector e satisfying

$$He = s, \quad \text{wt}(e) \leq t. \quad (3.1)$$

Here e records incorrect readings, not negative prime signs.

Maintain a set F of coordinates already chosen for correction and the current syndrome $s + H\mathbf{1}_F$. If it vanishes, return this correction. Otherwise select a violated row with support R . If the remaining budget is zero, or $R \setminus F$ is empty, close this branch. In every other case, branch over all $i \in R \setminus F$, replacing F by $F \cup \{i\}$ and updating the entire syndrome.

Proposition 3.1 (Exact bounded-radius decision). *This search decides (3.1) and visits at most*

$$\sum_{j=0}^t \ell_N^j \leq (1 + \ell_N)^t \quad (3.2)$$

nodes. A successful leaf determines a genuine source satisfying the prescribed prime values.

Proof. Suppose a solution support F_* exists. Follow a branch with $F \subseteq F_*$. On a violated row, the remaining set $F_* \setminus F$ must have odd intersection with R , and in particular contains an element of $R \setminus F$. The search explores that choice. In at most $|F_*|$ steps this branch reaches a

zero syndrome. Thus failure on every branch proves nonexistence. A zero syndrome means that $w + \mathbf{1}_F$ satisfies the complete affine presentation, so the triangular reconstruction produces the claimed source. The depth and branching bound give (3.2). $\square$

All equations must be updated at each step: an equation previously satisfied can become false. The search is not a relaxation to an ordinary hitting-set problem. Its branching principle is classical; arithmetic completeness supplies a valid constraint of width $O(\log N)$ whenever the current word is inconsistent.

The work per node and the preparation of the arithmetic matrix are polynomial in N . Successively trying radii $0, 1, \dots, t_*$ finds an optimum at a further factor at most $t_* + 1$. The parameterised statement can also be written

$$N^{O(1)}(1 + \ell_N)^t \leq 2^{O(t \log(t+2))} N^{O(1)}.$$

Indeed, $1 + \ell_N \leq 8 \log(2N)$ and $x^t e^{-x} \leq (t/e)^t$ give, for $t \geq 1$,

$$(1 + \ell_N)^t \leq 2N(8t/e)^t.$$

In particular, the original decision bound is polynomial when $t = O(\log N / \log \log(3N))$.

3.2 A negative answer has a finite certificate

At an unsuccessful internal node, record the selected violated row and every allowed child. At a leaf, record either the exhausted budget or the fact that the violated support contains no unchosen coordinate. A checker verifies the square identities underlying the rows, the current syndromes, completeness of the child lists and the leaf conditions. Its work is polynomial in the arithmetic input and the length of the displayed tree. It need not repeat the strategy that selected each violated row.

The union of all supports used by the tree contains at most

$$\ell_N(1 + \ell_N)^t$$

labels, or $|I_N|$ if smaller. This restricted set, with the same prime constraints, already rules out a radius- t repair. This is a finite support bound for a refutation, not a polynomial bound independent of t . An optimal repair can be certified by its positive witness and a negative tree for the preceding radius.

3.3 Erasures are charged by their useful rank

Let $U \subseteq I_N$ be erased and $K = I_N \setminus U$ be known. A non-pivot appears only in its own equation. If that non-pivot is erased, remove its equation: once the pivots have been reconstructed, its missing value can always be filled. No guessing is required for these coordinates.

Let e now denote the number of erased pivots, not a correction vector. In the remaining equations, including the prescribed-prime constraints, write

$$Jx_K + Eu = b, \quad u \in \mathbb{F}_2^e, \quad r = \text{rank } E. \quad (3.3)$$

The rank depends on the erased positions and imposed constraints, not on the received signs.

Lemma 3.2 (Projection with controlled row width). *The known coordinates in (3.3) extend to a solution if and only if they satisfy a system of $O(N)$ equations of row weight at most $(r+1)\ell_N$. Each fixed extendible assignment on K has exactly 2^{e-r} completions to a word on I_N .*

Proof. Select r rows whose restrictions to erased pivot columns form a basis of the row space of E . In every other row, cancel those columns by a linear combination of these basis rows. Each resulting equation is a combination of at most $r + 1$ original rows, giving the asserted support bound.

If the projected equations hold, the chosen r equations impose a consistent rank- r system on u : their coefficient rows are independent, so every right-hand side is attained. It has 2^{e-r} solutions. The other equations follow by construction, and the erased non-pivots are filled uniquely using their removed equations. Necessity follows by eliminating u from any full solution. $\square$

Apply Proposition 3.1 to the projected system. The exact repair time becomes

$$N^{O(1)}[1 + (r + 1)\ell_N]^t \leq 2^{O(t \log(t+r+2))} N^{O(1)}. \quad (3.4)$$

Any number of erased non-pivots preserves the original width if no pivot is erased. At radius zero, extension is a polynomial linear-algebra calculation even if many pivots are erased. Neither observation implies that the original source is unique.

3.4 Recovering a value, or certifying ambiguity

For a prime target $p \in \mathcal{P}_N$, run the constrained search twice, with $h(p) = +1$ and $h(p) = -1$. If neither search succeeds, the data do not admit a source within the specified radius. If exactly one succeeds, that sign is forced by the data and budget. If both succeed, the two witnesses certify ambiguity. If $p \notin \mathcal{P}_N$ and is not externally prescribed, it is free. The two searches add the same coefficient row, supported on $B(p)$; only its right-hand side changes. With the same erasure mask and other constraints, their erased-pivot matrices are therefore identical:

$$E_+ = E_-, \quad \text{rank } E_+ = \text{rank } E_-.$$

They may reuse the same elimination of the erased columns, while propagating their different right-hand sides. Adding the target row can increase the rank relative to the system with no constraint on p , but changing the prescribed sign of that same target cannot.

A distance criterion explains when recovery is guaranteed regardless of the pattern of errors. If a word was produced by f , then suffered at most t flips and s erasures, any second compatible source g differs from f at at most $2t + s$ labels. Therefore

$$2t + s < m_p(N) \implies \text{every compatible source has the same value at } p. \quad (3.5)$$

To prove this, if $f(p) \neq g(p)$ then $h = fg$ is admissible in (1.4), and its negative labels are exactly their disagreements.

Example 3.3 (Why a nearest source need not be the original one). At $N = 100$, the prime 101 occurs only at the two labels with values $101 = Q_{-1}(10)$ and $8282 = Q_{-1}(91)$. The sources $f(m) = (-1)^{v_2(m)}$ and $g(m) = f(m)(-1)^{v_{101}(m)}$ differ at precisely these two labels. A word taking one of the two differing readings from each source is one flip from both. There is then no justified choice between $f(101)$ and $g(101)$, even though exact radius-one repair is possible.

Together, Theorem 2.4, Proposition 3.1 and Lemma 3.2 prove Theorems 1.1 and 1.2. The remaining issue is quantitative distance and source recovery, not the existence of a complete system of checks.

4 Replicating a pivot without a regulator

A single short certificate for p may depend on a few badly corrupted readings. We now replace each of its pivots by distinct readings with exactly the same value under every source. The construction starts from a pivot itself, rather than from a fundamental unit in a varying quadratic field.

The qualitative repetition of a represented square class by Pell equations is an antecedent of this construction: see Borwein–Choi–Ganguli [4, Theorem 2.2]. For our equation $x^2 - d = Dy^2$, the starting solution is positive and D is nonsquare, so the nondegenerate setting required here is satisfied. What must still be controlled is the height of enough distinct repetitions, uniformly over the pivots in a target certificate. The explicit unit below gives that control without estimating a fundamental unit.

4.1 The explicit norm-one unit

Write a pivot as

$$D = r^2 - d > 1, \quad d \in \mathcal{D}.$$

The integer D is not a square. Put

$$U = \frac{2r^2 - d}{|d|}, \quad V = \frac{2r}{|d|}. \quad (4.1)$$

Both are positive integers, and direct calculation gives

$$U^2 - DV^2 = 1, \quad U + V\sqrt{D} = \frac{(r + \sqrt{D})^2}{|d|}.$$

Starting with $(x_0, y_0) = (r, 1)$, define

$$x_{j+1} = Ux_j + DVy_j, \quad y_{j+1} = Vx_j + Uy_j. \quad (4.2)$$

Then $x_j^2 - d = Dy_j^2$, and x_j increases strictly. Thus

$$h(Q_d(x_j)) = h(D) \quad (h \in \mathcal{M}^\pm). \quad (4.3)$$

There is no assertion that $U + V\sqrt{D}$ is fundamental. Its explicit size is the advantage.

Lemma 4.1 (Uniform height and disjointness). *If the pivot belongs to a prime $q \leq P$, where $P \geq 3$, then*

$$x_j < P^{2j+1}. \quad (4.4)$$

The replica labels of distinct pivots are disjoint.

Proof. For $q \geq 5$, Lemma 2.1 gives $r < q/2$ and $\sqrt{D} < q/2$, hence $r + \sqrt{D} < q$. The same bound with P holds for the initial pivots: $1 + \sqrt{2} < 3$ and $1 + \sqrt{3} < 3$. From (4.2),

$$x_j + y_j\sqrt{D} = (r + \sqrt{D})^{2j+1}/|d|^j < P^{2j+1}.$$

Every value in an orbit has square class $\text{core}(D)$. The pivot square classes are distinct: each has its own largest prime factor, of odd valuation. A label shared by two orbits would have both classes, which is impossible. $\square$

4.2 Disjoint certificates for a target prime

For p , use the s_p pivots in (2.6). Take R replicas of each pivot, and at level j combine the j th replica from every pivot. The resulting R certificates each have square class p , and are pairwise disjoint in labels. They lie in I_N whenever

$$N \geq B_p^{2R-1}, \quad B_p = \max(3, p). \quad (4.5)$$

Thus $h(p) = -1$ forces at least one negative reading in every certificate, yielding the elementary bound

$$m_p(N) \geq \left\lfloor \frac{1}{2} + \frac{\log N}{2 \log B_p} \right\rfloor \quad (4.6)$$

whenever the right side is positive. This bound is uniform but logarithmic at fixed p . The next section amplifies each pivot much more strongly.

The $s_p R$ readings also admit R^{s_p} transversal certificates, by independently selecting one replica of each pivot. This combinatorial count does not multiply their information content. Every certificate of square class p in this sample uses an odd number of readings from each pivot group, because the pivot classes are independent. Giving every reading unit capacity, the total weight of any fractional packing of such certificates is at most R , by considering one group. The diagonal R disjoint certificates attain this value. Choosing one negative pivot and all other pivot signs positive shows that the minimum number of negative readings on the sample is exactly R as well.

4.3 A finite adversarial guarantee

Proposition 4.2 (Simultaneous recovery from explicit replicas). *Let $P \geq 3$ be an integer and let $t, s \geq 0$. Put $R = 2t + s + 1$ and suppose $N \geq P^{4t+2s+1}$. Then $R\pi(P)$ distinct nonadaptive queries with indices at most N suffice to recover all source values $h(m)$, $m \leq P$, after at most t incorrect readings and s erased readings in total.*

Proof. Use R replicas of every pivot belonging to $q \leq P$. In any one group, if t' readings are false and s' are erased, then $2t' + s' \leq 2t + s < R$. Strict majority of the remaining readings therefore equals that pivot's true value. Once every pivot has been recovered, (2.2) gives the prime signs and then every $h(m)$ with $m \leq P$. Lemma 4.1 supplies the height and disjointness. $\square$

This is recovery of arbitrary source signs, not decoding of messages placed in a preselected multiplicative code. The query pattern is chosen before the received values. Its sufficient height is explicit; no optimality in the height or error budget is asserted.

5 Balanced divisors and uniform amplification

Replication gives one new reading per recurrence step. To obtain more redundancy at a given height, we use a term with many divisors and turn these divisors into disjoint pairs. The crucial accounting is that the logarithmic cost of reserving the divisors is small compared with the available logarithmic height.

5.1 A cube of disjoint pairs

Lemma 5.1 (Balanced-divisor pairs). *Let $D \geq 2$ be nonsquare, $d \in \mathcal{D}$, and m, u be positive integers with $m^2 - d = Du^2$. Let $W \mid u$ be squarefree and coprime to D , with $s = \omega(W)$. For*

every choice $\varepsilon_\ell \in \{-1, 0, 1\}$, $\ell \mid W$, set

$$a = \frac{u}{W} \prod_{\ell \mid W} \ell^{1+\varepsilon_\ell}, \quad b = \frac{Du}{W} \prod_{\ell \mid W} \ell^{1-\varepsilon_\ell}, \quad x = m + a, \quad y = m + b. \quad (5.1)$$

The 3^s pairs (x, y) use $2 \cdot 3^s$ distinct labels on trace d and satisfy

$$Q_d(x)Q_d(y) = D[u(x + y)]^2. \quad (5.2)$$

Every index lies in $(m, m + DuW]$.

Proof. We have $ab = Du^2 = m^2 - d$, so

$$Q_d(m + a) = a(2m + a + b) = a(x + y), \quad Q_d(m + b) = b(x + y).$$

Their product is (5.2). Within the a -family, the valuations at the reserved primes determine all trits ε_ℓ ; the same holds within the b -family. To exclude a collision between the two families, choose any prime dividing D . It does not divide W , and its valuation in every b exceeds its valuation in every a by its positive valuation in D . Thus no two indices coincide. Finally $a \leq uW$ and $b \leq DuW$. $\square$

The three pairs in the introduction are this cube with $d = -1$, $D = 2$, $m = 7$ and $u = W = 5$: the choices $\varepsilon_5 = -1, 0, 1$ give $(8, 57)$, $(12, 17)$ and $(32, 9)$, respectively. Thus one reserved prime already produces three disjoint pairs, with the last pair written in the opposite order in the introduction. If $h(D) = -1$, every pair contributes one reading of each sign. The squarefree hypothesis here is convenient for the primitive-divisor argument; Section 6 replaces it by pairwise coprime blocks without losing injectivity.

