HOW SMALL CAN A COUNTEREXAMPLE TO THE NON-CANCELLING-INTERSECTIONS CONJECTURE BE?

KOREA SUPERINTELLIGENCE LABS

Abstract. Wilhelm has refuted the Non-Cancelling-Intersections conjecture of Amarilli, Monet and Suciu by showing that for every prime $p \geq 10^5$ some marking $\mathfrak{m}$ of the lines of $\mathbb{F}_p^2$ makes the lattice $P_{p,\mathfrak{m}}$, of $p^3 + 2p^2 + 2$ elements, admit no winning dot-algebra tree; the smallest lattice his argument produces has 1 000 110 003 900 047 elements, and he asks how small a counterexample can be. We answer with exact integer arithmetic on his own first moment. First, his chain of inequalities, evaluated instead of simplified, already closes at $p = 5273$, and 5273 is the least such prime; the threshold 10^5 comes from a single lossy step. The chain is moreover not monotone in p: it fails again at $p = 5309$, exactly where $\lceil\sqrt{2p}\,\rceil$ jumps. Second, the same first moment used to its full strength — the exact hypergeometric hit probability, a sharper Cauchy–Schwarz count of lines, and linear-programming duality over the trace profile — closes at $p = 59$, giving a lattice of 212 343 elements with no winning dot-algebra tree, smaller by a factor 4 709 879 788.36 . . . . Here 59 is least, and again the bound is not monotone: it fails at 61 and closes again at 67. From below, every lattice with at most 8 elements admits a winning dot-algebra tree, so the smallest counterexample has between 9 and 212 343 elements. All the statements above are machine-checked in Lean 4.

1. Introduction

The conjecture and its refutation. Let $U = A_1 \cup \cdots \cup A_n$ be a union of finitely many sets in a measure space. The *Non-Cancelling-Intersections* (NCI) conjecture of Amarilli, Monet and Suciu [1] says, in one formulation, that whenever the measure of U is determined by inclusion–exclusion from the measures of some family of intersections of the A_i, the set U can already be built from those same intersections using only two *cancellation-free* operations: disjoint union, and the complement of a subset.

The conjecture has a purely lattice-theoretic form. Let P be a finite lattice with top $\hat{1}$ and Möbius function μ. A *dot-algebra tree* (*da-tree*) for P is a finite binary tree in which

- each leaf is labelled either by $\emptyset$ or by a vertex $v \neq \hat{1}$ with $\mu(v) \neq 0$, and carries the state $S_v = \{u \in P : u \leq v\} \subseteq P \setminus \{\hat{1}\}$;
- each internal node is labelled $+$ or $-$; a $+$ node with children carrying A and B is legal only when $A \cap B = \emptyset$ and carries $A \cup B$; a $-$ node is legal only when $B \subseteq A$ and carries $A \setminus B$.

The tree is *winning* when the root carries $P \setminus \{\hat{1}\}$. The conjecture asserts that every finite lattice has a winning da-tree; nothing in the definition constrains the intermediate states, so a winning da-tree exists if and only if $P \setminus \{\hat{1}\}$ lies in the closure of $\{\emptyset\} \cup \{S_v : v \neq \hat{1},\ \mu(v) \neq 0\}$ under disjoint union and subset complement.

Wilhelm refuted the conjecture in [3], eight days after refuting its left-linear case [2]. His counterexamples are the lattices $P_{p,\mathfrak{m}}$ of [2, §5]: for a prime p one puts $w = \lceil\sqrt{2p}\,\rceil + 1$ and lets a *marking* $\mathfrak{m}$ assign to every one of the $p^2 + p$ lines ℓ of the affine plane $\mathbb{F}_p^2$ a set $\mathfrak{m}(\ell) \subseteq \ell$ of w *marked* points. The lattice $P_{p,\mathfrak{m}}$ has a top, p^2 elements of the first level indexed by the points of $\mathbb{F}_p^2$, $p - 1$ elements of the second level for each line, $p^2 + p$ elements of the third level indexed by the lines, and a bottom, hence

$$|P_{p,\mathfrak{m}}| = p^3 + 2p^2 + 2. \tag{1}$$

Wilhelm's Theorem 1.1 reads, verbatim: *"For every prime $p \geq 10^5$ there is a marking $\mathfrak{m}$ such that the lattice $P_{p,\mathfrak{m}}$ admits no winning dot-algebra tree. Consequently the NCI conjecture is false."* With the smallest prime it allows, $p = 100\,003$, his Remark 8.3 records a counterexample of $100\,003^3 + 2 \cdot 100\,003^2 + 2 < 1.1 \cdot 10^{15}$ elements; by (1) the number in question is

$$100\,003^3 + 2 \cdot 100\,003^2 + 2 \;=\; 1\,000\,110\,003\,900\,047.$$

The first of the open problems of [3, §9], which we call Open Problem 1 throughout, then asks, verbatim: *"Explicit counterexamples and lower bounds. Theorem* 8.1 *is still a first-moment argument and produces no explicit marking. What is the smallest lattice on which no winning da-tree exists? Exhaustive search on $P_{p,\mathfrak{m}}$ for small p is now conceivable."* (Theorem 8.1 is Theorem 1.1 as proved in [3, §8]; all numbered references to [2, 3] in this paper are to the version 1 e-prints.)

