A quadratic form interpolating `dinv`, with Lean auto-formalization

Yifeng Huang

USC

May. 4th, 2026 at CSUN

Outline

- An algebraic question encountered in my research
- A combinatorial, "human-style" solution
- An auto-formalization

It is not ...

- a toy problem just to test the "AI for Math" engine.

It is ...

- a real research problem benefited from human-AI interaction.

Algebra: Numerical semigroup

In 19th century, Frobenius and Sylvester studied the problem:

Given infinite supplies of coins of values $a_1, \dots, a_e \in \mathbb{Z}_{\geq 1}$, what values can you *not* make?

In algebraic language,

Consider the sub-semigroup $\Gamma \subseteq \mathbb{N}$ generated by $a_1, \dots, a_e$. What is its set of **gaps**, $G := \mathbb{N} \setminus \Gamma$?

Example

The gap set of $\langle 3, 4 \rangle$ is $\{1, 2, 5\}$. $(6 = 3 + 3, 7 = 3 + 4, 8 = 4 + 4, \dots)$

Sylvester's theorem

If there are only two generators, the gap set is well-understood.

Theorem (Sylvester, 1883)

If $\gcd(a, b) = 1$, *then* $\max G = (a-1)(b-1) - 1 = ab - a - b$, *and* $|G| = \dfrac{(a-1)(b-1)}{2}$. *In fact, the latter is a manifestation of a stronger symmetry: for* $0 \leq x \leq \max G$,

$$x \in G \iff \max G - x \notin G.$$

Example

If $(a, b) = (3, 4)$, then $(a-1)(b-1) = 6$. The gap set $\{1, 2, 5\}$ takes up exactly half of $\{0, 1, \ldots, 5\}$ and takes one of each of the mirror pairs $\{0, 5\}, \{1, 4\}, \{2, 3\}$.

My favorite proof

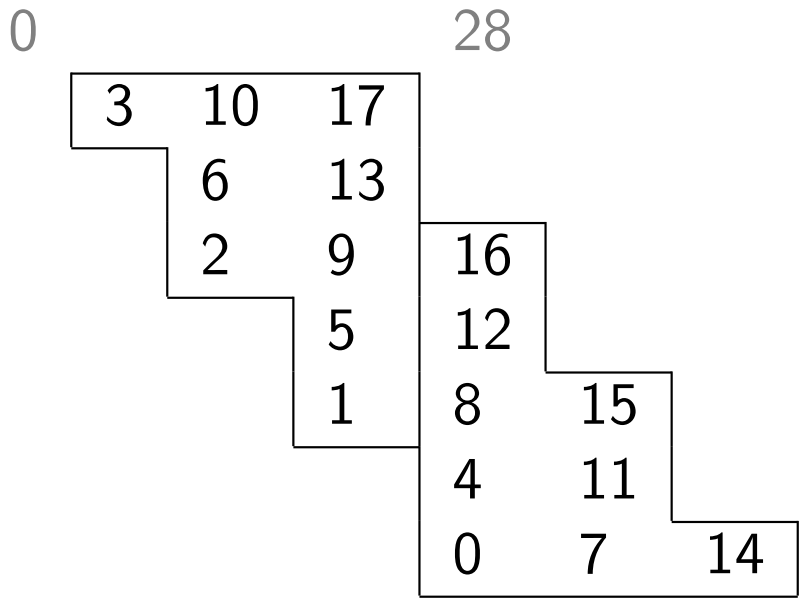


Figure: Proof without words, $(a, b) = (4, 7)$.

Takeaway: G can be organized on 2D grid.

$$G = \{ab - ax - by \geq 0 : x, y \geq 0\}.$$

Combinatorics: Catalan number

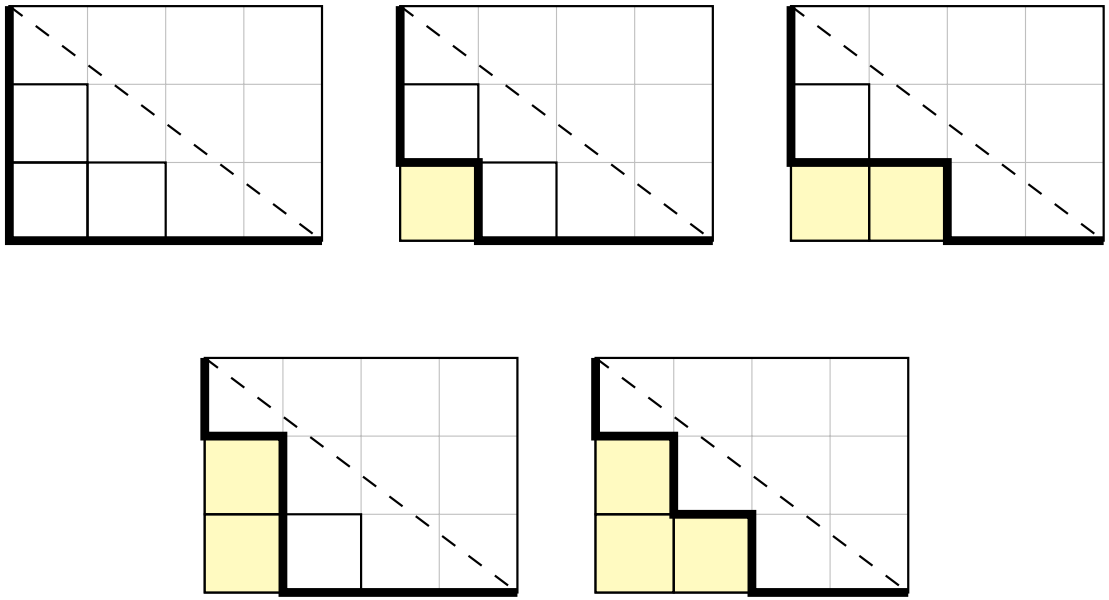
The Catalan number

$$C_n = \frac{1}{n+1}\binom{2n}{n}$$

famously counts many objects; Stanley's *Enumerative Combinatorics* lists 95 of them.