5.2 A Lehmer sequence attached to each pivot

The next construction has two obligations: provide many reserved factors, and keep their product small enough that all pair indices fit below N . Its counting mechanism is

$$\underbrace{\tau(b) = 2^t}_{\substack{b \text{ squarefree} \\ t \text{ odd prime factors}}} \implies \omega(W) \geq 2^t - 15 \implies 3^{\max(0, 2^t - 15)} \text{ pairs.}$$

Here b is a divisor of the recurrence rank, not a pair divisor in (5.1). A distinct primitive factor will be reserved for each divisor of b above thirty. The primordial choice gives $t \sim \log K / \log \log K$, explaining the double growth, but we must also prove $\log W = o(\log N)$ uniformly in p . The normalisation below makes both the supply of primitive factors and this height cost explicit.

For a pivot $D = r^2 - d$, put

$$a_0 = |d|, \quad e = d/a_0, \quad \lambda = \frac{r + \sqrt{D}}{\sqrt{a_0}}, \quad \zeta = \frac{r - \sqrt{D}}{\sqrt{a_0}} = e/\lambda. \quad (5.3)$$

The use of a_0 here is local to this subsection; it is not a divisor in (5.1). We have

$$\frac{1}{2} < \log \lambda, \quad \lambda < B_p, \quad \sqrt{D} < B_p \quad (5.4)$$

for every pivot in the certificate of p . The lower bound follows already from the three smallest possible seeds, and the upper bounds follow from Lemma 2.1 and the two initial pivots.

For odd $k \geq 1$, define integers m_k, u_k by

$$m_k + u_k \sqrt{D} = (r + \sqrt{D})(U + V \sqrt{D})^{(k-1)/2}. \quad (5.5)$$

Then

$$m_k^2 - d = Du_k^2, \quad \lambda^k/4 \leq m_k \leq \sqrt{2}\lambda^k, \quad u_k \leq \sqrt{2/D}\lambda^k. \quad (5.6)$$

Indeed, the sum and difference with the conjugate give $m_k = \sqrt{a_0}(\lambda^k + \zeta^k)/2$ and $u_k = \sqrt{a_0}(\lambda^k - \zeta^k)/(2\sqrt{D})$; the bounds follow from $|\zeta| = \lambda^{-1}$ and (5.4).

For all positive j , use the Lehmer normalisation

$$L_j = \begin{cases} (\lambda^j - \zeta^j)/(\lambda - \zeta), & j \text{ odd}, \\ (\lambda^j - \zeta^j)/(\lambda^2 - \zeta^2), & j \text{ even}. \end{cases} \quad (5.7)$$

Here $(\lambda + \zeta)^2 = 4r^2/a_0 =: A$ is a positive integer and $\lambda\zeta = e \in \{\pm 1\}$, so these two integers are coprime and nonzero. The numbers λ, ζ are algebraic integers: they satisfy $X^4 - (A - 2e)X^2 + 1 = 0$. Their ratio is not a root of unity. Thus they form a Lehmer pair in the sense of Bilu et al. [3]. In this normalisation,

$$L_1 = L_2 = 1, \quad L_3 = A - e, \quad L_4 = A - 2e, \quad L_j = (A - 2e)L_{j-2} - L_{j-4} \quad (j \geq 5). \quad (5.8)$$

In particular these are integers; for odd k , $u_k = L_k$. For odd $j \mid k$, the geometric factorisation of powers gives $L_j \mid L_k$.

The primitive-divisor input. We use the following consequence of Bilu et al. [3, Theorem 1.4]: for every $j > 30$, L_j has a prime divisor not dividing

$$(\lambda^2 - \zeta^2)^2 L_1 \cdots L_{j-1}. \quad (5.9)$$

This definition matters: for our pair, $(\lambda^2 - \zeta^2)^2 = 16r^2D/a_0^2$ is an integer divisible by every prime factor of D . Primitive divisors obtained at distinct ranks are distinct and avoid D . Only real Lehmer pairs and odd ranks greater than 30 are used. The earlier real-pair theorem of Carmichael–Ward, stated as Theorem A in [3], is already sufficient; we retain the common conservative threshold 30. No list of defective pairs at small ranks enters the argument.

Let b be an odd squarefree integer dividing the odd rank k . Choose one primitive prime at each divisor $j \mid b$ with $j > 30$, and let W be their product. There are at most fifteen positive odd integers at most 30, hence

$$W \mid u_k, \quad (W, D) = 1, \quad \omega(W) \geq \tau(b) - 15. \quad (5.10)$$

Also $L_j \leq \lambda^{2j}$ for the relevant ranks, by (5.7) and $\lambda > e^{1/2}$. Consequently

$$\log W \leq 2 \log \lambda \sum_{j \mid b} j \leq 2 \log \lambda b(1 + \log b). \quad (5.11)$$

The last inequality uses $\sigma(b)/b = \sum_{j \mid b} j^{-1} \leq 1 + \log b$. This height cost, not just the number of primitive factors, is needed below.

5.3 Fitting the entire cube in a terminal range

We now prove Theorem 1.3. For $\alpha < 0$, the assertion follows from the case $\alpha = 0$, so assume $0 \leq \alpha < 1$. Let $L = \log N$, $K = L/\log B_p$ and $\beta = (1 + \alpha)/2$. Choose b to be the largest odd primorial not exceeding

$$K/(\log K)^2. \quad (5.12)$$

The same b will work for all pivots in the certificate of p . For each such pivot, let k be the largest odd multiple of b not exceeding $\beta L/\log \lambda$. Once K is large, this rank exists and

$$\beta L - 2b \log B_p < k \log \lambda \leq \beta L. \quad (5.13)$$

The factor two pays the spacing between successive odd multiples.

Take W from (5.10). Combining (5.11) with (5.12),

$$\frac{\log W}{L} \leq \frac{2(1 + \log K)}{(\log K)^2} = o(1), \quad (5.14)$$

uniformly in p and in the chosen pivot. By (5.6) and Lemma 5.1, the resulting pair indices satisfy

$$m_k < x, y \leq m_k + Du_k W \leq 3\sqrt{D}\lambda^k W.$$

The lower and upper logarithmic bounds are therefore

$$\frac{\log m_k}{L} > \beta - \frac{2}{(\log K)^2} - \frac{\log 4}{K \log 3}, \quad (5.15)$$

$$\frac{\log \max(x, y)}{L} \leq \beta + \frac{2}{K} + \frac{2(1 + \log K)}{(\log K)^2}. \quad (5.16)$$

For a threshold depending only on α , the first expression exceeds α and the second is less than one. This proves that every selected pair lies in $(N^\alpha, N]$, with a uniform threshold. The primordial choice spends only a vanishing fraction of the available logarithmic height on divisors; the remaining fixed margin separates the cube from both endpoints.

5.4 How many pairs this gives

Write b as the product of the first t odd primes. The prime number theorem gives

$$\log b \sim \log K, \quad t = (1 + o(1)) \frac{\log K}{\log \log K}, \quad \tau(b) = 2^t.$$

Indeed the logarithm of the next prime is negligible compared with $\log b$, so taking the largest primordial below (5.12) does not alter this asymptotic. Only the ordinary prime number theorem is used here [13, §27.12].

Let

$$M(K) = 3^{\max(0, \tau(b) - 15)}. \quad (5.17)$$

For every $0 < c < \log 2$ and all sufficiently large K ,

$$\log \log M(K) \geq (\log 2 - o(1)) \frac{\log K}{\log \log K} \geq c \frac{\log K}{\log \log K}. \quad (5.18)$$

Thus every pivot has at least $\Phi_c(K)$ disjoint pairs of its own square class in the desired interval.

Finally, (2.6) gives

$$-1 = h(p) = \prod_{j \in B(p)} h(Q_j).$$

At least one of these pivots, say D , is negative. Its own pair family alone supplies $M(K)$ readings of each sign. No summation over the pivot families is required. This proves (1.6), with one threshold $K_0(\alpha, c)$ independent of p and of all source signs, and completes the proof of Theorem 1.3.

5.5 Recovery consequences, and where overlap is harmless

The pair families are fixed before the source is known. In each family, multiply the two received readings in a pair and take a majority over pairs with no erasure. If the whole observation has t incorrect labels and s erased labels, then at most t pairs in this particular family have

an incorrect product and at most s are erased. Hence all pivots, and then $h(p)$, are recovered whenever

$$2t + s < M(K). \quad (5.19)$$

Different pivot families may overlap. This does not affect (5.19), since the same global budget bounds the damage in each family separately. It would affect an attempt to add their capacities. In particular, neither this recovery argument nor the proof of Theorem 1.3 claims a disjoint packing of direct target- p certificates of size $M(K)$ across all pivots.

Corollary 5.2 (Moving target ranges). *If $\log P_N = o(\log N)$, then for every $0 < c < \log 2$ and all sufficiently large N ,*

$$\min_{p \leq P_N} m_p(N) \geq \Phi_c \left(\frac{\log N}{\log \max(3, P_N)} \right).$$

For fixed $\kappa > 0$, the range $p \leq (\log N)^\kappa$ admits the bound

$$\exp \left(\exp \left(c \frac{\log \log N}{\log \log \log N} \right) \right) \quad (0 < c < \log 2).$$

For $p \leq \exp((\log N)^\delta)$, $0 < \delta < 1$, the same displayed bound holds for every $0 < c < (1 - \delta) \log 2$.

Proof. For large K , $\Phi_c(K)$ is increasing, so the first assertion follows from the uniform threshold. In the two special ranges, substitute the smallest permitted K and first apply Theorem 1.3 with a slightly larger constant than the one required in the conclusion. This fixed slack absorbs the lower-order logarithms. $\square$

6 Compact families without factoring large recurrence terms

The proof of the uniform bound selects primitive prime divisors only to obtain independent choices among divisors. Finding those primes by factoring a large Lehmer number would introduce a computational task absent from the existence argument. We now replace prime divisors by coprime integer blocks. This preserves the arithmetic identities and gives a compact description of the resulting family; it does not make an exponentially long list short to print.

6.1 Coprime blocks carry the same independent choices

Suppose that $m^2 - d = Du^2$, where $D \geq 2$ is not a square. Let $g_1, \dots, g_s > 1$ be pairwise coprime, put $W = \prod_i g_i$, and assume

$$W \mid u, \quad (W, D) = 1.$$

For $\mathbf{t} \in \{0, 1, 2\}^s$, set

$$a_{\mathbf{t}} = \frac{u}{W} \prod_i g_i^{t_i}, \quad b_{\mathbf{t}} = D \frac{u}{W} \prod_i g_i^{2-t_i}. \quad (6.1)$$

Their product is Du^2 , so the pairs $(m + a_{\mathbf{t}}, m + b_{\mathbf{t}})$ satisfy (5.2) with this D .

Proposition 6.1 (A block cube). *The 3^s pairs in (6.1) use $2 \cdot 3^s$ distinct labels of trace d . Their smallest and largest indices are exactly*

$$m + u/W, \quad m + DuW. \quad (6.2)$$

Neither primality nor squarefreeness of the blocks is required.

Proof. For a prime dividing g_i , its valuation in a_t determines t_i , because it divides no other block. Thus the a 's are distinct; the same holds for the b 's. Since D is nonsquare, it has a prime divisor of odd valuation. That prime divides none of the blocks, and its valuations in the a 's and the b 's differ by the fixed positive valuation in D . Hence the two sets are disjoint. The minimum and maximum follow by choosing all exponents equal to zero or two; $D \geq 2$ makes the largest b the global maximum. $\square$

For example, the centre $239^2 + 1 = 2 \cdot 169^2$ admits the single block 169. It yields three pairs, at indices between 240 and 57361, without requiring the factorisation $169 = 13^2$. The repeated prime in this block causes no collision: only its three distinct exponents matter.

6.2 Producing the blocks by greatest common divisors

For positive integers v, H , define

$$\text{sat}(v, H) = \prod_{q \nmid H} q^{v_q(v)}.$$

This notation describes an integer that can be computed without its factorisation: start with $z = v$ and repeatedly replace z by $z / \gcd(z, H)$ until the greatest common divisor is one. Each nontrivial step at least halves z , so at most $\text{bl}(v)$ such steps are needed, where $\text{bl}(v) = \lfloor \log_2 v \rfloor + 1$.

Fix the Lehmer sequence from Section 5, an odd integer b , and an odd multiple k of b . Process the odd divisors $j > 1$ of b in increasing order. Starting with $W = 1$, compute

$$g_j = \text{sat}(L_j, DW). \quad (6.3)$$

Whenever $g_j > 1$, keep it and replace W by Wg_j .

Proposition 6.2 (Factorisation-free reserved blocks). *The blocks retained by (6.3) are pairwise coprime and coprime to D . Their product divides u_k . If s is their number, then*

$$s \geq \tau(b) - 15, \quad \log W \leq 2(\log \lambda)\sigma(b). \quad (6.4)$$

Proof. The coprimality assertions follow from the definition of saturation. Each block divides L_j , which divides L_k and hence u_k . Pairwise coprimality then implies that their product divides u_k . If $j > 30$, a primitive divisor of L_j divides neither D nor an earlier Lehmer term, by (5.9). It therefore survives saturation, and the corresponding block exceeds one. At most fifteen odd divisors of b are at most thirty. Finally $g_j \leq L_j$ and $\log L_j \leq 2j \log \lambda$, so summation gives the height bound. $\square$

Thus the same choice of b and k as in Section 5 gives the same asymptotic lower bound. The primitive-divisor theorem is still an existence input guaranteeing many nontrivial blocks. The computation does not have to identify the primitive prime in each block.