What is settled here. The threshold $p \geq 10^5$ enters [3] at exactly one place, the first-moment estimate of its Lemma 7.2, and the size $1.1 \cdot 10^{15}$ is its consequence through (1). Wilhelm himself flags the estimate as wasteful — his Remark 7.3 says that it "has enormous slack" and that "neither constant in Lemma 7.1 matters" — but does not say how much slack there is. This paper measures it, in exact integer arithmetic, from both directions.

Let E_p denote the expected number of sets $T \subseteq \mathbb{F}_p^2$ with $2p \leq |T| \leq 4p$ that survive a uniformly random marking (Section 2); $E_p < 1$ produces a counterexample lattice of size $p^3 + 2p^2 + 2$. The paper proves three things about E_p.

(A) *The chain of* [3]*, evaluated rather than simplified, closes at* $p = 5273$ (Theorem 3.1), and 5273 is the least prime at which it closes (Theorem 3.3). The gap between 5273 and 10^5 is one lossy step, $96 \leq p^{0.4}$. The chain is *not monotone* in p: $p = 5309$ is the unique prime in $(5273, 6100]$ at which it fails, and it is exactly where $\lceil \sqrt{2p}\, \rceil$ increases (Theorem 3.4). The simplified form $p^{5p-p^2/120}$ printed in [3] is monotone, so the simplification hides this.

(B) *The same first moment, used to its full strength, closes at* $p = 59$ (Theorem 4.1): a lattice with $212\,343$ elements and no winning da-tree, against $1\,000\,110\,003\,900\,047$, a factor $4\,709\,879\,788.36\ldots$. Here 59 is least (Theorem 4.3), and the bound is again non-monotone — it fails at 61 and closes again at 67 (Theorem 4.4). The ingredients are the exact hypergeometric hit probability in place of a union bound, a Cauchy–Schwarz count of lines that is twice as strong as the one in [3], and linear-programming duality over the trace profile.

(C) *Every lattice with at most* 8 *elements admits a winning da-tree* (Proposition 5.1), by exhaustion.

Together (B) and (C) bracket Wilhelm's Open Problem 1:

$$9 \;\leq\; \min\{|P| : P \text{ a finite lattice with no winning da-tree}\} \;\leq\; 212\,343.$$

The three thresholds and the lattice sizes they produce are:

bound on E_p	least prime	$\lvert P_{p,\mathfrak{m}}\rvert$	source
simplified chain	100 003	1 000 110 003 900 047	[3], Remark 8.3
same chain, evaluated exactly	5273	146 668 890 477	Theorems 3.1, 3.3
first moment at full strength	59	212 343	Theorems 4.1, 4.3

The first improvement divides the size of the lattice by more than 6818, the second by a further 690 716.

Everything below is finite exact arithmetic. We do not reformalise the probabilistic argument of [3], its lattice $P_{p,\mathfrak{m}}$, or its structural lemmas; we recompute, exactly, the quantities its first moment is built from, and Section 2 states precisely which results of [3] the counterexample statements rest on. A failure statement — "the bound does not close at p" — says that this estimate does not produce a marking at p, and never that $P_{p,\mathfrak{m}}$ has a winning da-tree.

2. Preliminaries

The plane, the marking, admissible sets. Throughout, p is a prime and $\mathbb{F}_p^2$ is the affine plane over $\mathbb{F}_p$, with its $p^2 + p$ lines; every point lies on exactly $p + 1$ lines and every pair of distinct points on exactly one line. Put

$$w \;=\; w(p) \;=\; \lceil \sqrt{2p}\, \rceil + 1.$$

A *marking* is a family $\mathfrak{m} = (\mathfrak{m}(\ell))_\ell$ with $\mathfrak{m}(\ell) \subseteq \ell$ and $|\mathfrak{m}(\ell)| = w$. For $T \subseteq \mathbb{F}_p^2$ write $j_\ell = |T \cap \ell|$ for the *trace* of T on ℓ, and call T *admissible* (for $\mathfrak{m}$) when every line ℓ with $j_\ell \geq 2$ satisfies $T \cap \mathfrak{m}(\ell) \neq \emptyset$.

We use the structural half of [3] as a black box.

Fact 2.1 ([3, Lemmas 4.2 and 6.1])**.** Let $p \geq 11$ and let $\mathfrak{m}$ be a marking. If $P_{p,\mathfrak{m}}$ admits a winning da-tree, then there is an admissible $T \subseteq \mathbb{F}_p^2$ with $2p \leq |T| \leq 4p - 2$.

This is the composite that [3] runs in the proof of its Theorem 8.1: Lemma 6.1 turns a winning da-tree for $P_{p,\mathfrak{m}}$ into a winning plane tree, and Lemma 4.2 extracts from that tree a node whose state is admissible and has $2p \leq |T| \leq 4p-2$. (Lemma 6.1 rests in turn on the blocking-gadget Lemma 5.1 of [3]. The hypothesis $p \geq 11$ is the one under which [3, Remark 3.4] states the lattice formulation, and is inherited here.)

Remark 2.2 (the window). Lemma 4.2 of [3] produces a node with $2p \leq |T| \leq 4p-2$, whereas the first moment we recompute — its Lemmas 7.1 and 7.2 — is stated over the wider window $2p \leq |T| \leq 4p$. Every computation in this paper uses the wider window, exactly as [3] does, and this is safe in the direction we need: a marking with *no* admissible set of size in $[2p, 4p]$ has none of size in $[2p, 4p-2]$ either, since $[2p, 4p-2] \subseteq [2p, 4p]$. The wider window makes the estimate harder to satisfy, never easier.