Among them is the **Dyck path**: lattice path in an $n \times (n+1)$ rectangle that stays below the main diagonal.

$C_3 = \frac{1}{4}\binom{6}{3} = 5$.



The q, t-Catalan number

... is a celebrated refinement that tracks two statistics on Dyck paths: `area` and `dinv`.

`area`:

- Straightforward definition.
- Counts full squares between the Dyck path and the diagonal.

`dinv`:

- "Diagonal inversions".
- Somewhat curious, admits several non-obviously equivalent definitions.

Definition

Let $\gcd(a, b) = 1$. Then

$$C_{a,b}(q, t) := \sum_{D \in \mathrm{Dyck}_{a,b}} q^{\mathtt{area}(D)} t^{\mathtt{dinv}(D)}.$$

The classical Catalan number corresponds to $(a, b) = (n, n+1), q = t = 1$.

Gorsky–Mazin definition of dinv

It counts cells $c \in D$ that "contribute to dinv", which means

$$\text{small hook slope} = \frac{\operatorname{leg}(c)}{\operatorname{arm}(c)+1} < \frac{a}{b} < \frac{\operatorname{leg}(c)+1}{\operatorname{arm}(c)} = \text{large hook slope}.$$

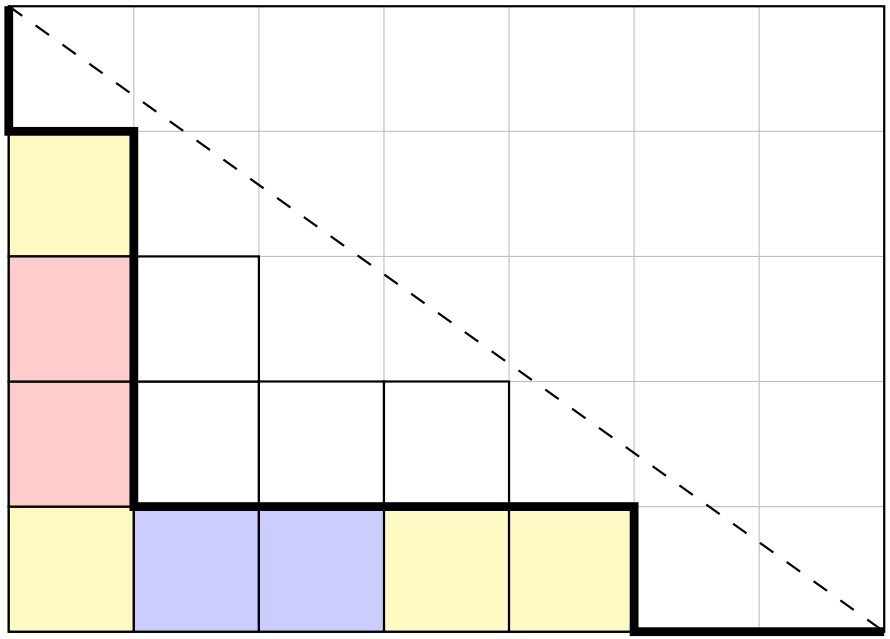
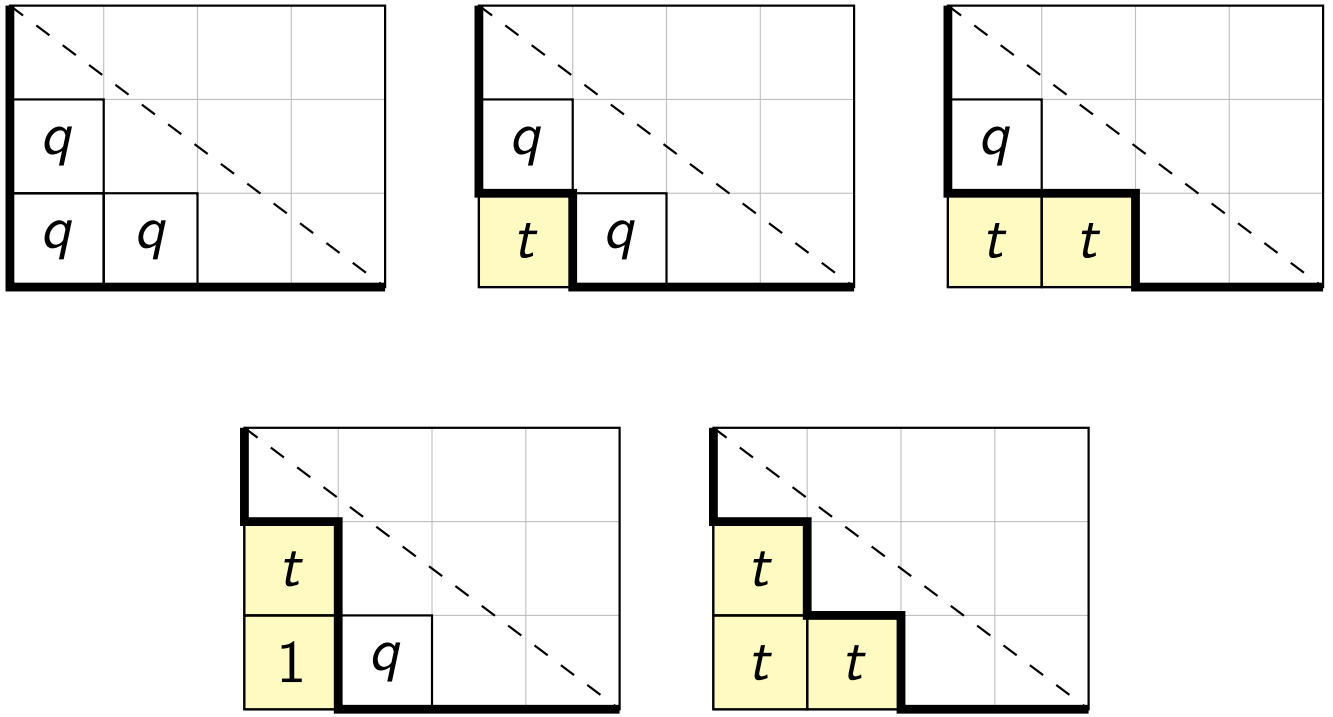