6.3 What a compact description certifies

A family description records d, D, m, u , the pairwise coprime blocks, their product W , and the height bound. The verifier checks the norm equation, divisibilities, coprimality and (6.2). Proposition 6.1 then certifies its cardinality and disjointness symbolically. To obtain a specified pair, write its index in base three and apply (6.1). Each such query requires a number of integer operations polynomial in the binary lengths of the stored data.

There is also a polynomial-time search for these descriptions, once the seed data are supplied. More precisely, consider finitely many seeds $D_i = r_i^2 - d_i \geq 2$ and a certified identity

$$\prod_i D_i = tz_0^2, \quad (6.5)$$

where $t \geq 2$ is nonsquare. Let S denote the total binary length of the seed data and let $T = \text{bl}(N)$. One may try each odd initial primorial $b \leq T$, construct its divisors by their known prime factors, form the blocks (6.3) for each seed, and search the odd multiples k of b for which (6.2) stays below N . The largest admissible k for each seed is sufficient. Select among these trials a family with largest minimum block-cube cardinality.

Only polynomially many ranks and divisors are tested: $b \leq T$, and $m_k \geq \lambda^k/4$ with $\log \lambda > 1/2$ bounds the relevant ranks by $O(T)$. Recurrences, Euclidean algorithms and integer comparisons involve numbers of polynomial binary length in $T + S$. Hence the search and verification cost is polynomial in $T + S$. A failed search only means that these candidates did not fit; it is not an impossibility certificate for other arithmetic families. A prescribed terminal interval can be enforced by checking its lower endpoint as well.

For canonical prime-reconstruction seeds, the asymptotic primorial of Section 5 is among these trials for large K . The search therefore retains that lower-bound scale. Preparing the canonical seeds themselves may require work polynomial in the *numerical prime* p ; the binary-time assertion here starts after the seed certificate is supplied. Similarly, a height $N = 10^E$ has binary length of order E , not of order $\log E$.

If intervals for the different seeds are made disjoint, choosing equally indexed pairs from their families and using (6.5) gives direct certificates for t . Without such a separation, the minimum bound still follows by selecting a negative seed, but a collection of direct certificates with unit loads requires a separate overlap argument. No such composition is implicit in a compact description.

Coprime factor refinement is classical; Bernstein's work [2] gives a much more general algorithmic setting. The specialised saturation procedure above is included to make the arithmetic certificate and its complexity parameter explicit. Its value is access to a large family without factoring its large recurrence terms, not a faster asymptotic growth of $m_p(N)$.

7 Direct prime certificates on a prescribed trace

The regulator-free argument reconstructs $h(p)$ as a product of pivot signs. When $h(p) = -1$, it uses whichever pivot is negative; consequently the trace carrying both signs can depend on the source. A different construction keeps the trace fixed by p and makes every pair read $h(p)$ directly. Its uniform prime range is smaller, but this geometric feature is not implied by Theorem 1.3.

Define

$$d_p = \begin{cases} -1, & p = 2 \text{ or } p \equiv 1 \pmod{4}, \\ -2, & p \equiv 3 \pmod{8}, \\ 2, & p \equiv 7 \pmod{8}. \end{cases} \quad (7.1)$$

Lemma 7.1 (A direct seed and its height). *There are positive integers m_0, u_0 with $m_0^2 - pu_0^2 = d_p$ such that, on putting $a = |d_p|$ and*

$$\lambda = \frac{m_0 + u_0\sqrt{p}}{\sqrt{a}},$$

one has

$$\lambda^2 = \epsilon_p, \quad \frac{1}{2} < \log \lambda \leq 3\sqrt{p}(\log(4p) + 2), \quad (7.2)$$

where $\epsilon_p = X_p + Y_p\sqrt{p}$ is the least unit of norm one with positive integer coordinates.

Proof. Existence of ϵ_p is the classical Pell theorem; see [5]. For $p = 2$, take $m_0 = u_0 = 1$. For $p \equiv 1 \pmod{4}$, a norm-one solution has X_p odd and Y_p even. The consecutive coprime integers $(X_p - 1)/2$ and $(X_p + 1)/2$ have product $p(Y_p/2)^2$. The assignment in which the second factor

is a square would give a smaller positive norm-one solution. Thus

$$m_0^2 = (X_p - 1)/2, \quad u_0^2 = (X_p + 1)/(2p).$$

For $p \equiv 3 \pmod{4}$, an odd X_p would give either the same minimality contradiction or a norm-minus-one solution, impossible modulo p . Hence X_p is even and Y_p odd. The coprime factors $X_p - 1$ and $X_p + 1$ have product pY_p^2 . Quadratic reciprocity gives

$p \pmod{8}$	m_0^2	u_0^2
3	$X_p - 1$	$(X_p + 1)/p$
7	$X_p + 1$	$(X_p - 1)/p$.

The excluded assignments would give respectively a norm $+2$ or -2 which is not a quadratic residue modulo p . These formulas prove the norm identity and $\lambda^2 = \epsilon_p$.

For completeness, the height estimate uses only an upper bound for an L -value. For the fundamental discriminant $\Delta \leq 4p$ of $\mathbb{Q}(\sqrt{p})$, the analytic class number formula and quadratic zeta factorisation give

$$L(1, \chi_\Delta) = \frac{2h_K R_K}{\sqrt{\Delta}}, \quad R_K \leq \frac{\sqrt{\Delta}}{2}(\log \Delta + 2).$$

The first identity is the real-quadratic specialisation of [15, Theorems 19.12 and 19.15]. The second uses $h_K \geq 1$ and $L(1, \chi_\Delta) \leq \log \Delta + 2$, obtained by cutting the character series at Δ and summing the tail by parts with partial sums bounded by Δ .

If $\eta > 1$ is a fundamental unit in the full ring of integers, then η^6 has norm one and lies in $\mathbb{Z}[\sqrt{p}]$. For $p \equiv 1 \pmod{4}$, the unit group of the ring modulo two has order one or three, so η^3 has integral $\sqrt{p}$ -coordinates; squaring gives norm one. In the other cases a square suffices. Therefore $\log \epsilon_p \leq 6R_K$, which proves the upper bound in (7.2). Finally $X_p \geq 2$ gives $\epsilon_p \geq 2 + \sqrt{3}$ and the lower bound. No lower bound of Siegel type is used. $\square$

For odd k , put

$$m_k + u_k \sqrt{p} = (m_0 + u_0 \sqrt{p}) \epsilon_p^{(k-1)/2}.$$

With $\zeta = (m_0 - u_0 \sqrt{p})/\sqrt{a} = (d_p/a)/\lambda$, the pair (λ, ζ) is a Lehmer pair: $(\lambda + \zeta)^2 = 4m_0^2/a$ is an integer, $\lambda\zeta = \pm 1$, and their quotient is not a root of unity. The same recurrence as (5.8) gives $u_k = u_0 L_k$, and the same primitive-divisor argument yields a squarefree $W \mid u_k$, coprime to p , with

$$\omega(W) \geq \tau(b) - 15, \quad \log W \leq 2(\log \lambda)\sigma(b) \tag{7.3}$$

for every odd $b \mid k$. Here the excluded discriminant is $16m_0^2 p u_0^2 / a^2$, so the primitive divisors avoid p .

Write

$$F_c(N) = \exp\left(\exp\left(c \frac{\log \log N}{\log \log \log N}\right)\right)$$

for sufficiently large N .

Theorem 7.2 (Direct pairs, fixed and mobile targets). *Fix $\alpha < 1$. For every fixed prime p and $0 < c < \log 2$, all sufficiently large N admit at least $F_c(N)$ pairwise disjoint pairs of labels of trace d_p , with both indices in $(N^\alpha, N]$, whose products are p times squares. More uniformly, for $0 < \kappa < 2$ and*

$$0 < c < (1 - \kappa/2) \log 2,$$

the same assertion holds for every prime $p \leq (\log N)^\kappa$, with a threshold independent of p . The families depend on p, N , not on the source.

Proof. It suffices to consider $0 \leq \alpha < 1$. Set $L = \log N$, $\beta = (1 + \alpha)/2$ and $K' = \beta L / \log \lambda$. For fixed p , $K' \asymp_p L$. In the mobile range, (7.2) gives

$$C_{\kappa, \alpha}^{-1} \frac{L^{1-\kappa/2}}{\log L} \leq K' \leq 2\beta L. \quad (7.4)$$

Choose the largest odd initial primorial $b \leq K' / (\log K')^2$, and the largest odd multiple k of b with $k \leq K'$. Then $K' - 2b < k \leq K'$ and

$$\log m_k = \beta L + o(L), \quad \log W = o(L),$$

uniformly on (7.4). The bounds follow directly from the formulas for the orbit and (7.3); in particular no p -dependent bounded error is left uncontrolled.

The balanced divisor cube of Lemma 5.1, with $D = p$, gives $3^{\omega(W)}$ disjoint pairs. Their indices exceed $m_k > N^\alpha$ and are at most

$$m_k + pu_k W \leq 3\sqrt{p} \lambda^k W = N^{\beta+o(1)} < N.$$

If b has r prime factors, the prime number theorem gives

$$r = (1 + o(1)) \frac{\log K'}{\log \log K'}, \quad \log \log(3^{\omega(W)}) \geq (\log 2 - o(1)) \frac{\log K'}{\log \log K'}.$$

For fixed p this yields every $c < \log 2$. In the mobile range, (7.4) gives every $c < (1 - \kappa/2) \log 2$. The cube identity makes each product p times a square. $\square$

Every pair therefore votes directly for $h(p)$. Discarding pairs meeting an erasure and taking a majority recovers the sign whenever $2t + s < F_c(N)$, where t and s bound all false and erased labels. This works simultaneously for all requested primes in the stated range: each target has disjoint pairs internally, even though different targets may reuse labels. No independence between targets is needed for this adversarial conclusion. Unlike the compact-description construction, this theorem does not by itself assert a polynomial-time preparation bound at the full amplified scale.

8 Recovering true signs under independent reading noise

Bounded-distance repair makes no assumption on the positions of errors, but its cost grows with the error budget. Independent noise permits a different strategy: take several distinct readings of each pivot sign, correct those signs first, and only then multiply them to reconstruct the target. This order prevents the signal loss caused by multiplying many noisy readings.

8.1 One noise variable per label

For each positive label i , independently sample $\xi_i \in \{-1, 0, 1\}$ with

$$\mathbb{P}(\xi_i = 0) = a, \quad \mathbb{P}(\xi_i = -1) = (1-a)b, \quad \mathbb{P}(\xi_i = 1) = (1-a)(1-b), \quad \mu = (1-a)(1-2b) > 0, \quad (8.1)$$

where $0 \leq a < 1$ and $0 \leq b < 1/2$. The observation from source h is $Y_i = h(Q_i)\xi_i$; zero marks a known erasure. These variables are attached to labels once and for all. Re-querying the same label does not provide another independent sample.

If R distinct labels have the same square class D , they all have the true sign $h(D)$. Majority of their nonzero observations, with a tie declared a failure, has error probability at most

$$\mathbb{P}\left(\sum_{j=1}^R \xi_j \leq 0\right) \leq \exp(-\mu^2 R/2). \quad (8.2)$$

Here and below the event bounding failure does not depend on h . One may therefore couple *all* sources to the same noise variables and obtain a simultaneous all-source guarantee on that event.

For clarity, (8.2) follows from the elementary bounded-variable exponential estimate. If $Z \in [-1, 1]$, the second derivative of $\log \mathbb{E} e^{tZ}$ is a variance under an exponential tilt, hence at most one. Integrating twice gives $\mathbb{E} e^{t(Z - \mathbb{E} Z)} \leq e^{t^2/2}$. Apply this to the independent ξ_j , use Markov's inequality, and choose $t = -\mu$. This is the usual Hoeffding argument [10]; no distributional independence of prime signs is assumed.

8.2 Correct the pivots before multiplying

Let $C(p)$ be a square-class certificate for p using s_p pivots, with $s_p \leq \lfloor \log_2 p \rfloor$ as in (2.6). Repeat each pivot R times by Section 4. If all pivot majorities are correct, their product is $h(p)$. The union bound gives

$$\mathbb{P}(\text{failure at } p) \leq s_p e^{-\mu^2 R/2}. \quad (8.3)$$

The height is at most B_p^{2R-1} , where $B_p = \max(3, p)$, and the number of distinct queried labels is $s_p R$. Thus

$$R \geq \frac{2}{\mu^2} \log \frac{s_p}{\delta}, \quad N \geq B_p^{2R-1} \quad (8.4)$$

suffices for failure probability at most δ .

The alternative of forming every transversal product does not create R^{s_p} independent observations. Algebraically,

$$\sum_{j_1, \dots, j_{s_p}=1}^R \prod_{v=1}^{s_p} Y_{v, j_v} = \prod_{v=1}^{s_p} \left(\sum_{j=1}^R Y_{v, j} \right).$$

Moreover, a single transversal product has noise mean μ^{s_p} , which can be much smaller than μ . Pivot majorities keep the concentration parameter at μ and pay only a union bound over the pivots.

Theorem 8.1 (A requested prime and a simultaneous prefix). *Fix the channel (8.1) and $A \geq 1$. Put $L = \log N$. For all sufficiently large N , any separately requested prime*

$$p \leq \exp\left(\frac{\mu^2}{16(A+2)} \frac{L}{\log L}\right) \quad (8.5)$$

can be recovered with failure probability at most L^{-A} using $O_{a,b,A}(L)$ distinct readings of indices at most N .