Consequently, a marking with no admissible T of size in $[2p, 4p]$ refutes the conjecture on $P_{p,\mathfrak{m}}$, and by (1) produces a counterexample lattice with $p^3 + 2p^2 + 2$ elements.

The first moment. Draw the sets $\mathfrak{m}(\ell)$ independently, each uniform among the $\binom{p}{w}$ w-subsets of its line. For a fixed T with trace j on a fixed line, the probability that the line is *hit*, i.e. that $T \cap \mathfrak{m}(\ell) \neq \emptyset$, is exactly the hypergeometric quantity

$$q_j \;=\; 1 - \binom{p-j}{w} \Big/ \binom{p}{w}, \tag{2}$$

and distinct lines are independent, so with $m_j = \#\{\ell : j_\ell = j\}$ for $j \geq 2$,

$$\Pr[\,T \text{ admissible}\,] \;=\; \prod_{j \geq 2} q_j^{m_j}. \tag{3}$$

Define

$$E_p \;=\; \sum_{t=2p}^{4p} \sum_{|T|=t} \Pr[\,T \text{ admissible}\,],$$

the expected number of admissible sets in the relevant window. If $E_p < 1$ then some marking admits none, so by Fact 2.1 the lattice $P_{p,\mathfrak{m}}$ has no winning da-tree. This is the only place the threshold 10^5 enters [3] — the other lower bounds on p there are the $p \geq 5$ of its Lemma 7.1 and the $p \geq 11$ of its Remark 3.4 — and it is the object of everything below.

Two identities and their consequences. Fix T with $|T| = t$. Counting incidences and pairs,

$$\sum_\ell j_\ell = t(p+1), \qquad \sum_\ell \binom{j_\ell}{2} = \binom{t}{2}, \tag{4}$$

the sums running over all $p^2 + p$ lines. Write

$$N = \#\{\ell : j_\ell \geq 2\}, \qquad \Sigma_1 = \sum_{j_\ell \geq 2} j_\ell, \qquad u = u(t) = (p+1)(t-p).$$

Since at most $p^2 + p$ lines meet T at all, the first identity gives $\Sigma_1 \geq t(p+1) - (p^2 + p - N)$, that is

$$\sum_{j \geq 2} (j-1) m_j \;=\; \Sigma_1 - N \;\geq\; u. \tag{5}$$

The second identity gives $\sum_{j_\ell \geq 2} j_\ell^2 = t(t-1) + \Sigma_1$, so Cauchy–Schwarz reads $\Sigma_1^2 \leq N\big(t(t-1) + \Sigma_1\big)$; substituting $\Sigma_1 \geq u + N$ into the increasing function $x \mapsto x^2/(t(t-1)+x)$ and clearing denominators leaves $u^2 \leq N\big(t(t-1) - u\big)$, i.e.

$$N \;\geq\; N^-(t) \;:=\; \left\lceil \frac{u^2}{t(t-1)-u} \right\rceil. \tag{6}$$

At $t = 2p$ one has $u = p^2 + p$ and $N^-(2p) = \lceil p(p+1)^2/\big(3(p-1)\big)\rceil \sim (p+1)^2/3$, whereas the corresponding step of [3] — the display (7.4) inside its Lemma 7.1 — uses $u^2/\big(t(t+p)\big) \sim (p+1)^2/6$: a factor 2. At $p = 59$, $t = 118$ the two read 1221 and 600.

Finally, the second identity of (4) bounds long traces on its own: every line with $j_\ell \geq k+1$ contributes at least $\binom{k+1}{2}$ to $\binom{t}{2}$, so $\#\{\ell : j_\ell \geq k+1\} \leq \binom{t}{2}/\binom{k+1}{2}$. In the linear program of Section 4 this is subsumed by the identity itself and is not imposed separately.

Remark 2.3. All computations below evaluate $w(p)$ through a routine that is certified to return $\lceil\sqrt{2p}\,\rceil + 1$: for every $1 \leq p \leq 6200$ the returned value w satisfies $(w-2)^2 < 2p \leq (w-1)^2$, which pins w uniquely. No statement in the paper depends on how a square root is implemented.

Lemma 2.4. *The two identities* (4) *and the bound* (6) *hold on* every *one of the* 512 *subsets of* $\mathbb{F}_3^2$*, and on samples of* 4000 *and* 1500 *pseudo-random subsets of* $\mathbb{F}_5^2$ *and of* $\mathbb{F}_7^2$*; in the last sample all* 1500 *sets satisfy* $|T| > p$*, so* (6) *is not vacuous there. The lines are constructed explicitly, and at* $p = 7$ *the* 56 *line sets are pairwise distinct with* 7 *points each. Moreover the hit probability* (2) *agrees with a brute-force count of the* w*-subsets meeting a fixed* j*-set for every* $p \leq 12$ *and all* $1 \leq w, j \leq p$.

Proof sketch. Exhaustive computation. Points of $\mathbb{F}_p^2$ are encoded as bits of an integer mask, the p^2+p lines are built as masks, and the traces are read off by population count; each of the listed checks is a finite conjunction, evaluated in the kernel. ☐

3. The chain of [3], evaluated exactly

The chain, and its one lossy step. The estimate of [3] — its Lemma 7.2 — bounds (3) by charging each of the short traces a union bound: a trace of size $j \leq 47$ is hit with probability at most $jw/p \leq 47w/p$, and its Cauchy–Schwarz Lemma 7.1 supplies at least $\lceil (p+1)^2/12 \rceil$ lines with $2 \leq j_\ell \leq 47$. With the union bound over the $\sum_{t=2p}^{4p} \binom{p^2}{t}$ candidate sets this gives

$$E_p \;\leq\; W_K(p) \;:=\; \left(\sum_{t=2p}^{4p} \binom{p^2}{t}\right) \cdot \left(\frac{K\,w}{p}\right)^{\lceil (p+1)^2/12 \rceil}, \qquad K = 47. \tag{7}$$

The displayed inequality (7.5) of [3] rounds the base up to $48w/p$, so W_{47} is the tighter of its own two forms and W_{48} is the literal one; both are treated below.