Figure: dinv $= 4$ counts yellow cells

Example



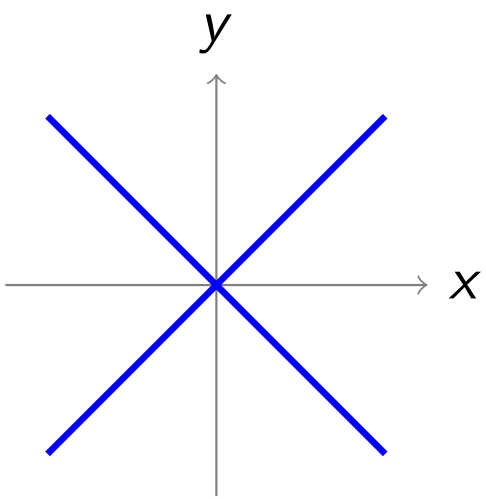
$$C_{3,4}(q,t) = q^3 + q^2t + qt^2 + qt + t^3.$$

Theorem (Garsia–Haiman, 1996)

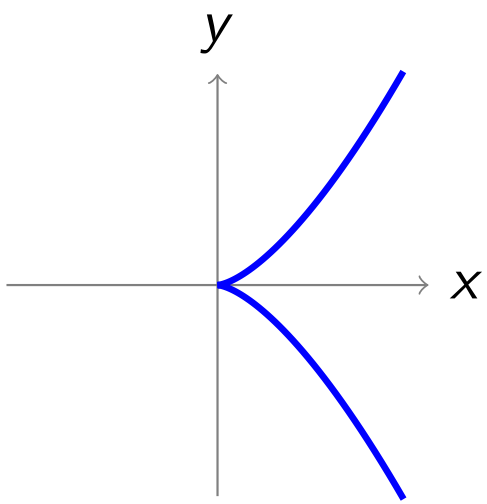
The q,t-Catalan polynomial $C_{a,b}(q,t)$ is symmetric in q and t.

Geometry: Curve singularity

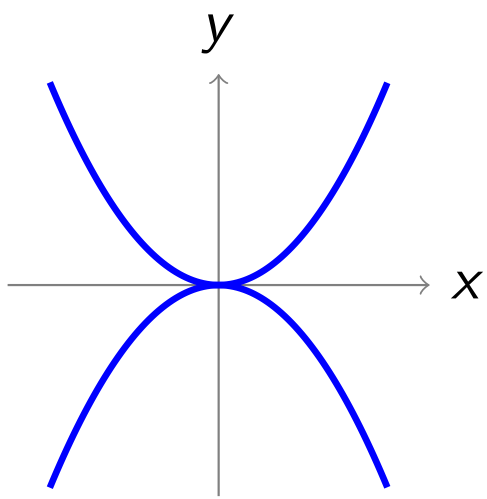
For $a, b \geq 2$, the origin of the curves $y^a = x^b$ give the first examples of familiar curve singularities.



Node ($y^2 = x^2$)



Cusp ($y^2 = x^3$)



Tacnode ($y^2 = x^4$)

Counting sheaves

In algebraic geometry, we care about **sheaves** over these curves. Algebraically, they are represented by **modules** over the ring $R = k[[x, y]]/(y^a - x^b)$. (Modules are like vector spaces, except that the behaviors can be much wilder because R is more complicated than a field.)

Question

How "many" modules are there?

The question needs to be made precise. As is a standard way to count objects up to isomorphism, we consider the "**groupoid volume**".

Precise question

Let $k = \mathbb{F}_q$ (finite field with q elements). For R above, what is

$$|\mathbf{FinMod}_R| := \sum_{M \in \mathbf{FinMod}_R/\sim} \frac{1}{|\mathrm{Aut}_R(M)|}?$$

H.–Jiang–Oblomkov

We answer the coprime case in terms of numerical semigroups, motivating key objects of this talk.
Recall $G = \mathbb{N} \setminus \langle a, b \rangle$. On the vector space $\mathbb{R}^G = \{\mathbf{n} = (n_g)_{g \in G}\}$, define a **cone**

$$C_{\mathbb{R}} = \{\mathbf{n} \in \mathbb{R}^G_{\geq 0} : n_i \leq n_j \text{ if } j - i \in \Gamma\}$$

and a **quadratic form**

$$Q(\mathbf{n}) = \sum_{i,j \in G} K(j-i) n_i n_j,$$

where $K(d) = \mathbf{1}_{d \geq 0} - \mathbf{1}_{d \geq a} - \mathbf{1}_{d \geq b} + \mathbf{1}_{d \geq a+b}$.