There is also a single family of queries recovering all prime signs $p \leq P$, and hence all values $h(n)$ for $n \leq P$, where

$$P = \left\lfloor \exp\left(c\sqrt{L}\right) \right\rfloor, \quad c = \frac{\mu}{4\sqrt{A+2}}. \quad (8.6)$$

It uses $O_{a,b,A}(P)$ readings and has failure probability at most P^{-A-1} . Each assertion holds on an event of noise configurations common to every $h \in \mathcal{M}^\pm$.

Proof. For the single target, choose

$$R = \left\lceil \frac{2}{\mu^2} (A \log L + \log s_p) \right\rceil.$$

For large N , $\log s_p \leq \log L$ and $R \leq 2(A+2)\mu^{-2} \log L$. Combining this with (8.5) gives $(2R-1) \log B_p < L$. Equation (8.3) proves the probability bound. The query count is $s_p R = O(L)$, using $s_p \ll \log p \ll L/\log L$.

For the simultaneous statement, estimate all first-occurrence pivots $b(q)$ with $q \leq P$, not separate copies of the entire certificate for every target. They form a triangular information set for these primes, so their correct values determine the whole prefix. Take

$$R = \left\lceil 2(A+2)\mu^{-2} \log P \right\rceil.$$

Their replica groups are disjoint, and each group has height at most P^{2R-1} (the finitely many small cases use $B_P = \max(3, P)$). For large N ,

$$(2R-1) \log P \leq 4(A+2)\mu^{-2}(\log P)^2 + O(\log P) \leq L/4 + O(\sqrt{L}) < L.$$

The union bound over at most P pivots gives $Pe^{-\mu^2 R/2} \leq P^{-A-1}$. Their number times R is $\pi(P)R = O(P)$, using $\pi(P) \ll P/\log P$. Every bound concerns only the signs of the noise sums, so the good event works simultaneously for all sources. $\square$

The separately requested range (8.5) is not a simultaneous guarantee over all its primes. Conversely, the simultaneous construction does not claim polynomial work in $\log N$: preparing its information set costs a polynomial in the numerical P and in $\log N$. The larger statistical range and the preparation cost are separate conclusions.

The simultaneous failure probabilities in (8.6) are summable along $N = 2^k$. Borel–Cantelli therefore gives almost-sure eventual recovery at these sizes, on the same event for all sources. Using the most recent dyadic size gives an all- N assertion with any smaller constant in place of c in the recovered prefix. The deterministic query sets are fixed before the noise is drawn; this step is not an unproved supremum over adaptive experiments.

8.3 Amplified pairs recover larger simultaneous prefixes

Replication is useful because its height bound is explicit. Amplification supplies more votes at the same horizon. A pair now reads a pivot sign through the product of two independent noise variables, so its mean noise is μ^2 rather than μ . The larger family compensates for this loss when the channel is fixed.

Corollary 8.2 (Simultaneous recovery from amplified pairs). *Fix the channel (8.1), $0 < \delta < 1$ and $A \geq 1$. For all sufficiently large N , put*

$$P = \left\lfloor \exp((\log N)^\delta) \right\rfloor. \tag{8.7}$$

A deterministic, non-adaptive family of readings of indices at most N recovers all prime signs $h(p)$ for $p \leq P$, and hence all $h(n)$ for $n \leq P$, with failure probability at most P^{-A-1} . The number of distinct readings is $O_{a,b,A}(P)$. Preparation and decoding take time polynomial in the numerical P and in $\log N$.

The successful event depends only on the label noises and is common to every $h \in \mathcal{M}^\pm$. The threshold may depend on a, b, A, δ ; no uniformity as $\delta \rightarrow 1$ is asserted.

Proof. Write $L = \log N$ and $K = L/\log P$. For every first-occurrence pivot D_q with $q \leq P$, use the pair construction in Sections 5–6. The relevant bounds are

$$\frac{1}{2} < \log \lambda_q < \log P, \quad \sqrt{D_q} < P$$

for $P \geq 3$. Thus the common primordial choice and the height estimates in the proof of Theorem 1.3 apply to *each* such pivot, independently of its sign. With, for example, the fixed terminal-range parameter $\alpha = 0$, they supply at least $\Phi_c(K)$ internally disjoint pairs per pivot, for any fixed $0 < c < \log 2$ and sufficiently large K . Proposition 6.2 constructs coprime blocks with the same lower bound, without factoring the large recurrence terms.

Here $K = L^{1-\delta}(1 + o(1))$, and hence

$$\log \Phi_c(K) = \exp\left((c(1-\delta) + o(1)) \frac{\log L}{\log \log L}\right).$$

This grows faster than $\log L$. Consequently $\Phi_c(K)$ exceeds every fixed power of L , and in particular exceeds

$$R = \left\lceil \frac{2(A+2)}{\mu^4} \log P \right\rceil \quad (8.8)$$

for all sufficiently large N . Retain R pairs from each pivot family.

For a retained pair $((x, d), (y, d))$ carrying the square class of D_q , form

$$Z = Y_{(x,d)} Y_{(y,d)} = h(D_q) \xi_{(x,d)} \xi_{(y,d)}.$$

The relative noise belongs to $\{-1, 0, 1\}$ and has mean μ^2 . Within a pivot family the R pairs have disjoint labels, so their relative noises are independent. Apply the argument for (8.2) with mean μ^2 to get

$$\mathbb{P}(\text{failure of the majority at } D_q) \leq \exp(-\mu^4 R/2). \quad (8.9)$$

An erased endpoint makes its pair vote zero, and a tie is a failure. The fourth power in (8.8)–(8.9) is essential.

Different pivot families may share labels. A union bound, not independence between families, yields

$$\mathbb{P}(\text{some pivot fails}) \leq \pi(P) e^{-\mu^4 R/2} \leq P P^{-A-2} = P^{-A-1}.$$

When all pivot votes are correct, the triangular reconstruction (2.2) determines all the prime signs in question. Their products then determine every $h(n)$ for $n \leq P$. The event that every relative-noise sum is positive is independent of the source.

There are at most $2\pi(P)R = O_{a,b,A}(P)$ distinct queried labels. Overlap can only reduce this number: one shared label is queried once and its received value is reused. First-occurrence seeds and their cofactor data can be prepared in time polynomial in the numerical P . The compact construction of Section 6 is polynomial in the seed length and $\log N$; accessing the first R pairs per seed and taking their votes retains a polynomial cost in P and $\log N$. All queried integers have $O(\log N)$ bits. This establishes the stated computational bound, not a bound polynomial in $\log N$ alone. $\square$

For $\delta > 1/2$, (8.7) exceeds every prefix of the form $\exp(c\sqrt{\log N})$ with c fixed. The elementary replication theorem remains useful for its direct, finite height formula. The following result preserves a different advantage: preparation polynomial in $\log N$ alone. None of these independent-noise guarantees allows a fixed positive proportion of adversarial errors.

8.4 A smaller prefix with polylogarithmic preparation

The direct Pell seeds of Section 7 give a complementary computational regime. From the seed for p , take

$$m_j + u_j \sqrt{p} = (m_0 + u_0 \sqrt{p}) \epsilon_p^j, \quad 0 \leq j < R.$$

The R readings $Q_{d_p}(m_j) = pu_j^2$ are distinct and all read $h(p)$ directly. Readings for different primes are distinct as well, since their square classes differ. Lemma 7.1 implies

$$m_j \leq \sqrt{2} \exp(6R\sqrt{p}(\log(4p) + 2)). \quad (8.10)$$

Proposition 8.3 (Polylogarithmic prefix and preparation). *Fix $A \geq 2$ and the channel parameters. There is a constant $c_{a,b,A} > 0$ such that, for all large N , the signs at all primes*

$$p \leq P = c_{a,b,A} \frac{(\log N)^2}{(\log \log N)^4} \quad (8.11)$$

are recovered with failure probability at most $(\log N)^{-A-1}$. The query count is $O_{a,b,A}(P)$, and the preparation and decoding time is polynomial in $\log N$, in the ordinary bit-operation model.

Proof. Write $L = \log N$, $l = \log L$, and take

$$D_A = \left\lceil 2(A+3)\mu^{-2} \right\rceil + 1, \quad c_{a,b,A} = (36D_A)^{-2}, \quad R = \left\lceil 2(A+3)\mu^{-2}l \right\rceil.$$

For large N , $R \leq D_A l$ and $\log(4p) + 2 \leq 3l$ throughout (8.11). Therefore the exponent in (8.10) is at most $L/2$. All readings occur at indices at most $\sqrt{2N}$. The total failure probability is at most

$$\pi(P)e^{-\mu^2 R/2} \leq L^2 L^{-A-3} = L^{-A-1}.$$

Since $\log P \asymp l$, the elementary prime-counting upper bound $\pi(P) \ll P/\log P$ shows that $\pi(P)R = O(P)$.

Sieve the primes up to P , compute their Pell units by continued fractions, obtain the direct seeds from the formulas of Lemma 7.1, and generate the required R terms by integer recurrence. Continued-fraction periods and integer lengths are polynomially bounded in the numerical p and the output length; here both are polynomial in $\log N$. In particular, searching all integers up to the potentially enormous Pell solution is unnecessary. No factorisation of the observed quadratic values is required. Finally majority decoding uses the listed readings and integer counters. $\square$

This construction also gives almost-sure eventual recovery for all N . To make the interpolation precise, prepare the queries at $T_k = 2^{k+1}$ and use them for every $2^k \leq N < 2^{k+1}$. Their indices are at most $\sqrt{2T_k} \leq 2^k$ for large k , their prime range contains the range in (8.11), and their failure probabilities are summable in k .

When $b = 0$, a non-erased repeated reading is exact. On the successful event, every multiplicative source compatible with the unerased data has the recovered small-prime signs. With flips, the majority result is instead a probabilistic recovery guarantee under the specified channel. Neither statement is resistance to an adversary who can target the query set.

8.5 The recovery regimes in one place

Table 1 compares the four independent-noise guarantees. In its last row, δ is fixed in $(0, 1)$; in every row the channel and confidence parameter are fixed. The constants $c_1, c_2, c_3 > 0$ are those in the corresponding results, and $L = \log N$. Query counts do not charge repeatedly for the same label.

The adversarial statement in Section 4 is different: $R = 2t + s + 1$ copies per pivot and $N \geq P^{4t+2s+1}$ recover a source prefix through P despite any placement of at most t wrong signs and s erasures. It assumes a bounded absolute error budget, whereas Table 1 assumes independent noise of fixed rates.

Method	Recovered targets	Failure at most	Distinct labels	Preparation and decoding
Direct Pell, Proposition 8.3	All primes up to $P = c_1 L^2 / (\log L)^4$	L^{-A-1}	$O(P)$	Polynomial in $\log N$
Replication, Theorem 8.1	One requested prime $p \leq \exp(c_2 L / \log L)$	L^{-A}	$O(L)$	Polynomial in numerical p and $\log N$
Replication, Theorem 8.1	All primes up to $P = \lfloor \exp(c_3 \sqrt{L}) \rfloor$	P^{-A-1}	$O(P)$	Polynomial in numerical P and $\log N$
Amplified pairs, Corollary 8.2	All primes up to $P = \lfloor \exp(L^\delta) \rfloor$	P^{-A-1}	$O(P)$	Polynomial in numerical P and $\log N$

Table 1: Independent noise on readings of an arbitrary unchanged source. The single-target row is not a simultaneous guarantee over all primes in its range. All rows require sufficiently large N ; their constants and thresholds are not numerical performance guarantees.

9 How much information remains hidden

Recovery of small prime signs does not imply identification of all prime signs appearing in the observations. A prime larger than $2N$ occurs in at most three labels, one on each trace. If those labels are erased, even revealing all smaller prime signs leaves that prime completely free. There are linearly many such large primes.

9.1 Exact fibres after revealing the small primes

For $N \geq 5$, let

$$\mathcal{T}_N = \{q > 2N : q \text{ prime and } q \mid Q_i \text{ for some } i \in I_N\}, \quad J_q = \{i \in I_N : q \mid Q_i\}, \quad r_q = |J_q|.$$

An observation divisible by $q > 2N$ has the unique form

$$Q_i = qa_i, \quad a_i < N/2, \tag{9.1}$$

and q has valuation one. Indeed, two factors larger than $2N$, including a repeated factor, exceed $N^2 + 2$. Two different indices $n, m \leq N$ on one trace cannot both be roots modulo q , since neither $n - m$ nor $n + m$ is a nonzero multiple of q . Thus $1 \leq r_q \leq 3$, and the sets J_q are pairwise disjoint.

Let U be a set of erased labels. If the signs at all primes at most $2N$ are supplied, every unerased label in J_q determines $h(q)$ through (9.1). If $J_q \subseteq U$, no remaining observation constrains $h(q)$. Consequently the exact number of assignments on the *relevant* prime set $\mathcal{P}_N$ consistent with these data and with the supplied head is

$$2^{Z_N(U)}, \quad Z_N(U) = \#\{q \in \mathcal{T}_N : J_q \subseteq U\}. \tag{9.2}$$

Every assignment extends to a completely multiplicative function. Primes outside $\mathcal{P}_N$ are not counted in (9.2); their additional freedom is immaterial to this finite observation.

Under independent erasure probability a , the indicators in Z_N are independent Bernoulli variables with parameters a^{r_q} . In particular,

$$\mathbb{E}z^{Z_N} = \prod_{q \in \mathcal{T}_N} (1 - a^{r_q} + a^{r_q}z), \quad \mathbb{E}Z_N \geq a^3 |\mathcal{T}_N|. \tag{9.3}$$

This is a distributional identity for the erased groups, not a rank approximation.