Wilhelm never evaluates (7). He simplifies: his display (7.6) reads $48w/p \leq 96/p^{0.5} \leq p^{-0.1}$, "where the second inequality is $96 \leq p^{0.4}$, which holds because $p^{0.4} \geq (10^5)^{0.4} = 10^2 = 100$" — and that is where $p \geq 10^5$ is used; then $E_p \leq p^{4p+2} p^{-p^2/120} \leq p^{5p-p^2/120}$, whose exponent "is negative as soon as $p > 600$". So 10^5 is the cost of the single step $96 \leq p^{0.4}$ and of nothing else.

Where the chain really closes. Cleared of denominators, $W_K(p) < 1$ reads

$$\left(\sum_{t=2p}^{4p} \binom{p^2}{t}\right) \cdot (Kw)^E \;<\; p^E, \qquad E = \left\lceil \tfrac{(p+1)^2}{12} \right\rceil, \tag{8}$$

an inequality between two integers.

Theorem 3.1. $W_{47}(5273) < 1$*. Explicitly, at* $p = 5273$ *one has* $w = 104$ *and* $E = \lceil 5274^2/12 \rceil =$ 2 317 923*, and the two sides of* (8) *are integers of* 8 626 084 *and* 8 627 444 *decimal digits, the left one smaller.*

Corollary 3.2. *Granting Fact* 2.1 *and the estimate* (7) *of* [3]*, there is a marking* $\mathfrak{m}$ *of the lines of* $\mathbb{F}_{5273}^2$ *with* $|\mathfrak{m}(\ell)| = 104$ *for which* $P_{5273,\mathfrak{m}}$ *— a lattice with* $5273^3 + 2 \cdot 5273^2 + 2 = 146\,668\,890\,477$ *elements — admits no winning da-tree. This is more than* 6818 *times smaller than the lattice of* [3]*, and uses no inequality that is not already in* [3].

Theorem 3.3. 5273 *is the least prime at which the chain closes:* $W_{47}(p) \geq 1$ *for every prime* $p < 5273$.

Proof sketch. Two halves, both finite. For every $1 \leq p \leq 4559$ one has $p \leq 47\,w(p)$, so the base $47w/p$ of (7) is at least 1 and (8) fails whatever the exponent; this is a check over 4559 values of p. For $4560 \leq p \leq 5271$ the inequality (8) is evaluated exactly at each of the 81 primes in the range, and fails at every one. Since 5272 is not prime, the two halves together leave 5273. □

Non-monotonicity. The simplified form $p^{5p-p^2/120}$ of [3] is monotone in p, and this is an artefact of the simplification: the exact chain is not. The marking size $w = \lceil \sqrt{2p}\,\rceil + 1$ is a step function of p, and each of its jumps multiplies the base of (7) by $(w+1)/w$ — a cost of $E \log \frac{w+1}{w}$ in the exponent, which the slow growth of E and of $\log p$ over a short interval need not repay.

Theorem 3.4. $W_{47}(5309) \geq 1$*, and* 5309 *is the* only *prime* p *with* $5273 < p \leq 6100$ *at which the chain fails. The primes bracketing the failure,* 5303 *and* 5323*, both close.*

Proof sketch. Exhaustive evaluation of (8) at every prime in $[5274, 6100]$. The failure at 5309 is exactly where $\lceil \sqrt{2p}\,\rceil$ crosses from 102 to 103 and w from 104 to 105: over the interval the logarithm of W_{47} moves from $-17\,335$ at 5303 to $+2282$ at 5309, the jump in w costing $E \log(105/104) \approx 2.25 \cdot 10^4$ while the six extra units of p buy only about $2.9 \cdot 10^3$. □

The margin at the threshold is correspondingly thin: at $p = 5273$ the two sides of (8) differ by 1360 decimal digits out of more than 8.6 million.

Proposition 3.5. *With the constant* 48 *that* [3] *actually prints, the least prime at which the chain closes is* 5471*:* $p \leq 48\,w(p)$ *for all* $p \leq 4752$*, and* $W_{48}(p) \geq 1$ *at every prime in* $[4753, 5469]$*, while* $W_{48}(5471) < 1$*. There is no later failure below* 6200.

This is the same computation as Theorems 3.1–3.4 with one constant changed, recorded because 5471 is what a literal reading of [3] gives while 5273 is what its own union bound gives.

4. The first moment at full strength

Section 3 changed nothing in the argument of [3]. This section keeps its setting verbatim — the plane, the marking size w, the window $2p \leq t \leq 4p$, the independence — and replaces only the estimate of (3).