Example

For $(a, b) = (3, 4)$, $C_{\mathbb{R}} = \{(n_1, n_2, n_5) : 0 \leq n_1 \leq n_5, 0 \leq n_2 \leq n_5\}$,

$$Q(n_1, n_2, n_5) = n_1^2 + n_2^2 + n_5^2 + n_1 n_2 - n_1 n_5.$$

H.–Jiang–Oblomkov

Theorem (HJO)

For $\gcd(a,b)=1$, $R=\mathbb{F}_q[[x,y]]/(y^a-x^b)$, *we have*

$$|\mathbf{FinMod}_R| = \left(\prod_{n=1}^{\infty}(1-z^n)^{-1}\right) \sum_{\mathbf{n}\in\mathbb{Z}^G\cap C_{\mathbb{R}}} z^{Q(\mathbf{n})}(1+O_{\mathbf{n}}(z)) \in [0,\infty],$$

where $z=q^{-1}$ *and* $O_{\mathbf{n}}(z)\in z\mathbb{N}[z]$ *is explicit.*[a]

[a] $1+O_{\mathbf{n}}(z)$ is a generalized q-multinomial coefficient.

Sum=Product identity

The summation (denoted by $Z_{a,b}(z)$) is not just a random thing. It seems to equal an explicit infinite product!

HJO conjecture

There is an explicit sequence $r_{a,b}(i)$ $(i \geq 0)$ that is periodic of period $a+b$ such that

$$Z_{a,b}(q) = \prod_{i \geq 0} (1-q^i)^{r_{a,b}(i)}.$$

Example ($(a,b) = (2,3)$, reduces to Rogers–Ramanujan)

$$\sum_{n \geq 0} q^{n^2} \frac{1}{(1-q)\cdots(1-q^n)} = \prod_{m \geq 0} \frac{1}{(1-q^{5m+1})(1-q^{5m+4})}.$$

Example ($(a,b) = (3,4)$, amounts to an open identity)

$$\sum_{0 \leq n_1, n_2 \leq n_5} q^{n_1^2+n_2^2+n_5^2+n_1 n_2 - n_1 n_5}(1+O(q)) = \prod_{m \geq 0} \frac{1}{(1-q^{7m+1})^2(1-q^{7m+3})(1-q^{7m+4})(1-q^{7m+6})^2}.$$

Fundamental question

Question

Is Q positive definite on the cone $C_{\mathbb{R}}$?

This is necessary and sufficient for $Z_{a,b}(q)$ to be well-defined as a power series, and converges for $|q| < 1$.

After some attempt, I soon realized this question is much trickier than it seems. It is not true that Q is globally positive definite. Linear programming algorithm can find certificate for fixed a, b but it doesn't suggest a generalizable pattern.

Example $((a, b) = (4, 5))$

The answer is yes because

$$Q = \frac{{n_1}^2}{2} + (n_{11} - n_1)(n_7 - n_3) + n_1 n_2 + \frac{1}{2}(n_6 - n_1)^2 + (n_{11} - n_6)(n_{11} - n_7) + \frac{{n_2}^2}{2} + n_2 n_3 + \frac{1}{2}(n_7 - n_2)^2 + {n_3}^2 + n_3 n_6 + \frac{{n_6}^2}{2} + \frac{{n_7}^2}{2}.$$

Main result

The answer is yes!

Theorem (H., 2026, Theorem 1.3)

For $\mathbf{n} \in C_{\mathbb{R}} \setminus \{0\}$, *we have* $Q(\mathbf{n}) > 0$.

The proof requires connecting Q to the combinatorics of `dinv` and its generalization. We obtain two theorems below, which turn out to strengthen our understanding about Q beyond what was aimed for.

Subdiagram and Dyck paths

We equate G to a Young diagram, and subdiagrams of G to Dyck paths in an obvious way. By convention, assume $a < b$ and orient the diagram so the ambient rectangle is "wide" $(a \times b)$.

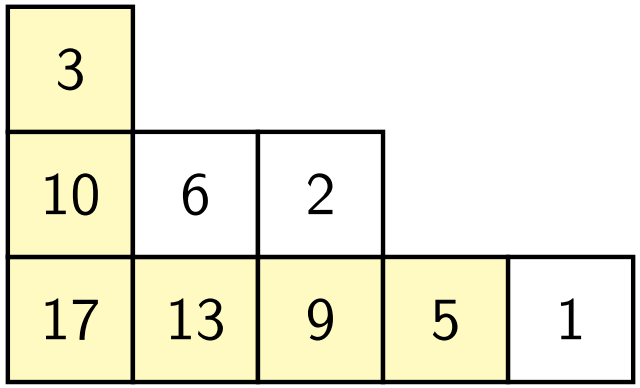


Figure: The $(4, 7)$-Dyck path shown is viewed as the subset $D = \{3, 10, 17, 13, 9, 5\}$.

For a subdiagram D, the indicator vector $\mathbf{1}_D$ is always in $C_{\mathbb{R}}$.

First cases of positivity

Theorem (H., 2026, Theorem 1.1)

For a subdiagram $D \subseteq G$, we have $Q(\mathbf{1}_D) = \mathtt{dinv}(D) \geq 0$.

How about general $\mathbf{n} \in C_{\mathbb{R}}$?
ChatGPT 5.3 gave me an idea: write $\mathbf{n}$ as a linear combination of $\mathbf{1}_{D_i}$ and expand $Q(\mathbf{n})$. It suffices to show the "cross-terms" are nonnegative.