9.2 Linearly many large-prime groups

The following count is a specialisation of the primitive-divisor estimate of Everest–Stevens–Tamsett–Ward [7, Theorem 5.1], not a new large-prime-factor bound. Their first-occurrence characterisation shows that discarding primitive primes at most $2N$ removes only $O(\pi(2N))$ terms on a fixed trace. Every remaining term has a prime factor greater than $2N$. We retain the underlying logarithmic-mass argument to make the required error term explicit. For subsequent developments relating smooth quadratic values and primitive divisors, see Mine [12, Section 1.3, Theorem 1.4 and Corollary 1.5]; no stronger constant from that work is needed here.

Lemma 9.1 (A large factor on many indices). *For each $d \in \mathcal{D}$,*

$$\#\{n \leq N : Q_d(n) > 0, P^+(Q_d(n)) > 2N\} \geq \frac{N}{2} - O\left(\frac{N}{\log N}\right). \quad (9.4)$$

In particular $|\mathcal{T}_N|$ satisfies the same lower bound.

Proof. The logarithm of the product of the positive values of Q_d is

$$\sum_{n \leq N, Q_d(n) > 0} \log Q_d(n) = 2N \log N + O(N).$$

For an odd prime $q \leq 2N$, its total valuation in this product is at most

$$\frac{\rho_d(q)N}{q-1} + O\left(\frac{\log N}{\log q}\right),$$

where $\rho_d(q) \in \{0, 2\}$ counts the roots of Q_d modulo q . This follows by summing the root counts over $q^j \leq N^2 + 2$; each root is simple and has one lift at each level. The prime two contributes $O(N)$ to the weighted logarithmic sum.

The visible odd primes for each trace occupy two of the four odd residue classes modulo eight. The prime number theorem in these fixed progressions, followed by partial summation, gives

$$\sum_{q \leq 2N} \frac{\rho_d(q) \log q}{q-1} = \log N + O(1).$$

The fixed-modulus form, including the remainder sufficient for this weighted sum, is recorded in [1, Theorem 3.3 and the following discussion]; the fixed-progression prime number theorem is also stated in [13, Eq. 27.12.8]. The rounding errors contribute $O(\pi(2N) \log N) = O(N)$. Thus factors at most $2N$ account for at most $N \log N + O(N)$ of the logarithmic mass.

The remaining mass is at least $N \log N - O(N)$. Each index contributes at most $\log(N^2 + 2)$ to it, proving (9.4). A prime larger than $2N$ occurs at most once on a fixed trace, so the corresponding indices give distinct members of $\mathcal{T}_N$. $\square$

Theorem 9.2 (Exponential ambiguity under erasure). *Fix $0 < a < 1$ and take independent erasures on all labels. For all sufficiently large N , with probability at least*

$$1 - \exp(-a^3 N/24),$$

the erased observation, even supplemented by every prime sign at most $2N$, admits at least $2^{a^3 N/6}$ different assignments of relevant large-prime signs. Almost surely this holds for all sufficiently large N , on an event common to every source.

Proof. By Lemma 9.1, $|\mathcal{T}_N| \geq N/3$ for large N . Hence $\mathbb{E}Z_N \geq a^3 N/3$. The standard exponential-moment estimate for a sum of independent Bernoulli variables gives

$$\mathbb{P}(Z_N < \tfrac{1}{2} \mathbb{E}Z_N) \leq \exp(-\mathbb{E}Z_N/8).$$

For instance this follows from $\mathbb{E}e^{-tZ_N} \leq \exp((e^{-t} - 1)\mathbb{E}Z_N)$ and optimisation, or the weaker choice giving the displayed constant. Apply (9.2). The failure probabilities are summable over all integer N , and the event concerns only erasures, not the source. $\square$

There is an analogous obstruction within a prime prefix of linear size. For $N < q \leq 2N$, every prime is visible by a centred root, and appears in at most six labels. The groups for distinct such primes are disjoint, since a quadratic value cannot contain two factors greater than N . Revealing all other prime signs leaves every fully erased group free. There are $\pi(2N) - \pi(N) \gg N/\log N$ such groups, each erased with probability at least a^6 . Concentration therefore leaves $\gg_a N/\log N$ unidentified signs in this range with probability tending to one (indeed with summable exceptional probabilities). Thus a universal erasure decoder cannot recover all prime signs up to $2N$.

9.3 A decision-theoretic obstruction when flips are present

With flips, every assignment may have positive likelihood; literal compatibility is then not the right measure. Give the large-prime signs an independent fair prior and reveal the small-prime signs. This is a device for bounding any uniform decoder, not an assumption in our recovery theorems. Each group J_q becomes r_q independent uses of the channel (8.1) for one unknown bit.

Let

$$b_j(b) = \mathbb{P}(\text{Bin}(j, b) > j/2) + \frac{1}{2}\mathbb{P}(\text{Bin}(j, b) = j/2).$$

The Bayes error from r readings is

$$e_r(a, b) = \sum_{j=0}^r \binom{r}{j} (1-a)^j a^{r-j} b_j(b). \quad (9.5)$$

In particular $b_0 = 1/2$, $b_1 = b_2 = b$, $b_3 = 3b^2 - 2b^3$, and

$$e_3(a, b) = \frac{a^3}{2} + 3a(1-a)b + (1-a)^3(3b^2 - 2b^3). \quad (9.6)$$

More readings cannot increase the optimal Bayes error, so $e_{r_q} \geq e_3$.

Proposition 9.3 (Unrecoverable large-prime information). *Write $K_N = |\mathcal{T}_N|$. Under this prior, the largest possible probability of recovering all K_N signs is*

$$\prod_{q \in \mathcal{T}_N} (1 - e_{r_q}(a, b)) \leq e^{-e_3(a, b)K_N}. \quad (9.7)$$

The smallest expected number of wrong large-prime signs is $\sum_q e_{r_q}(a, b) \geq e_3(a, b)K_N$. These inequalities also obstruct any guarantee claimed uniformly over all deterministic sources, whenever $e_3(a, b) > 0$.

Proof. Conditionally on the data, the posterior factors across the disjoint groups, because both the prior and the noises do. The most likely complete assignment therefore chooses the most likely bit in each group. Averaging its posterior probability factors as well and gives the product in (9.7). Expected Hamming loss is additive and minimised coordinatewise, giving the sum. Finally, a guarantee holding for every deterministic source would hold after averaging over the chosen prior. The prior bounds thus imply a worst-source obstruction for each decoder; they do not say that every single deterministic source is hard for every decoder. $\square$

The small-prime recovery and the large-prime ambiguity occur in the same observation model. They are compatible because arithmetic replication supplies many independent noisy readings of selected small signs, whereas a large sign may have only one, two or three opportunities to be observed.

10 The boundary between reconstruction and a statistical inverse

The complete presentation answers which tables come from sources. Bounded-distance repair finds such a source near a received table. Replication and amplification force a growing number of disagreements whenever a specified prime sign changes. These are different tasks: a short presentation need not distribute its checks evenly over the coordinates, and a nearest source need not be the source that generated a corrupted observation.

10.1 Large prime signs can have bounded distance

Proposition 10.1. *For $N \geq 3$ and a prime $N < q \leq 2N + 1$,*

$$1 \leq m_q(N) \leq 6.$$

Consequently no decoder can universally identify $h(q)$ from these observations in the presence of three adversarial label errors.

Proof. The centred-root descent reconstructs every prime at most $2N + 1$ from labels of I_N , so positivity on all labels implies $h(q) = 1$; this proves the lower bound. For the upper bound, take the source $\beta_q(n) = (-1)^{v_q(n)}$. Each of the three quadratics has at most two roots modulo q in the index range, and $q^2 > N^2 + 2$. Thus at most six readings are negative. For any fixed source f , the two sources f and $f\beta_q$ disagree on at most six labels. Dividing those labels into two parts of size at most three produces a received word within three errors of both sources. Their signs at q differ, so universal identification is impossible. $\square$

Example 3.3 shows that a single error can already suffice at a particular height. Neither this example nor Proposition 10.1 establishes an optimal frontier for the subpolynomial prime ranges in Section 8.

10.2 What the integer-centre construction alone can supply

Proposition 10.2 (A limitation of one certificate family). *Consider all pairs obtained from integer centres $m^2 - d = pu^2$ by the factorisation identity of Lemma 5.1, for all $d \in \mathcal{D}$, keeping only pairs with both indices at most N . For every $\delta > 0$, their number is $O_\delta(N^\delta)$, uniformly in p .*

Proof. Every retained centre has $m < N$. For two centres of the same norm d , with $m_1 < m_2$, put $z_i = m_i + u_i\sqrt{p}$ and $t = z_2/z_1 > 1$. Then

$$t + t^{-1} = \frac{2(m_1m_2 - pu_1u_2)}{d}$$

is an integer larger than two, hence at least three. Therefore $t \geq (3 + \sqrt{5})/2$. Since $1 < z_i \leq 2N + 1$, there are $O(\log N)$ centres for each d , with an absolute implied constant. Each centre supplies at most $\tau(m^2 - d)/2$ unordered factor pairs. The elementary bound $\tau(v) \ll_\epsilon v^\epsilon$, uniform in v , with $v \leq N^2 + 2$, completes the proof after absorbing the logarithm. $\square$

This proposition is about the specified integer-centre family, not all two-label certificates and not $m_p(N)$. A general pair of one trace with $Q_d(x)Q_d(y) = pz^2$ has a rational centre

$$m = \frac{xy + d}{x + y}, \quad u = \frac{z}{x + y}, \quad m^2 - pu^2 = d;$$

its denominator need not be one. Moreover a small available certificate family is not an upper bound on the minimum number of negative readings forced by genuine multiplicative sources.

10.3 The remaining inverse question

For each fixed p , Theorem 1.3 exceeds every fixed power of $\log N$, but its stated lower bound is smaller than N^δ for every fixed $\delta > 0$. This last statement concerns the bound, not the unknown order of $m_p(N)$. In particular it does not show that $m_p(N) = o(N)$.

A bound $m_p(N) \geq c_p N$ for every fixed prime and all large N would imply the following qualitative inverse: if a fixed source is positive on all but $o(N)$ of the three traces, then it is identically one. Indeed any negative prime would contradict that bound. The reverse implication is not asserted, since the minimising source in $m_p(N)$ may vary with N .

The appendices identify restrictions under which a linear conclusion is available, and isolate an exact large-prime elimination. Their hypotheses are not consequences of a small trace error. They therefore delimit, rather than close, the unrestricted inverse problem. In particular, preserving the observation of an arbitrary source throughout this article is essential: constructing a special source that encodes a message would solve a different recovery problem.

A Exact elimination and localisation of large factors

The minimum $m_p(N)$ can be reduced to signs at primes at most $2N$, but shared large primes leave a nonzero cost. The reduction is useful precisely because it retains that cost instead of treating all large signs as independently adjustable observations.

Assume $N \geq 5$ and $p \leq 2N$. Let $S_N = \{i \in I_N : P^+(Q_i) \leq 2N\}$. For a completely multiplicative assignment κ on the primes at most $2N$, define

$$A_N(\kappa) = \sum_{i \in S_N} \frac{1 - \kappa(Q_i)}{2}, \quad \phi_q(\kappa) = \frac{r_q - \left| \sum_{i \in J_q} \kappa(a_i) \right|}{2},$$

using the groups and cofactors in (9.1).

Proposition A.1 (The residual cost is exact). *One has*

$$m_p(N) = \min_{\kappa(p)=-1} \left(A_N(\kappa) + \sum_{q>2N} \phi_q(\kappa) \right). \quad (\text{A.1})$$

For a fixed source h with restriction κ , the expression inside the minimum is a lower bound for $E_N(h)$, not necessarily its value.

Proof. Once κ is fixed, the cost of the group J_q is

$$\sum_{i \in J_q} \frac{1 - h(q)\kappa(a_i)}{2}.$$

Minimising over the one sign $h(q)$ gives ϕ_q . The groups are disjoint and all cofactors lie below $N/2$, so these minimisations are independent and are simultaneously attained by choosing the sign of each cofactor sum (arbitrarily in a tie). This proves equality after minimisation and the stated inequality for an unchanged source. $\square$

If $u_i = \kappa(a_i)$, the three possibilities are

$$\phi_q = \begin{cases} 0, & r_q = 1, \\ (1 - u_1 u_2)/2, & r_q = 2, \\ (3 - u_1 u_2 - u_1 u_3 - u_2 u_3)/4, & r_q = 3. \end{cases} \quad (\text{A.2})$$

Each shared group costs zero or one. For example, at $N = 20$, the prime 41 divides $9^2 + 1 = 2 \cdot 41$, $11^2 + 2 = 3 \cdot 41$ and $17^2 - 2 = 7 \cdot 41$. Its cost vanishes exactly when $\kappa(2), \kappa(3), \kappa(7)$ agree. These values remain multiplicative functions of small-prime signs; they are not independent signs assigned to three abstract vertices.

A shared prime larger than $2N$ belongs to the class 1 (mod 8). Indeed, a prime in any of the other odd classes has roots for only one of the three quadratics, whereas J_q contains at most one label of each trace. This fact locates the shared groups but does not make their energy expand.

Lemma A.2 (Uniform counting with two fixed cofactors). *Let $1 \leq a, b \leq Y \leq N$ and let $d, e \in \mathcal{D}$ be distinct. The number of positive solutions $n, m \leq N$ of*

$$bn^2 - am^2 = bd - ae \quad (\text{A.3})$$

is $O_\epsilon(N^\epsilon)$ for every $\epsilon > 0$, uniformly in all these parameters.