A linear program per cardinality. Fix p and t with $2p \leq t \leq 4p$. By (3), the survival probability of a set T of size t is determined by its trace profile $m = (m_j)_{2 \leq j \leq p}$, which satisfies

$$\textstyle\sum_j m_j \;\geq\; N^-(t) \tag{C1}$$

$$\textstyle\sum_j (j-1) m_j \;\geq\; u(t) \tag{C2}$$

$$\textstyle\sum_j \binom{j}{2} m_j \;=\; \binom{t}{2} \tag{C3}$$

by (6), (5) and the second identity of (4). Relaxing m to a nonnegative real vector and maximising, put

$$L_p(t) \;=\; \max\Big\{ \prod_{j=2}^{p} q_j^{m_j} \;:\; m \in \mathbb{R}_{\geq 0}^{p-1} \text{ satisfies (C1)–(C3)} \Big\}, \qquad \mathrm{FM}(p) \;=\; \sum_{t=2p}^{4p} \binom{p^2}{t} L_p(t).$$

Taking logarithms turns the maximisation into a linear program with three constraints, and $E_p \leq \mathrm{FM}(p)$ because every actual T of size t has a feasible profile. Both sides of $\mathrm{FM}(p) < 1$ admit exact rational certificates.

Closure (dual). Let $A, B, C > 0$ with $A \le 1$, $B \le 1$ and

$$q_j \;\le\; A\,B^{\,j-1}C^{\binom{j}{2}} \qquad (2 \le j \le p). \tag{9}$$

Then for any feasible m, $\prod_j q_j^{m_j} \le A^{\sum m_j} B^{\sum (j-1)m_j} C^{\binom{t}{2}} \le A^{N^-(t)} B^{u(t)} C^{\binom{t}{2}}$, the second step using $A, B \le 1$ with (C1) and (C2). Hence if for every $t \in [2p, 4p]$ there are such A_t, B_t, C_t with

$$(2p+1)\binom{p^2}{t} A_t^{N^-(t)} B_t^{u(t)} C_t^{\binom{t}{2}} \;<\; 1, \tag{10}$$

then $\mathrm{FM}(p) < 1$, the $2p+1$ summands each being below $1/(2p+1)$.

Failure (primal). Conversely, a single t and a single integer profile m satisfying (C1)–(C3) with $\binom{p^2}{t}\prod_j q_j^{m_j} \ge 1$ shows $\mathrm{FM}(p) \ge 1$.

Both certificates are checked in exact integer arithmetic: the q_j are kept as the numerators $\binom{p}{w} - \binom{p-j}{w}$ over the common denominator $\binom{p}{w}$, and A, B, C as dyadic rationals $a/2^{24}$, $b/2^{24}$, $c/2^{24}$, so that (9) and (10) become comparisons of integers.

What the certificates say.

Theorem 4.1. $\mathrm{FM}(59) < 1$. *A dual certificate consists of* 119 *triples* (A_t, B_t, C_t) *of dyadic rationals with denominator* 2^{24}*, one for each cardinality* $t = 118, \ldots, 236$*, each satisfying* $A_t, B_t \le 1$*, the feasibility conditions* (9) *for all* $2 \le j \le 59$*, and the objective* (10)*.*

Corollary 4.2. *Granting Fact* 2.1*, there is a marking* $\mathfrak{m}$ *of the* 3540 *lines of* $\mathbb{F}_{59}^2$ *with* $|\mathfrak{m}(\ell)| = 12$ *for which no* T *with* $118 \le |T| \le 236$ *is admissible, so the lattice* $P_{59,\mathfrak{m}}$ *— with*

$$59^3 + 2\cdot 59^2 + 2 \;=\; 212\,343$$

elements — admits no winning da-tree. The lattice of [3] *is larger by the factor*

$$\frac{1\,000\,110\,003\,900\,047}{212\,343} \;=\; 4\,709\,879\,788.36\ldots \;>\; 4.7\cdot 10^9.$$

Theorem 4.3. 59 *is the least prime at which this bound closes: for every prime* $5 \le p \le 53$ *there is an explicit cardinality* t *and an explicit integer trace profile, feasible for* (C1)–(C3)*, whose single term* $\binom{p^2}{t}\prod_j q_j^{m_j}$ *is already at least* 1*; hence* $\mathrm{FM}(p) \ge 1$ *there. The primes* 2 *and* 3 *are excluded because* $w(p) > p$ *for them, so no marking exists.*

The profiles are short. At $p = 53$ the certificate is $t = 201$ with $m_5 = 2010$ and no other m_j; at $p = 13$ it is $t = 52$ with $m_4 = 221$; at $p = 5$ it is $t = 10$ with $m_2 = 45$. The relaxation does not ask a profile to be realised by an actual point set — the one at $p = 5$ has more lines than the plane has — so a failure witness certifies exactly what Theorem 4.3 claims, that *this bound* does not close at p, and nothing about E_p itself.

Theorem 4.4. *The bound is not monotone in* p *either. It fails at* $p = 61$*: at* $t = 244$ *the profile* $m_2 = 6$*,* $m_5 = 2196$*,* $m_6 = 512$ *is feasible for* (C1)–(C3) *and its term is at least* 1*, so* $\mathrm{FM}(61) \ge 1$*. It closes again at* $p = 67$*, by a dual certificate of* 135 *triples covering* $t = 134, \ldots, 268$*; the corresponding lattice has* 309 743 *elements.*

The mechanism is the one of Theorem 3.4, one level down: w jumps from 12 to 13 between $p = 59$ and $p = 61$, and the loss is not repaid until $p = 67$, where w is still 13.