Cross-terms

Define $B(-,-)$ to be the symmetric bilinear pairing associated with Q, so $Q(\mathbf{n}) = B(\mathbf{n},\mathbf{n})$ and $B(\mathbf{n},\mathbf{n}') = B(\mathbf{n}',\mathbf{n})$.

Question

Is it true that for subdiagrams $D, E \subseteq G$, we have $B(\mathbf{1}_D, \mathbf{1}_E) \geq 0$?

To my initial surprise, a quick vibe-coding check finds no counterexample. So ChatGPT's idea could work!

Theorem (H., 2026, Theorem 1.2)

For subdiagrams $D, E \subseteq G$, we have $B(\mathbf{1}_D, \mathbf{1}_E) = \texttt{cross-dinv}(D, E) \geq 0$ for a combinatorial statistics `cross-dinv` *whose definition is discovered in the proof.*

Definition of cross-dinv

For a cell $c \in D \cap E$, define **(small and large) mixed hook slopes**

$$m_D^E(c) = \frac{\mathrm{leg}_E(c)}{\mathrm{arm}_D(c)+1} < M_D^E(c) = \frac{\mathrm{leg}_E(c)+1}{\mathrm{arm}_D(c)}.$$

Define the **asymmetric cross-dinv** by

$$\mathtt{dinv}_D^E = \#\left\{c \in D \cap E : m_D^E(c) < \frac{a}{b} < M_D^E(c)\right\}.$$

Finally, the cross-dinv is given by

$$\mathtt{cross\text{-}dinv}(D,E) := \frac{1}{2}(\mathtt{dinv}_D^E + \mathtt{dinv}_E^D).$$

Now, I have fully described the precise claim of Theorem 1.2, the main engine of the paper.[1]

[1] Clearly $\mathtt{dinv}(D) = \mathtt{cross\text{-}dinv}(D,D)$, so Thm 1.1 is a special case of Thm 1.2.

Additional takeaway

1. Not only is `dinv` interpolated by a quadratic form (a very rigid property!), but the cross-pairing also has a combinatorial meaning.
2. $B(\mathbf{1}_D, \mathbf{1}_E) \leq |D \cap E|$.
3. For $\mathbf{n}, \mathbf{n}' \in C_{\mathbb{R}}$, we have $B(\mathbf{n}, \mathbf{n}') \geq 0$. *So the positivity of Q on $C_{\mathbb{R}}$ need not be explained by sums of squares!*

Proof workflow

1. An old-school human bijective proof.
2. First, simplify the algebra to get a "cancellation-free" formula. Evaluating Q amounts to counting certain "arrows" generated by some rule.
3. I want to prove that the number of certain "arrows" is the number of certain "cells".
4. Vibe-code to generate lots of examples. Use visual observation to guess a bijection. *AI failed to come up with anything close.*
5. Verify the bijection works and write a clean proof. *Lean auto-formalization makes sure the proof has no flaw.*

Proof of Theorem 1.1: $Q(\mathbf{1}_D) = \mathtt{dinv}(D)$

For $i, j \in G$, draw an arrow $i \to j$ if $0 \leq j - i < a$. Let U_D be the cells in $G \setminus D$ "just above" D (including bottom row).

Lemma (Proved by telescoping; proof omitted)

$$Q(\mathbf{1}_D) = |D| - \#\{(i,j) \in D \times U_D : i \to j\}$$

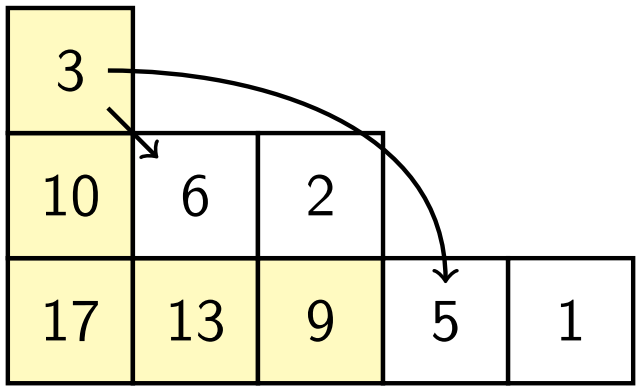


Figure: The $(4,7)$-Dyck path D has 2 arrows from D to U_D, so $Q(\mathbf{1}_D) = 5 - 2 = 3$.

Q vs dinv

To prove they are the same, we need to prove there are as many arrows as cells *not* contributing to dinv (shaded gray).