Proof. Put $K = b(bd - ae)$ and $X = bn$. If $K = 0$, the positive ratio $a/b = d/e$ is either 2 or $1/2$; equation (A.3) would make that ratio a rational square. Thus there is no solution. Suppose $K \neq 0$. Then

$$X^2 - abm^2 = K, \quad |K| \leq 4Y^2.$$

If ab is a square, factoring the left-hand side gives at most $2\tau(|K|)$ possibilities. Otherwise write $ab = D_0 c^2$ with D_0 squarefree. Each solution yields an algebraic integer $\eta = bn + cm\sqrt{D_0}$ of norm K in a real quadratic field. There are at most $\tau(|K|)$ integral ideals of norm $|K|$: for a rational prime occurring to exponent v , at most $v + 1$ allocations between the primes above it are possible.

Two positive generators of the same ideal and the same norm differ by a unit of norm one. If their ratio exceeds one, its trace is an integer at least three, so the ratio is at least $(3 + \sqrt{5})/2$. Meanwhile

$$(2NY)^{-1} \leq \eta \leq 2NY,$$

since both embeddings have absolute value at most $2NY$ and $|K| \geq 1$. There are therefore $O(\log(2NY))$ such generators per ideal. The pair (n, m) is determined by η . We obtain $O(\tau(|K|) \log(2NY))$, and the divisor bound $\tau(v) \ll_\delta v^\delta$ proves the assertion. The argument uses factorisation of ideals in a quadratic field, not an estimate for its regulator or class number. $\square$

Let $J_N(R)$ be the number of primes $q > R$ appearing on at least two labels, where $2N \leq R \leq N^2 + 2$. Choosing two of their labels and writing

$$n^2 - d = qa, \quad m^2 - e = qb$$

gives (A.3), with $d \neq e$ and $a, b \leq (N^2 + 2)/R$. There are at most three unordered trace pairs. Lemma A.2 consequently gives

$$J_N(R) \ll_\epsilon N^\epsilon \left(\frac{N^2 + 2}{R} \right)^2. \quad (\text{A.4})$$

Define the truncated minimum by retaining only labels with $P^+(Q_i) \leq R$:

$$m_p^{\leq R}(N) = \min_{h(p)=-1} \sum_{\substack{i \in I_N \\ P^+(Q_i) \leq R}} \mathbf{1}_{h(Q_i)=-1}.$$

Theorem A.3 (Localisation of the minimum). *Uniformly for $p \leq 2N$ and $2N \leq R \leq N^2 + 2$,*

$$0 \leq m_p(N) - m_p^{\leq R}(N) \leq J_N(R) \ll_{\epsilon} N^{\epsilon} \left(\frac{N^2 + 2}{R} \right)^2. \quad (\text{A.5})$$

In particular, for fixed $0 < \delta < 1/2$,

$$m_p(N) = m_p^{\leq N^{3/2+\delta}}(N) + O_{\epsilon}(N^{1-2\delta+\epsilon}).$$

Proof. The truncated version of (A.1) removes exactly the terms ϕ_q with $q > R$. Their sum is nonnegative and at most $J_N(R)$, since singleton groups cost zero and every shared group costs at most one. These bounds hold for each κ before minimisation, so they hold for the difference of minima. Equation (A.4) finishes the proof. $\square$

Choose $\epsilon < 2\delta$ to make the displayed remainder $o(N)$. The concrete choice $R = N^{7/4}$ gives $O_{\epsilon}(N^{1/2+\epsilon})$. These are estimates on minima: a fixed source may have many negative readings on the removed singleton groups, even though their signs can be optimised freely in the minimisation.

A related localisation holds for certificates with unit loads. If a certificate for p meets a label containing $q > R$, it must meet another label of J_q , because the total q -valuation is even. It therefore meets the union of shared groups above R , which has at most $3J_N(R)$ labels. Summing the unit-load inequalities over those labels bounds the total weight of all such certificates by $3J_N(R)$. This does not construct a positive-density family; it only bounds the portion that could lie above the cutoff.

B Linear separation under a local prime budget

The unrestricted minimum allows every other prime sign to depend on N . A useful controlled class only restricts negative primes below N , leaving all signs above N arbitrary. Smooth values of a quadratic see no part of that upper tail.

A direct antecedent is Teräväinen's pretentious-case theorem [16, Theorem 2.9]. For a fixed completely multiplicative function g pretending to a Dirichlet character times n^{it} , an admissible pair (F, g) and property S of F , it bounds the limiting upper modulus of the mean of $g(F(n))$ strictly below one. For sign-valued g , this gives positive lower proportions of both signs. Admissibility is a hypothesis of that statement, not a consequence of pretentiousness alone. The transfer below instead keeps a uniform threshold over mobile families described by a local prime budget, with all signs above N free. It uses the same smooth-value mechanism, but records the finite-head law and the cost of the remaining visible primes explicitly.

B.1 The smooth-value input and the finite local law

We use property S from [16, Definition 2.8 and Proposition 2.10]. For each $d \in \mathcal{D}$ there is $\eta_d > 0$ such that, for every *fixed* modulus $W \geq 1$ and residue r ,

$$\liminf_{N \rightarrow \infty} \frac{1}{N} \#\{n \leq N : n \equiv r \pmod{W}, Q_d(n) > 0, P^+(Q_d(n)) \leq n\} \geq \frac{\eta_d}{W}. \quad (\text{B.1})$$

The same η_d works for all fixed W, r , but the threshold may depend on them. This is the published quadratic smooth-value input; no uniformity for moduli growing with N is assumed here. We may decrease η_d so that $\eta_d \leq 1$.

For fixed $Y \geq 2$, let $h_{\leq Y}$ retain the signs of h at primes at most Y and equal one at all other primes. For odd q , let $\rho_d(q)$ be the number of roots of Q_d modulo q . Set

$$H_{d,h}(Y, N) = \sum_{\substack{Y < q \leq N \\ h(q) = -1, \rho_d(q) = 2}} \frac{1}{q}, \quad H_h(Y, N) = \sum_{\substack{Y < q \leq N \\ h(q) = -1}} \frac{1}{q}, \quad (\text{B.2})$$

$$L_{d,Y}(h) = \begin{cases} 0, & h(2) = -1, \\ \prod_{\substack{3 \leq q \leq Y \\ h(q) = -1}} \left(1 - \frac{2\rho_d(q)}{q+1}\right), & h(2) = 1, \end{cases} \quad \delta_{d,Y}(h) = \frac{1 - L_{d,Y}(h)}{2}. \quad (\text{B.3})$$

All sums and products indexed by q in this appendix are over primes.

The quantity $\delta_{d,Y}(h)$ is exactly the natural density of negative readings of $h_{\leq Y}$ on trace d . At an odd prime, simple-root lifting gives

$$\text{dens}\{v_q(Q_d(n)) = j\} = \frac{\rho_d(q)(q-1)}{q^{j+1}} \quad (j \geq 1).$$

The density of odd valuation is $\rho_d(q)/(q+1)$, giving the local factor in (B.3). Valuation at two is zero or one, each on one parity class. Truncate the valuations at the finitely many primes, apply the Chinese remainder theorem, and let the valuation truncations increase to obtain the product law. All its odd factors lie in $[0, 1]$.

The condition $P^+(Q_d(n)) \leq n$ has a second purpose besides removing the upper tail: any changed prime divisor q satisfies $n \geq q$. Counting its root classes therefore starts after the first incomplete block modulo q . The transfer below uses this fact to avoid an additive error for every changed prime.

Theorem B.1 (Uniform smooth-core transfer). *For every fixed $Y \geq 2$ and $\epsilon > 0$, all sufficiently large N satisfy, for every source h and every d ,*

$$\frac{E_{d,N}(h)}{N} \geq \eta_d \delta_{d,Y}(h) - 2H_{d,h}(Y, N) - \epsilon, \quad (\text{B.4})$$

$$\frac{E_{d,N}(h)}{N} \leq 1 - \eta_d(1 - \delta_{d,Y}(h)) + 2H_{d,h}(Y, N) + \epsilon, \quad (\text{B.5})$$

where $E_{d,N}(h)$ counts the negative readings of trace d . The threshold is independent of h , and no signs at primes above N are restricted.

Proof. Let $B_d(N)$ be the smooth set in (B.1). Choose fixed valuation cutoffs at primes at most Y so that their exceptional residue classes have total density at most a small $\tau > 0$. Off these classes the sign of $h_{\leq Y}(Q_d(n))$ is determined modulo a fixed product W of prime powers. Its negative classes occupy at least the proportion $\delta_{d,Y}(h) - \tau$, and its positive classes at least $1 - \delta_{d,Y}(h) - \tau$. Equation (B.1), summed over these classes, gives at least

$$N(\eta_d \delta_{d,Y}(h) - O(\tau)), \quad N(\eta_d(1 - \delta_{d,Y}(h)) - O(\tau))$$

negative and positive smooth readings, respectively. One threshold suffices for all residues and all assignments at the finitely many primes at most Y .

On $B_d(N)$ a disagreement between h and $h_{\leq Y}$ requires a negative prime $Y < q \leq n \leq N$ dividing $Q_d(n)$. For each root modulo q , the additional condition $n \geq q$ leaves at most $\lfloor N/q \rfloor$ such indices: write $n = r + kq$ with $0 < r < q$ and $k \geq 1$. Thus the total number of disagreements on the smooth set is at most $2NH_{d,h}(Y, N)$. There is no additive error per prime in this count. Subtract it from each of the two smooth counts and choose τ in terms of ϵ . $\square$

B.2 Uniformly tight tails and a necessary escape of mass

Let $\mathcal{H}_N$ be any family of sources such that

$$\lim_{Y \rightarrow \infty} \limsup_{N \rightarrow \infty} \sup_{h \in \mathcal{H}_N} H_h(Y, N) = 0. \quad (\text{B.6})$$

An empty supremum in this nonnegative budget is zero. Put $\mathcal{D}_2 = \mathcal{D}$, and, for odd p , let $\mathcal{D}_p = \{d \in \mathcal{D} : (d/p) = 1\}$. It is nonempty by quadratic reciprocity. Finally set

$$a_2 = \frac{1}{2}, \quad a_p = \frac{2}{p+1} \ (p \text{ odd}), \quad \Gamma_p = a_p \sum_{d \in \mathcal{D}_p} \eta_d > 0.$$

If $Y \geq p$, $h(p) = -1$ and $d \in \mathcal{D}_p$, then $\delta_{d,Y}(h) \geq a_p$: the other nonnegative local factors cannot increase the first moment beyond the one with only p negative.

Corollary B.2 (A linear bound with free upper tail). *Under (B.6), for each fixed prime p ,*

$$\liminf_{N \rightarrow \infty} \inf_{\substack{h \in \mathcal{H}_N \\ h(p) = -1}} \frac{E_N(h)}{N} \geq \Gamma_p.$$

In particular (B.6) holds if, for fixed $0 < \sigma < 1$ and $M < \infty$,

$$\sum_{\substack{q \leq N \\ h(q) = -1}} q^{-\sigma} \leq M \quad (h \in \mathcal{H}_N). \quad (\text{B.7})$$

If $h(2) = -1$, each of the two signs has lower asymptotic proportion at least $\eta_d/2$ on every trace, uniformly within such a family.

Proof. Sum (B.4) over $\mathcal{D}_p$, take the infimum and lower limit in N , then let $Y \rightarrow \infty$ through (B.6) and finally $\epsilon \rightarrow 0$. Condition (B.7) gives $H_h(Y, N) \leq MY^{\sigma-1}$, proving tightness. For $h(2) = -1$, the local density is $1/2$ on every trace, so both (B.4) and (B.5) apply symmetrically. $\square$

These are bounds for restricted families, not lower bounds for the unrestricted minimum. They nevertheless impose a condition on any hypothetical quasi-saturation. If $h_N(p) = -1$ and $E_N(h_N) = o(N)$, then, for every fixed $Y \geq \max(2, p)$ and $d \in \mathcal{D}_p$,

$$\liminf_{N \rightarrow \infty} H_{d, h_N}(Y, N) \geq \eta_d a_p / 2. \quad (\text{B.8})$$

This follows directly from (B.4). In particular every budget in (B.7) must diverge: for $q > Y$, $q^{-\sigma} \geq Y^{1-\sigma}/q$; choose Y first and then N . The mass required by (B.8) can be shared by the three traces through primes $1 \pmod{8}$. The inequalities do not themselves rule out such a shared tail.

C A minimum under a cardinality constraint

A small number of negative primes is different from a small harmonic budget. Here the negative primes may lie anywhere below the maximal observation height $N^2 + 2$. A uniform small-prime model, followed by an incidence bound for the remaining primes, determines the first-order minimum in this class.

Let

$$k_N(h) = \#\{q \leq N^2 + 2 : q \text{ prime}, h(q) = -1\}, \quad m_{p,K}(N) = \min_{h(p) = -1, k_N(h) \leq K} E_N(h).$$

For p fixed and N large this class is nonempty when $K \geq 1$. Put

$$\gamma_2 = \frac{3}{2}, \quad \gamma_p = \frac{2|\mathcal{D}_p|}{p+1} \quad (p \text{ odd}). \quad (\text{C.1})$$

Thus $\gamma_p = 6/(p+1)$ for $p \equiv 1 \pmod{8}$ and $2/(p+1)$ in the other odd classes.

Theorem C.1 (Restricted minimum). *There are absolute constants $C, \delta_0 > 0$ such that, for each fixed prime p , all sufficiently large N and every $1 \leq K \leq N^{\delta_0}$,*

$$\left| \frac{m_{p,K}(N)}{N} - \gamma_p \right| \leq C \left(\frac{\log(K+1)}{\log N} + \frac{1}{\sqrt{\log N}} \right). \quad (\text{C.2})$$

In particular $m_{p,K_N}(N)/N \rightarrow \gamma_p$ whenever $\log(K_N+1) = o(\log N)$ and $K_N \geq 1$.