Proof sketch for Theorems 4.1–4.4. All three are finite exact computations over the explicit certificates. For Theorem 4.1: for each of the 119 rows, verify $A_t, B_t \le 1$, then (9) at each of the 58 trace sizes $2 \le j \le 59$, then (10); the row list is also checked to be exactly $t = 118, \ldots, 236$, so that no cardinality is skipped. For Theorem 4.3: for each of the 14 primes $5 \le p \le 53$, verify that the listed profile has $2 \le j \le p$ throughout, meets (C1)–(C3), and has term at least 1; the list of primes covered is itself checked against the primes in $[5, 61]$ other than 59. Theorem 4.4 is one primal check and one dual certificate of 135 rows. The margins are thin: at $p = 59$ the worst cardinality is the largest, $t = 236$, where (10) holds with about 19.5 nats to spare. ∎

Remark 4.5 (the certificate checkers are not vacuous). Four controls were run on the machinery of this section. Lowering C by 1000, or A by 10^5, in the first row of the $p = 59$ certificate breaks dual feasibility, so the rationals carry no slack to spare; deleting one row makes the closure test fail, so the rows must cover every cardinality; a profile violating the identity (C3) by one is rejected. The control that matters concerns the failure test: at $p = 59$, $t = 236$ the profile $m_5 = 2065$, $m_6 = 472$ *is* feasible for (C1)–(C3) — it meets (C2) with equality, $\sum(j-1)m_j = 10\,620 = u(236)$, and has $\sum\binom{j}{2}m_j = 27\,730 = \binom{236}{2}$ and $\sum m_j = 2537 \geq N^-(236) = 2516$, and is in fact the maximiser of the linear program there — and the failure test still rejects it, because its term is below 1. The test is therefore decided by the value, not by feasibility.

Where the strength comes from. Three replacements separate FM from (7), and each is elementary.

The hit probability. The union bound jw/p used in the proof of [3, Lemma 7.2] is not merely lossy but vacuous where it is applied: at $p = 571$, $w = 35$ and $j = 19$ it reads $19 \cdot 35/571 = 1.16 > 1$, while the exact q_{19} is 0.705. Keeping (2) is what allows long traces to be charged at all.

The count of lines. Inequality (6) is twice the strength of the Cauchy–Schwarz step (7.4) of [3, Lemma 7.1] at $t = 2p$, as computed in Section 2.

The combination. Instead of charging a single cutoff k — all traces of size at most k charged q_k, everything else charged 1 — the linear program uses the two identities (4) directly, and this is the largest of the three gains. Two intermediate bounds locate it. For a fixed cutoff k, the identity (C3) caps the number of lines with $j_\ell \geq k+1$ at $\binom{t}{2}/\binom{k+1}{2}$, so at least $N^-(t) - \lfloor\binom{t}{2}/\binom{k+1}{2}\rfloor$ lines have $2 \leq j_\ell \leq k$ and are each hit with probability at most q_k, giving

$$E_p \;\leq\; \min_k \sum_{t=2p}^{4p} \binom{p^2}{t}\, q_k^{\,N^-(t)-\lfloor\binom{t}{2}/\binom{k+1}{2}\rfloor}.$$

The right-hand side first falls below 1 at $p = 109$, where the best cutoff is $k = 7$; it exceeds 1 at every prime $5 \leq p \leq 107$. Charging instead each line q_j for its own j, and spreading the $N^-(t)$ lines over the trace sizes as favourably as the tail bounds $\#\{\ell : j_\ell \geq k\} \leq \binom{t}{2}/\binom{k}{2}$ permit — a "staircase" — first falls below 1 at $p = 83$, and exceeds 1 at every prime $5 \leq p \leq 79$. The linear program reaches 59.

These two waypoints are *measurements*: they were computed in floating point, outside the verified development. Their margins are wide — in nats, $+19.0$ at $p = 107$ against -60.9 at $p = 109$, and $+27.8$ at $p = 79$ against -132.8 at $p = 83$ — but no statement of this paper rests on them.

5. The bottom of the range

Open Problem 1 of [3] asks for the smallest lattice with no winning da-tree. Section 4 gives an upper bound of 212 343; the complementary bound is a small exhaustive search.

Proposition 5.1. *Every lattice with at most* 8 *elements admits a winning da-tree. Hence the smallest lattice on which no winning da-tree exists has at least* 9 *elements.*

Proof sketch. Since the definition of a da-tree constrains no intermediate state, P has a winning da-tree if and only if $P \setminus \{\hat{1}\}$ lies in the closure of $\{\emptyset\} \cup \{S_v : v \neq \hat{1},\ \mu(v) \neq 0\}$ under $A \uplus B$ (defined when $A \cap B = \emptyset$) and $A \setminus B$ (defined when $B \subseteq A$). For $|P| = n$ this is a reachability computation inside the 2^{n-1} subsets of $P \setminus \{\hat{1}\}$, which is run to a fixed point.

Every finite poset has a linear extension, so every isomorphism class of n-element lattices occurs among the orders on $\{0, \dots, n-1\}$ for which $x < y$ implies $x < y$ as integers. Those are enumerated element by element: the strict down-set of a new element must be an order ideal of what is already placed, and, because any lower bound of i and j is numerically at most $\min(i, j)$, the meet of any two placed elements must already be present — which prunes the enumeration to meet-semilattices. A finite meet-semilattice with a top is a lattice, and the top is the last element. Every isomorphism class therefore occurs at least once, which is all the exhaustiveness claim requires. The counts obtained are $1, 1, 1, 2, 7, 39, 320, 3637$ for $n = 1, \dots, 8$, against the $1, 1, 1, 2, 5, 15, 53, 222$ isomorphism classes of lattices on n unlabelled nodes, which are the terms $a(1)$ through $a(8)$ of [7, A006966] (that entry has offset 0). The Möbius function is computed from the down-sets by $\mu(\hat{1}) = 1$, $\mu(v) = -\sum_{u>v} \mu(u)$. All 3637 lattices with $n = 8$, and all smaller ones, are found to be winning.