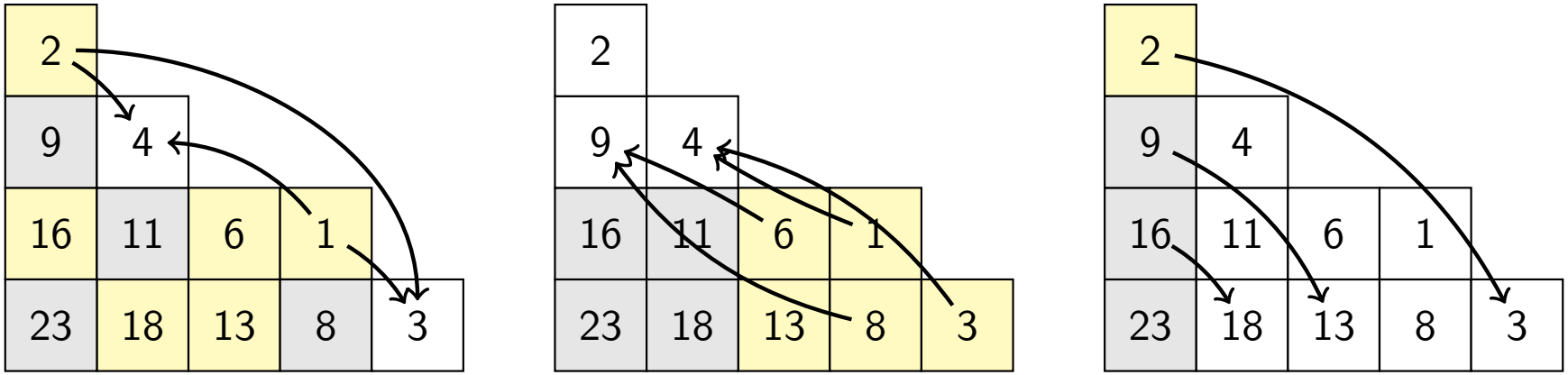


Figure: $(a, b) = (5, 7)$

Observation: map an arrow to "its southwest corner"...but not quite.

Towards a precise bijection

To fix the "not quite", let's recall a cell can fail to contribute to `dinv` in two ways: too steep (red) or too flat (blue). Get a finer picture.

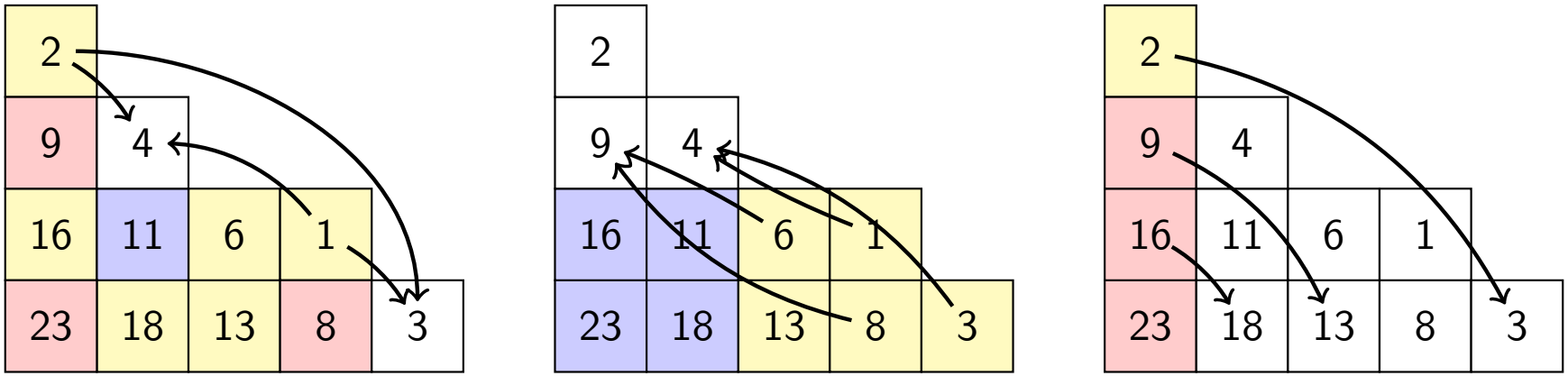


Figure: $(a, b) = (5, 7)$

Observation: southeast-pointing arrows go to red cells (modification needed); northwest-point arrows go to blue cells (no modification needed?).

The finalized rule

Color arrows based on general orientation. To construct bijection,

- blue arrows: just "do it".
- red arrows: **move it up** parallelly until the source lands at the top cell of D, then "do it".

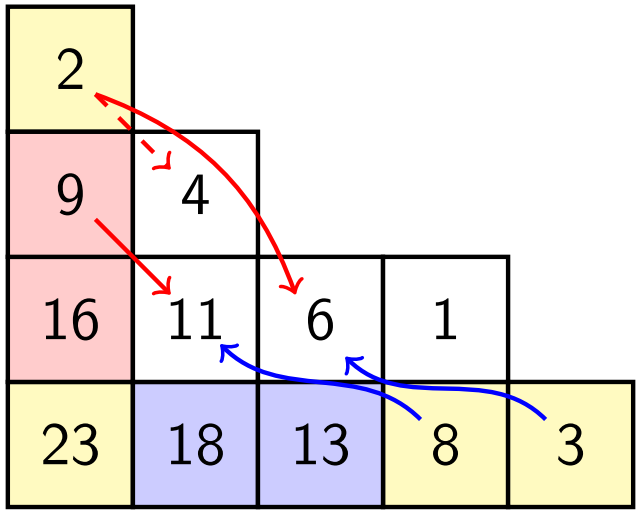


Figure: $(a, b) = (5, 7)$

Proof of Theorem 1.2

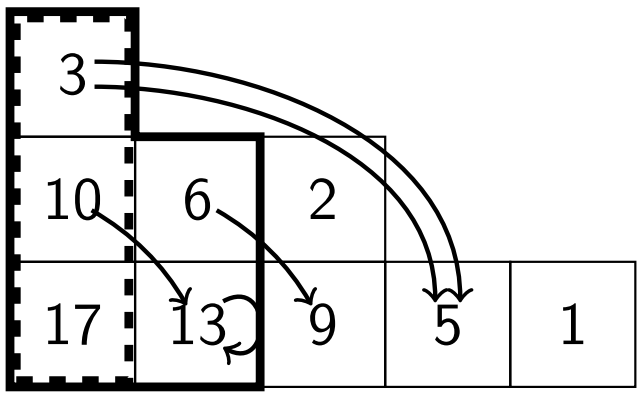
Let $N(X, Y)$ be the set of arrows $i \to j$ such that $i \in X$ and $j \in Y$.