C.1 The local distribution of three signs

Observe n uniformly in $\{2, \dots, N\}$, so all three values are positive. The two additional labels at $n = 1$ change a total count by at most two. For nonempty $J \subseteq \mathcal{D}$, define

$$P_J(T) = \prod_{d \in J} (T^2 - d), \quad \rho_J(q) = \sum_{d \in J} \rho_d(q) \quad (q \text{ odd}).$$

The roots of the factors are disjoint and simple at every odd prime. Only the differences 1, 3, 4 between the constants could cause an overlap; at three, the two factors whose constants agree have no root.

Define a law $\pi_{h,y}$ on $\{\pm 1\}^3$ by multiplying independent local vectors over primes at most y . A positive prime contributes $(1, 1, 1)$. At an odd negative prime q , the local vector flips exactly coordinate d with probability $\rho_d(q)/(q+1)$ and flips none with the remaining probability. If $h(2) = -1$, the factor at two is $(-, +, +)$ or $(+, -, -)$, each with probability $1/2$. These probabilities are nonnegative and sum to one: a prime with all three traces visible is at least seventeen, while all other odd primes see only one trace.

The moment of the product of the coordinates in J is

$$M_J(h, y) = a_J(h) \prod_{\substack{3 \leq q \leq y \\ h(q) = -1}} \left(1 - \frac{2\rho_J(q)}{q+1} \right), \quad (\text{C.3})$$

where $a_J(h) = 1$ if $h(2) = 1$, and otherwise

$$a_J(h) = \frac{(-1)^{\mathbf{1}_{-1 \in J}} + (-1)^{\mathbf{1}_{-2 \in J} + \mathbf{1}_{2 \in J}}}{2}.$$

The empty moment is one. The law is a model for the observation at a random index; its independent prime factors are not a randomness assumption on h .

Proposition C.2 (Uniform local-model comparison). *There are absolute $C_0, U_0 > 0$ such that, for $2 \leq y \leq N$ and $u = \log N / \log y \geq U_0$,*

$$\sup_h d_{\text{TV}}(\mathcal{L}_N((h_{\leq y}(Q_d(n)))_{d \in \mathcal{D}}), \pi_{h,y}) \leq C_0 \left(\frac{1}{u} + \frac{(1 + \log N)^{11}}{\sqrt{N}} \right). \quad (\text{C.4})$$

Here $\mathcal{L}_N$ refers to uniform $2 \leq n \leq N$, and d_{TV} is the supremum over events, equivalently half the ℓ^1 distance on this finite space.

C.2 The sieve input and its application

We use the valuation comparison of Gorodetsky [8, Theorem 2.3]. We specify the form consumed in the present argument. Let A be a positive integer-valued random variable of bounded support, let $\mathcal{P}$ be a finite set of primes at most y , and let g be multiplicative on the semigroup $\langle \mathcal{P} \rangle$, with $g(1) = 1$, $g(q) < 1$, and $g(q^j)$ decreasing to zero. Its dimension condition is a bound, uniform in $m \in \langle \mathcal{P} \rangle$,

$$\prod_{a \leq q \leq b, q \in \mathcal{P}} \left(1 - \frac{g(qm)}{g(m)}\right)^{-1} \leq \left(\frac{\log b}{\log a}\right)^\kappa \exp(B/\log a), \quad 2 \leq a \leq b. \quad (\text{C.5})$$

All $g(m)$ in our application are positive. Let G_q be independent with $\mathbb{P}(G_q \geq j) = g(q^j)$ and put $R = \prod_{q \in \mathcal{P}} q^{G_q}$. For $S/T \geq y$, the imported estimate bounds the total variation of $(v_q(A))_{q \in \mathcal{P}}$ from $(G_q)_{q \in \mathcal{P}}$ by a constant times $D_1 + D_2$, where the terms used here have the form

$$D_1 = \mathbb{P}(R > T) + \mathbb{E} \left[\mathbf{1}_{R \leq T} f\left(\frac{\log(S/R)}{\log y}\right) \right], \quad (\text{C.6})$$

$$D_2 = \sum_{\substack{m \leq S \\ m \in \langle \mathcal{P} \rangle}} |\mathbb{P}(m \mid A) - g(m)| \left(2^{\omega(m)} + \prod_{q \in \mathcal{P}} \left(1 + \frac{g(qm)}{g(m)}\right) \right). \quad (\text{C.7})$$

Here $f(t) = \exp\{-t \log t + t \log_3 \max(t, 100) + C_* t\}$, with $\log_3$ denoting the threefold iterated natural logarithm. The constants depend on the fixed dimension data. We only apply this estimate when its argument tends into a range on which $f \leq 1$ and its tail supremum is $O(1/t)$. The proof of this sieve theorem is external; the substitutions and costs below are part of the present proof.

Proof of Proposition C.2. Fix nonempty J and a parity class. Let $A = P_J(n)$ with n uniform on that class in $\{2, \dots, N\}$, of cardinal $L_b \asymp N$. Its support is contained in $[1, (N^2 + 2)^3]$; this is the support-height parameter, distinct from the index length N . Take

$$\mathcal{P} = \{q \leq y : q \text{ odd}, \rho_J(q) > 0\}, \quad g(q^j) = \rho_J(q)/q^j.$$

By the Chinese remainder theorem,

$$|\mathbb{P}(m \mid A) - g(m)| \leq \rho_J(m)/L_b, \quad \rho_J(m) = \prod_{q \mid m} \rho_J(q) \leq 6^{\omega(m)}. \quad (\text{C.8})$$

The ratio in (C.5) is $\rho_J(q)/q$ when $q \nmid m$ and $1/q$ otherwise. Mertens' estimate gives (C.5) with $\kappa = 6$ and an absolute B , uniformly over all seven J . Indeed the logarithms of the factors are at most $6/q + O(q^{-2})$ at the large primes; the finitely many primes at most eleven are absorbed into B .

Take $S = N^{1/2}$ and $T = N^{1/4}$. For $u \geq 4$, $S/T \geq y$. The model has

$$\mathbb{E} \log R = \sum_{q \in \mathcal{P}} \frac{\rho_J(q) \log q}{q - 1} \ll \log y.$$

On $R \leq N^{1/8}$, the argument of f is at least $3u/8$; on $R \leq T$ it is at least $u/4$. Increase U_0 so that $f \leq 1$ on the latter range and $\sup_{t \geq 3u/8} f(t) \ll 1/u$. Markov's inequality gives $D_1 \ll 1/u$.

The product in (C.7) is at most $\prod_{q \leq y} (1 + 6/q) \ll (1 + \log y)^6$. Therefore

$$\begin{aligned} D_2 &\ll \frac{1}{N} \sum_{m \leq S} 6^{\omega(m)} (2^{\omega(m)} + (1 + \log y)^6) \\ &\ll \frac{S}{N} ((1 + \log S)^{11} + (1 + \log y)^6 (1 + \log S)^5) \ll \frac{(1 + \log N)^{11}}{\sqrt{N}}. \end{aligned}$$

We used $r^{\omega(m)} \leq \tau_r(m)$ and $\sum_{m \leq S} \tau_r(m) \leq S(1 + \log S)^{r-1}$, obtained by summing over products of r positive integers. No estimate uniform in a growing polynomial degree is needed.

Every assignment of small-prime signs is a bounded test of the valuation vector. Multiplying by the deterministic factor at two in the chosen parity class and averaging the two classes gives an error $O(D_1 + D_2 + 1/N)$ in each of the seven moments (C.3). Finite Fourier inversion on $\{\pm 1\}^3$ proves (C.4), uniformly in h . $\square$

C.3 Paying for the primes omitted from the model

If at most K negative primes lie between $y > 3$ and $N^2 + 2$, then

$$|E_N(h) - E_N(h_{\leq y})| \leq 6K(N/y + 1). \quad (\text{C.9})$$

A changed reading requires one of these primes to divide a quadratic value; each such prime meets at most $2N/q + 2$ labels on a given trace. Union over the primes and three traces proves the bound.

Proof of Theorem C.1. Take $\delta_0 < \min(1/4, 1/(2U_0))$ and

$$y = (K + 1) \exp \sqrt{\log N}.$$

For p fixed and N large, $p \leq y$ and $u \geq U_0$, uniformly for $K \leq N^{\delta_0}$. Every singleton moment has nonnegative odd-prime factors. If $h(p) = -1$, its local negative probability is at least $1/2$ for $p = 2$ and $2/(p+1)$ on each visible trace for odd p . Summing over the visible traces gives γ_p . Proposition C.2 and (C.9) thus imply

$$\frac{E_N(h)}{N} \geq \gamma_p - O\left(\frac{\log(K+1)}{\log N} + \frac{1}{\sqrt{\log N}}\right).$$

Indeed the additional normalised tail cost is at most $6e^{-\sqrt{\log N}} + 6N^{\delta_0-1}$, and the sieve remainder is also absorbed.

For the opposite inequality, use the source negative only at p . Simple-root lifting and the alternating sum of the conditions $p^j \mid Q_d(n)$ give $2N/(p+1) + O_p(\log N)$ negative labels on each visible trace when p is odd. At two the total is $3N/2 + O(1)$. This source belongs to every class $K \geq 1$ and attains $\gamma_p N + O_p(\log N)$. The threshold may depend on p , as stated. $\square$

Consequently, for each fixed p there is $\delta_p > 0$ such that $h(p) = -1$ and $k_N(h) \leq N^{\delta_p}$ imply $E_N(h) \geq \gamma_p N/2$ for large N . A sequence with $h_N(p) = -1$ and $E_N(h_N) = o(N)$ must therefore have more than N^{δ_p} negative primes. The same conclusion holds when only primes appearing at odd valuation in the observations are counted: changing all inactive signs to positive does not alter a reading, and p itself is active for large N .

This restriction is not automatic in the free problem. It is also not equivalent to Appendix B: a subpolynomial number of negative primes can have growing harmonic mass, whereas a local harmonic bound permits arbitrarily many negative primes above N .

D Sources close to a moving quadratic character

The preceding cardinality bound measures distance from the constant-one source. Another structured class is close to a quadratic character whose conductor can grow. The ramified prime must be retained: deleting its multiples would lose a positive proportion of readings when the conductor is fixed.

For a prime $\ell \geq 5$, let χ_ℓ be the Legendre character and, for $\epsilon \in \{\pm 1\}$, define its nonvanishing completion by

$$g_{\ell, \epsilon}(m) = \epsilon^{v_\ell(m)} \chi_\ell(m/\ell^{v_\ell(m)}).$$

For a source h , set $\epsilon = h(\ell)$ and $\eta = hg_{\ell, \epsilon}$, so $\eta(\ell) = 1$. Count corrections by

$$D_{\ell, N}(h) = \#\{q \leq N^2 + 2 : q \text{ prime}, q \neq \ell, h(q) \neq \chi_\ell(q)\}.$$

Theorem D.1 (Mobile conductor, few corrections). *Fix $0 < \tau < 2$ and $K_N \geq 0$ with $\log(K_N + 1) = o(\log N)$. Uniformly over primes $5 \leq \ell \leq N^{2-\tau}$ and sources with $D_{\ell, N}(h) \leq K_N$, each trace contains at least $(1/2 - o(1))N$ negative labels and $(2/5 - o(1))N$ positive labels. If in addition $\ell \rightarrow \infty$, then every three-sign pattern has frequency $1/8 + o(1)$ at a common uniform index $2 \leq n \leq N$.*

D.1 The law at the conductor and sums in progressions

Choose r uniformly modulo ℓ . Form the vector $(\chi_\ell(Q_d(r)))_d$; if one coordinate is zero, replace it by a fair sign. Since $\ell \geq 5$, the three polynomials are separable and do not share a root, so at most one replacement is needed. This defines a law ν_ℓ on $\{\pm 1\}^3$ whose moments are

$$c_I(\ell) = \frac{1}{\ell} \sum_{r \bmod \ell} \chi_\ell(P_I(r)), \quad c_\emptyset = 1.$$

For a singleton $I = \{d\}$, $c_I = -1/\ell$: count the $\ell - 1$ pairs of nonzero factors of d using $(r - z)(r + z) = d$. For any nonempty I , the Weil bound gives $c_I \ll \ell^{-1/2}$, uniformly over the seven possibilities. Hence

$$d_{\text{TV}}(\nu_\ell, \text{Unif}(\{\pm 1\}^3)) \ll \ell^{-1/2}. \quad (\text{D.1})$$

The mixed character-sum form used below is [11, Lemma 3.1]: for a squarefree polynomial of degree at most six and every additive frequency, the complete multiplicative-additive sum is $O(\sqrt{\ell})$. The non-square condition is satisfied by each P_I modulo ℓ . This is a classical Weil estimate, not a new finite-field bound.

Lemma D.2 (All ramified valuations retained). *Let $(M, \ell) = 1$, $5 \leq \ell < N^2$, and let $\mathcal{A} = \{2 \leq n \leq N : n \equiv r \pmod{M}\}$ have cardinality L . For nonempty $I \subseteq \mathcal{D}$,*

$$\sum_{n \in \mathcal{A}} g_{\ell, \epsilon}(P_I(n)) = c_I(\ell)L + O(\sqrt{\ell} \log(2N)), \quad (\text{D.2})$$

uniformly in M, r, I, ϵ, ℓ .