Controls: the seven five-element orders produced are listed explicitly, and for the five-element chain the Möbius vector is $(0, 0, 0, -1, 1)$, so exactly two leaves are available — $\emptyset$ and the down-set of the coatom, which is already the whole of $P \setminus \{\hat{1}\}$, so the chain is won by a single leaf. □

Remark 5.2. The exhaustive search reported in [1, §7] is not comparable. It reads, verbatim: "We have checked in a brute-force fashion that the conjecture holds up to $n = 5$, i.e., on all intersection lattices such that $\hat{1}$ has cardinality at most 5. Unfortunately, already for $n = 6$ there are intersection lattices that are too large for the computation to finish sufficiently quickly." Three things differ. Their parameter n is the cardinality of $\hat{1}$ *as a set* — the ground set of the family, enumerated there through Sperner families on n elements — and not the number of lattice elements that Open Problem 1 asks about; their class is smaller (intersection lattices, rather than all lattices); and their conclusion is stronger (winning *left-linear* trees with the intersections used at fixed polarity, the variant since refuted in [2]).

Neither range contains the other. A seven-element chain is a lattice with at most 8 elements, but seven distinct nested subsets need $|\hat{1}| \geq 6$, so it lies outside $|\hat{1}| \leq 5$. Conversely the intersection lattice of the five 4-element subsets of a 5-element set is the Boolean lattice on 5 atoms: $|\hat{1}| = 5$, and 32 elements, so it lies outside ours.

Remark 5.3. One further item on the conjecture appeared while this work was being done. [4, Theorem 3] proves a sufficient condition: if the inclusion-maximal non-cancelling intersections admit a join tree with the running-intersection property whose nonempty edge separators are themselves non-cancelling, then the union has an explicit left-linear construction over the non-cancelling intersections. It is a positive result about a structural subclass, it cites [2] and not [3], and it states no threshold and no lattice size, so it bears on neither end of the bracket above.

Remark 5.4. Outside the formally verified development, the same enumeration and closure, run as a C program, reaches $n = 9$ (54 635 orders) and $n = 10$ (1 046 327 orders) in about two minutes, and finds every one of them winning. We record this as evidence and do not claim it as a theorem.

6. The published numbers, recomputed

Before any of the above was claimed, every number that [3] prints for its own argument was recomputed from its own definitions. This is background, not a new result.

Proposition 6.1. *The following hold.*

(1) $96 \leq (10^5)^{0.4}$, *i.e.* $96^5 \leq (10^5)^2$, *the one lossy step of the chain; and the step already holds from* $p = 90\,298$ *on, since* $96^5 \leq 90\,298^2$ *while* $96^5 > 90\,297^2$.

(2) $w(p) \leq 2\sqrt{p}$, *i.e.* $w(p)^2 \leq 4p$, *for every* $12 \leq p \leq 6200$.

(3) $5p < p^2/120$ *if and only if* $p > 600$, *checked for every* $p \leq 2000$*: the exponent of the simplified form is negative exactly beyond* 600.

(4) $100\,003^3 + 2 \cdot 100\,003^2 + 2 = 1\,000\,110\,003\,900\,047 < 1.1 \cdot 10^{15}$.

Item (1) is a small correction of emphasis: even the literal chain of [3] *does not need* 10^5.

Remark 6.2 (side conditions and non-degeneracy). The construction of $P_{p,\mathfrak{m}}$ imposes arithmetic conditions on (p, w), and they hold at the two primes this paper certifies at. At $p = 59$, $w = 12$ and at $p = 5273$, $w = 104$: there are $\binom{w}{2} \geq p - 1$ pairs of marked points to index the second level, at least two unmarked points per line ($w \leq p - 2$) for the third-level meets, $w \leq 2(p - 1)$, and $p \geq 11$ as [3, Remark 3.4] requires for the lattice formulation. The marking size is pinned at each of $59, 61, 5273, 5309$, both neighbours of the true w being rejected by the square inequalities of Remark 2.3. On the probability side, $0 < q_j < 1$ for every $2 \leq j \leq 47 = p - w$ at $p = 59$, $w = 12$, with $q_j = 1$ exactly from $j = 48$ on; if the q_j were degenerate the bound could never close. Finally the construction has no room at all for the smallest primes: $w(5) = 5 = p$ marks every point of every line, and $w(7) = 5$ leaves exactly the two unmarked points per line that the third level needs, which is why [3, Remark 3.4] states the lattice formulation from $p = 11$.

7. Verification

Every numbered statement of this paper carrying a computational claim has been checked in Lean 4 against *Mathlib* [5, 6]: Remark 2.3, Lemma 2.4, Theorems 3.1, 3.3, 3.4, 4.1, 4.3, 4.4, Propositions 3.5, 5.1, 6.1, and Remarks 4.5 and 6.2. The development is free of `sorry`; the large finite evaluations are discharged by the compiled evaluator (`native_decide`), so each such theorem carries its own compilation axiom, and a few additionally use propositional extensionality; no theorem uses the axiom of choice. All arithmetic is over the natural numbers with exact big integers: binomial coefficients are computed by the multiplicative formula with exact divisions and cross-checked against an independent Pascal recursion, and every rational appearing in a certificate is a dyadic rational compared after clearing denominators. What is *not* formalised is the probabilistic argument itself, the lattice $P_{p,\mathfrak{m}}$, and the structural lemmas recorded as Fact 2.1; the verified content is the finite exact arithmetic that those lemmas reduce the question to, together with the model checks of Lemma 2.4 that tie that arithmetic to real point sets in $\mathbb{F}_3^2$, $\mathbb{F}_5^2$ and $\mathbb{F}_7^2$. Also outside the verified development, and labelled as measurements where they appear, are the two waypoints of Section 4 ($p = 109$ for a single cutoff, $p = 83$ for the staircase) and the first-moment ceiling of Section 8; no numbered statement rests on them. Repository reference to be added at submission.