Lemma (Proof omitted)

For subdiagrams $D, E \subseteq G$, we have

$$2B(D, E) = |D| + |E| - |N(D, U_E)| - |N(E, U_D)|.$$

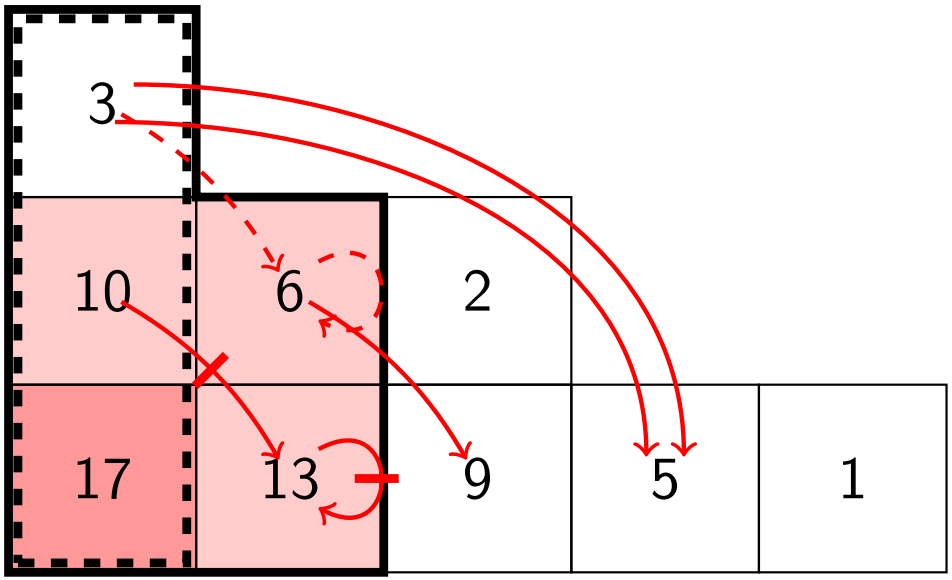
To prove its nonnegativity, we draw all arrows in $N(D, U_E)$ and $N(E, U_D)$, and show they are not as many as $|D| + |E|$.



Outline of D
Outline of E

Precise rule

New consideration: self-loops should be red, i.e., have the same special treatment like southeast-pointing arrows.