Proof. For any positive integer A ,

$$g_{\ell, \epsilon}(A) = \sum_{j \geq 0} \epsilon^j \mathbf{1}_{\ell^j | A} \chi_\ell(A/\ell^j). \quad (\text{D.3})$$

Only the term $j = v_\ell(A)$ is nonzero. The term $j = 0$ in (D.3), summed on $\mathcal{A}$, has mean c_I and error $O(\sqrt{\ell} \log(2\ell))$: remove complete periods and use Fourier completion on the remaining interval with the stated mixed Weil estimate.

For $j \geq 1$, there are at most six simple roots of P_I modulo ℓ^j . Combining one such root with the progression modulo M gives $n = b + M\ell^j k$, and

$$\frac{P_I(b + M\ell^j k)}{\ell^j} \equiv \frac{P_I(b)}{\ell^j} + MP'_I(b)k \pmod{\ell}.$$

Its slope is nonzero modulo ℓ . The character of this linear polynomial has zero complete mean, so its interval sum is $O(\sqrt{\ell} \log(2\ell))$ by the same completion argument. Terms with a deeper valuation are automatically zero here. Since $P_I(n) \leq (N^2 + 2)^3$, there are $O(\log(2N)/\log \ell)$ relevant j . Summing their errors proves (D.2). $\square$

The fair replacement in ν_ℓ thus represents the vanishing mean of the unit part on the ramified strata. It is not an additional randomisation of h .

D.2 A positive tilt makes the sieve comparison applicable

Let $\pi_{\eta,y}^{(\ell)}$ be the local law of Appendix C for the correction signs, omitting the prime ℓ . Write its moments as $M_J(\eta, y)$. For a singleton, $0 \leq M_{\{d\}} \leq 1$. Put

$$X = N/\sqrt{\ell}, \quad v = \log X / \log y, \quad e_{N,\ell}(y) = \frac{1}{v} + \frac{(1 + \log N)^{12}}{\sqrt{X}}.$$

We claim that, for v larger than an absolute constant,

$$d_{\text{TV}}(\mathcal{L}_N(G, H), \nu_\ell \otimes \pi_{\eta,y}^{(\ell)}) \ll e_{N,\ell}(y), \quad (\text{D.4})$$

where $G = (g_{\ell,\epsilon}(Q_d(n)))_d$ and $H = (\eta_{\leq y}(Q_d(n)))_d$, and n is uniform in $\{2, \dots, N\}$.

To prove this, fix nonempty I, J and one parity class. Let $A = P_J(n)$, $\xi = g_{\ell,\epsilon}(P_I(n))$, and $\mu_0 = \mathbb{E}\xi$. Choose $s \in \{\pm 1\}$ with $s\mu_0 \geq 0$ and set

$$W = \frac{1 + s\xi}{2} \in \{0, 1\}, \quad \beta = \mathbb{E}W = \frac{1 + s\mu_0}{2} \geq \frac{1}{2}.$$

Weighting by W/β gives a genuine probability law. No sieve theorem is being applied to a signed measure.

Take the prime set of Appendix C for P_J , with ℓ removed, and the same $g(q^j) = \rho_J(q)/q^j$. For m in its semigroup, the Chinese remainder theorem and Lemma D.2, applied to each root progression of modulus $2m$, give

$$\begin{aligned} \mathbb{P}(m \mid A) &= g(m) + O(\rho_J(m)/N), \\ \mathbb{E}(\xi \mathbf{1}_{m \mid A}) &= c_I(\ell)g(m) + O\left(\rho_J(m) \frac{\sqrt{\ell} \log(2N)}{N}\right), \\ \mu_0 &= c_I(\ell) + O(\sqrt{\ell} \log(2N)/N). \end{aligned}$$

Since $2\beta \geq 1$, the exact normalisation

$$\mathbb{P}_W(m \mid A) = \frac{\mathbb{P}(m \mid A) + s\mathbb{E}(\xi \mathbf{1}_{m \mid A})}{2\beta}$$

yields

$$|\mathbb{P}_W(m \mid A) - g(m)| \ll \rho_J(m) \frac{\sqrt{\ell} \log(2N)}{N}. \quad (\text{D.5})$$

This is the arithmetic step which supplies the comparison of the model and correction vectors; their independence has not been assumed.

Apply (C.6)–(C.7) to both the ordinary and tilted laws with $S = X^{1/2}$ and $T = X^{1/4}$. Their integer support height remains $(N^2 + 2)^3$, not X . The dimension constants are unchanged by deleting ℓ . The same estimate of $\mathbb{E} \log R$ gives $D_1 \ll 1/v$. From (D.5) and the divisor sums used earlier,

$$D_2 \ll \frac{\log(2N)}{X} \sum_{m \leq S} 6^{\omega(m)} (2^{\omega(m)} + (1 + \log y)^6) \ll \frac{(1 + \log N)^{12}}{\sqrt{X}}.$$

Thus a bounded product F of the odd correction signs has the same model mean under both probability laws, up to $O(e_{N,\ell}(y))$. As $\xi = s(2W - 1)$,

$$\mathbb{E}(\xi F) = s(2\beta \mathbb{E}_W F - \mathbb{E}F) = c_I(\ell)M_J^{\text{odd}} + O(e_{N,\ell}(y)).$$

Reinsert the deterministic factor at two on each parity class and average the two classes. This gives the mixed moment $c_I(\ell)M_J(\eta, y)$ with the same error. If either I or J is empty, the ordinary sieve comparison or Lemma D.2 applies directly. Fourier inversion over the sixty-four points of $\{\pm 1\}^3 \times \{\pm 1\}^3$ proves (D.4).

D.3 From the joint model to complete readings

If at most K corrections lie above y , their effect has probability $O(K/y + K/N)$ by the incidence bound (C.9). Multiplication of the two vectors contracts total variation. Consequently

$$d_{\text{TV}}(\mathcal{L}_N((h(Q_d(n))))_d, \nu_\ell * \pi_{\eta, y}^{(\ell)}) \ll e_{N, \ell}(y) + K/y + K/N, \quad (\text{D.6})$$

where $*$ means coordinatewise multiplication of independent vectors with the indicated laws.

Proof of Theorem D.1. Take $y = (K_N + 1)e^{\sqrt{\log N}}$. Because $\ell \leq N^{2-\tau}$, $X \geq N^{\tau/2}$ and

$$\frac{1}{v} \leq \frac{2}{\tau} \left(\frac{\log(K_N + 1)}{\log N} + \frac{1}{\sqrt{\log N}} \right), \quad \frac{(1 + \log N)^{12}}{\sqrt{X}} \leq (1 + \log N)^{12} N^{-\tau/4}.$$

Every error in (D.6) tends to zero uniformly in the stated class. The singleton moment of the model is

$$-\frac{M_{\{d\}}(\eta, y)}{\ell}, \quad 0 \leq M_{\{d\}}(\eta, y) \leq 1.$$

Its negative probability is at least $1/2$, and its positive probability is at least $(1 - 1/\ell)/2 \geq 2/5$. Return to the original counts by adding the at most two labels at $n = 1$. If $\ell \rightarrow \infty$, (D.1) and contraction under convolution show that the model tends to the uniform law, proving the last assertion. $\square$

For example, at fixed conductor $\ell = 5$ with no corrections, every trace has limiting negative proportion $3/5$, not $1/2$. The limiting joint law need not be uniform at a fixed conductor. The first assertion of the theorem deliberately retains this possibility.

The estimates also give a polynomial exclusion radius. For each fixed $\tau > 0$, choose $\delta(\tau) > 0$ sufficiently small and replace K_N by $N^{\delta(\tau)}$ above. The right-hand side of (D.6) is then bounded by a small constant uniformly in $\ell \leq N^{2-\tau}$. Both signs occur at least $N/4$ times on every trace for large N . Therefore $E_N(h_N) = o(N)$ forces

$$\min_{\substack{5 \leq \ell \leq N^{2-\tau} \\ \ell \text{ prime}}} D_{\ell, N}(h_N) > N^{\delta(\tau)}$$

eventually. Inactive corrections can again be omitted from this count. This conclusion does not say that an arbitrary quasi-saturation must be close to one of the character models. The conductor restriction, the cardinality of corrections, and the preservation of the ramified sign are all essential parts of the statement.

Computational material and AI assistance

The companion source and verification archive, distributed alongside this PDF, contains the LaTeX sources, frozen bibliography, finite verification programs, data and execution logs. Its `README.md` gives build and reproduction commands; the source concordance records the editions and precise forms of the external inputs. The programs check arithmetic identities, parity presentations, finite repair certificates, noise probabilities and compact families. They do not establish asymptotic estimates or the imported theorems. The proofs above can be read independently of the computational archive.

GPT-6 Astra assisted mathematical exploration, calculations, drafting, bibliographical work, code, rechecking and editorial preparation. The author is responsible for the manuscript. No independent human specialist review, human replication or Lean formalisation of this article is claimed, nor does this declaration assert that a complete unaided human verification has taken place. Detailed provenance and the scope of each computational check are recorded in the archive.

References

- [1] M. Bardestani and T. Freiberg. Mertens’s theorem for splitting primes and more—a concise and adaptable proof of Hardy. arXiv:1309.7482v1, 2013. <https://arxiv.org/abs/1309.7482v1>. Theorem 3.3 and the following fixed-modulus error estimate.
- [2] D. J. Bernstein. Factoring into coprimes in essentially linear time. *Journal of Algorithms*, 54(1):1–30, 2005. <https://cr.yp.to/coprimes.html>. Context for coprime refinement; no complexity bound from this article is used.
- [3] Y. Bilu, G. Hanrot, and P. M. Voutier. Existence of primitive divisors of Lucas and Lehmer numbers. *Journal für die reine und angewandte Mathematik*, 539:75–122, 2001. doi:10.1515/cr11.2001.080. With an appendix by M. Mignotte. Definitions in Section 1, Theorem A (Carmichael–Ward), and Theorem 1.4.
- [4] P. Borwein, S. K. K. Choi, and H. Ganguli. Sign changes of the Liouville function on quadratics. *Canadian Mathematical Bulletin*, 56(2):251–257, 2013. doi:10.4153/CMB-2011-166-9. <https://arxiv.org/abs/1109.3107v1>. Theorem 2.2 of arXiv:1109.3107v1.
- [5] K. Conrad. Pell’s equation, I. Expository notes, n.d. <https://kconrad.math.uconn.edu/blurbs/ugradnumthy/pelleqn1.pdf>. Theorem 2.3 (Lagrange), and Sections 4–7. Accessed 27 September 2026.
- [6] R. de la Bretèche, V. Y. Wang, and M. W. Xu. Random multiplicative functions and making squares from polynomial values. arXiv:2607.06398v1, 2026. <https://arxiv.org/abs/2607.06398v1>. Introduction and Sections 5–7; contextual comparison, not a proof input.
- [7] G. Everest, S. Stevens, D. Tamsett, and T. Ward. Primes generated by recurrence sequences. *The American Mathematical Monthly*, 114(5):417–431, 2007. doi:10.1080/00029890.2007.11920430. <https://arxiv.org/abs/math/0412079v2>. Locators refer to arXiv:math/0412079v2: Lemma 4.1, Proposition 4.2 and Theorem 5.1.
- [8] O. Gorodetsky. A Kubilius model for sieve-theoretic sequences. *Analysis Mathematica*, 2026. doi:10.1007/s10476-026-00178-w. <https://arxiv.org/abs/2608.14190v1>. Published online 14 August 2026. The valuation-comparison locator is Theorem 2.3 of arXiv:2608.14190v1.
- [9] R. W. Hamming. Error detecting and error correcting codes. *Bell System Technical Journal*, 29(2):147–160, 1950. doi:10.1002/j.1538-7305.1950.tb00463.x.
- [10] W. Hoeffding. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association*, 58(301):13–30, 1963. doi:10.1080/01621459.1963.10500830.
- [11] L. Mérai, I. E. Shparlinski, and A. Winterhof. Character sums over sparse elements of finite fields. *Bulletin of the London Mathematical Society*, 56(4):1488–1510, 2024. doi:10.1112/blms.13008. <https://arxiv.org/abs/2211.08452v1>. The locator is Lemma 3.1 of arXiv:2211.08452v1, used only as a stated form of the classical mixed Weil bound.
- [12] M. Mine. An upper bound for the number of smooth values of a polynomial and its applications. arXiv:2410.09558v2, 2025. <https://arxiv.org/abs/2410.09558v2>. Revised 8 October 2025. Section 1.3, Theorem 1.4 and Corollary 1.5; contextual comparison.
- [13] NIST. Digital library of mathematical functions. Sections 27.9, 27.11 and 27.12, n.d. <https://dlmf.nist.gov/27>. Quadratic characters and fixed-modulus prime estimates, in particular Eq. 27.12.8. Accessed 28 September 2026.
- [14] A. Srinivasan. Infinitely many sign changes of the Liouville function on $x^2 + d$. *Proceedings of the American Mathematical Society*, 150(9):3799–3809, 2022. doi:10.1090/proc/15939. <https://arxiv.org/abs/2104.15004v2>. Theorem 1.3 of arXiv:2104.15004v2.
- [15] A. V. Sutherland. The analytic class number formula. MIT 18.785 Number Theory I, Lecture 19, 2017. <https://math.mit.edu/classes/18.785/2017fa/LectureNotes19.pdf>. Theorems 19.12 and 19.15, Fall 2017 lecture notes.
- [16] J. Teräväinen. On the Liouville function at polynomial arguments. *American Journal of Mathematics*, 146(4):1115–1167, 2024. doi:10.1353/ajm.2024.a932436. <https://arxiv.org/abs/2010.07924v4>. Locators refer to arXiv:2010.07924v4: Definition 2.8, Theorem 2.9, Proposition 2.10 and Section 6.