8. Open questions

The remaining bracket. Open Problem 1 of [3] is now bracketed between 9 and 212 343, and both ends look movable, for different reasons.

Below $p = 59$ needs a different method, not a better constant. The linear program of Section 4 extracts everything the two identities (4) and the exact q_j give through the three constraints (C1)–(C3): its dual certificate at $p = 59$ and its primal witness at $p = 53$ pin the threshold of that bound exactly, so no better choice of certificate can move it. The largest remaining slack is the union bound over the $\sum_t \binom{p^2}{t}$ candidate sets, which treats every set of the right size as a possible admissible set, though admissible sets are highly structured. A bound on the number of *admissible* candidates, rather than all candidates, is the next lever.

There is also a ceiling for first-moment arguments of this shape. Charging every line the smallest possible factor — $N \le p^2 + p$ lines, each hit with probability at least q_2 — and keeping only the single cardinality $t = 2p$ gives, for every p at which a marking exists,

$$E_p \;\ge\; \binom{p^2}{2p}\, q_2^{\,p^2+p},$$

a genuine lower bound on E_p and not on any particular relaxation of it. This lower bound exceeds 1 at every prime $5 \le p \le 13$ (at $p = 13$ its logarithm is $+31.2$), and first drops below 1 at $p = 17$ (logarithm -20.9). So $E_p \ge 1$ at every prime below 17, and no first-moment argument over this window can produce a marking below $p = 17$: at most a further factor of about 3.5 in p, i.e. about 40 in the size of the lattice, is available to this whole class of arguments, and the counterexample lattices they can produce will not go below roughly $5 \cdot 10^3$ elements. The numerical evaluation here is a *measurement*, computed in floating point outside the verified development; its margins ($+31.2$ against -20.9 nats) are far wider than any rounding involved, but no statement of this paper rests on it.

The lower bound is weak and cheap to push. Proposition 5.1 stops at $n = 8$ only because of the cost of the closure inside the verified development; $n = 10$ is already done outside it (Remark 5.4). The bottleneck is the $O(4^{\,n-1})$ closure rather than the enumeration of lattices, and the natural fix is to have the search return an explicit winning da-tree for each lattice and let the verifier only *check* it, which is linear in the size of the tree. That should reach $n = 11$ or 12. Nothing suggests that a counterexample lives anywhere near there, but the gap of nine orders of magnitude is the honest state of the problem.

Exhaustive search on $P_{p,\mathfrak{m}}$ itself. This is what Open Problem 1 suggests, and it looks out of reach as stated. The construction first has room at $p = 7$, where $|P_{7,\mathfrak{m}}| = 443$; a da-tree search there is a closure over subsets of a 442-element ground set, and neither the size of the closure nor its diameter has any known bound — in the small cases of Section 5 the closure routinely reaches *all* 2^{n-1} subsets. A smaller counterexample, if one exists, is more likely to come from a different construction than from searching this one.

Reusable machinery. The pair of certificate checkers of Section 4 — dual feasibility plus objective for closure, one feasible integer profile for failure — is not specific to $\mathbb{F}_p^2$. It applies verbatim to any first-moment bound whose inner maximisation is a linear program in a profile vector constrained by counting identities.

Acknowledgement of sources

The setting, the construction $P_{p,\mathfrak{m}}$, the structural lemmas recorded as Fact 2.1 and the first-moment estimate (7) are all due to Wilhelm [2, 3]; the conjecture and the prior exhaustive search of Remark 5.2 are due to Amarilli, Monet and Suciu [1]. What is new here is the exact evaluation of (7), the strengthened first moment and its certificates, and the small-lattice bound.

References

[1] A. Amarilli, M. Monet and D. Suciu, *The Non-Cancelling Intersections Conjecture*, arXiv:2401.16210v1 (2024).
[2] H. Wilhelm, *The Non-Cancelling-Intersections Conjecture Fails for Left-Linear Trees*, arXiv:2608.19414v1 (2026).
[3] H. Wilhelm, *Refutation of the Non-Cancelling-Intersections Conjecture*, arXiv:2608.27416v1 (2026).
[4] M. S. Yang, *A join-tree sufficient condition for the Non-Cancelling Intersections conjecture*, International Journal of Computer Techniques **13** (2026), no. 4, 266–275; `doi:10.5281/zenodo.22082890`.
[5] L. de Moura and S. Ullrich, *The Lean 4 Theorem Prover and Programming Language*, in: Automated Deduction — CADE 28, Lecture Notes in Computer Science 12699, Springer, 2021, pp. 625–635.
[6] The mathlib Community, *The Lean Mathematical Library*, in: Certified Programs and Proofs (CPP 2020), ACM, 2020, pp. 367–381.
[7] OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, `https://oeis.org`; entry A006966, “Number of lattices on n unlabeled nodes”.