Outline of D

Outline of E

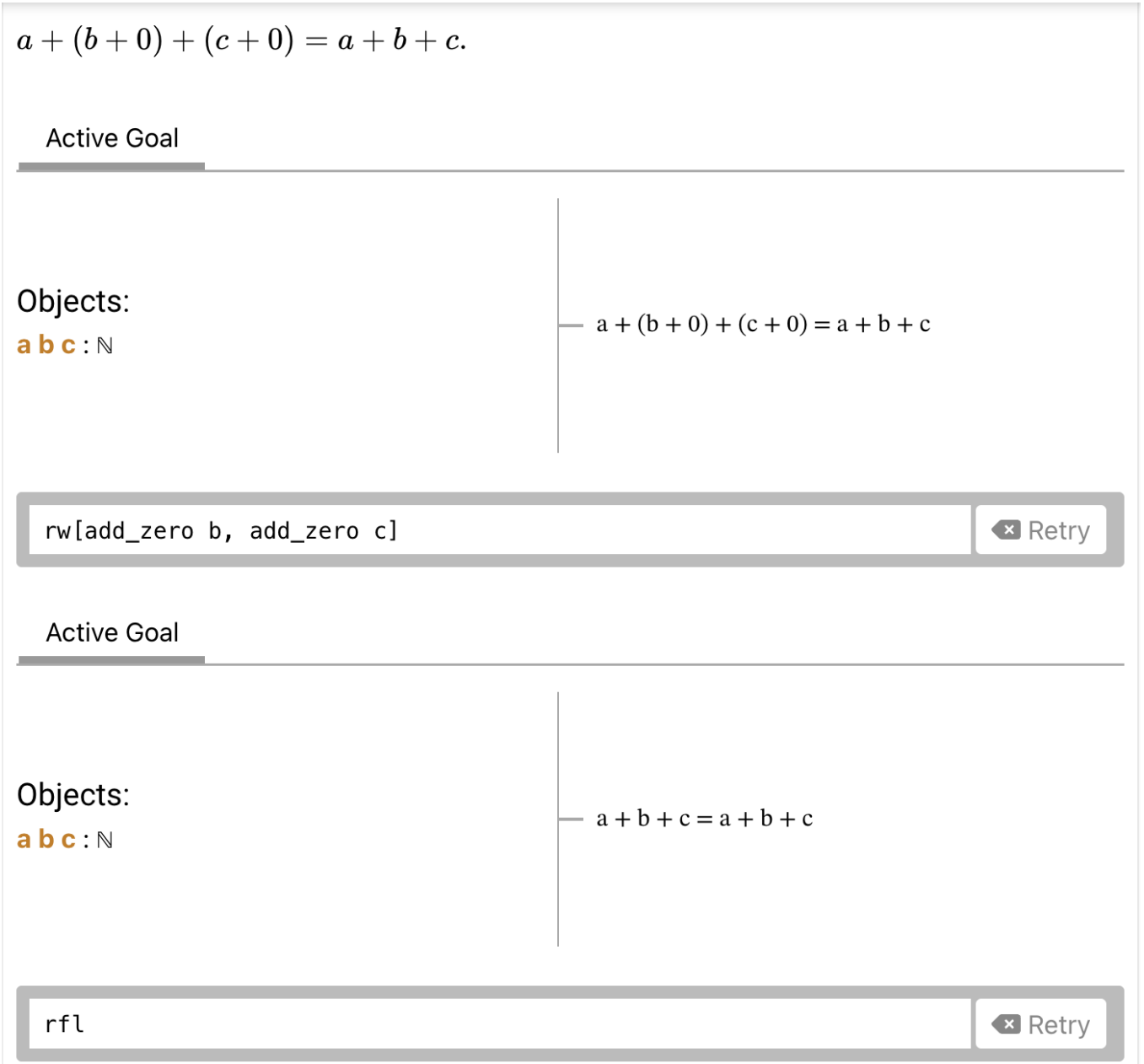
Original arrow

New arrow after shift

Old arrow before shift

What is Lean?

- A programming language that **verifies** theorem's proof.
- It only compiles when the proof works *without handwaving*.
- To get a hang of the language, play games at `https://adam.math.hhu.de/`.



What is auto-formalization?

- Human+Lean combo: Reliable, but human needs to deal with the syntax, library, etc.
- LLM proof: Get human-readable proof, but often wrong and hard to catch.
- **Auto-formalization**=LLM+Lean combo: Use LLM to read natural language proof and generate Lean code.
- Human's job: make sure the problem statement is correctly formalized; you can trust the proof!

Auto-formalization of Theorem 1.2 by AxiomMath

Problem statement in natural language

Main Definition(s)

Let a, b be coprime positive integers with $a < b$.

Definition 1 (Gap set and subdiagrams). The *numerical semigroup* generated by a and b is $\langle a, b\rangle = \{sa + tb : s, t \in \mathbb{Z}_{\geq 0}\} \subset \mathbb{Z}_{\geq 0}$. Its *gap set* is $G = \{n \in \mathbb{Z}_{>0} : n \notin \langle a, b\rangle\}$, a finite set of cardinality $(a-1)(b-1)/2$. We equip G with the partial order $i \preceq j$ defined by $j - i \in \langle a, b\rangle$ (where $j - i$ is ordinary integer subtraction; in particular $j \geq i$).

A *subdiagram* (or *Dyck path*) $D \subseteq G$ is an upward closed subset of $(G, \preceq)$: if $i \in D$ and $i \preceq j$ with $j \in G$, then $j \in D$.

Grid realization. The map $(x, y) \mapsto g(x, y) = ab - ax - by$ restricts to a bijection from $\{(x, y) \in \mathbb{Z}^2_{\geq 1} : g(x, y) > 0\}$ to G, realizing G as a Young diagram (oriented with $+x$ east and $+y$ north). Under this bijection, subtracting a from a gap value corresponds to moving one cell east in the grid, and subtracting b corresponds to moving one cell north. Subdiagrams correspond to sub-Young-diagrams in the usual sense.

Definition 2 (Quadratic form Q and bilinear form B). Define the kernel $K(d) = \mathbf{1}^{d \geq 0} - \mathbf{1}^{d \geq a} - \mathbf{1}^{d \geq b} + \mathbf{1}^{d \geq a+b}$ for $d \in \mathbb{Z}$, so that $K(d) = 1$ for $0 \leq d < a$, $K(d) = -1$ for $b \leq d < a + b$, and $K(d) = 0$ otherwise. The quadratic form on $\mathbb{R}^G$ is $Q(\mathbf{n}) = \sum_{i,j \in G} K(j - i)\, n_i\, n_j$, where the sum is over gap values $i, j \in G \subset \mathbb{Z}_{>0}$. The symmetric bilinear form associated with Q is $B(\mathbf{n}, \mathbf{n}') = \frac{1}{2}\big(Q(\mathbf{n} + \mathbf{n}') - Q(\mathbf{n}) - Q(\mathbf{n}')\big)$.

Definition 3 (Arm and leg lengths). For a subdiagram $D \subseteq G$ and a gap value $c \in D$, define: $\mathrm{arm}_D(c) = \max\{k \geq 0 : c - ka \in D\}$, $\quad \mathrm{leg}_D(c) = \max\{k \geq 0 : c - kb \in D\}$, where $c - ka$ and $c - kb$ denote ordinary integer subtraction. These are well-defined non-negative integers (the set contains $k = 0$ since $c \in D$, and is bounded since D is finite). In the grid realization, $\mathrm{arm}_D(c)$ counts consecutive cells eastward from c remaining in D, and $\mathrm{leg}_D(c)$ counts consecutive cells northward from c remaining in D.

Definition 4 (Cross-dinv). For subdiagrams $D, E \subseteq G$ and $c \in D \cap E$, say that c *contributes to* dinv^E_D if $b \cdot \mathrm{leg}_E(c) < a \cdot (\mathrm{arm}_D(c) + 1) \quad \text{and} \quad a \cdot \mathrm{arm}_D(c) < b \cdot (\mathrm{leg}_E(c) + 1)$. (When $\mathrm{arm}_D(c) > 0$, this is equivalent to $\frac{\mathrm{leg}_E(c)}{\mathrm{arm}_D(c)+1} < \frac{a}{b} < \frac{\mathrm{leg}_E(c)+1}{\mathrm{arm}_D(c)}$. When $\mathrm{arm}_D(c) = 0$, the second inequality holds automatically and the condition reduces to $b \cdot \mathrm{leg}_E(c) < a$.)

The *cross-dinv* of the pair (D, E) is $\mathrm{dinv}(D, E) = \frac{1}{2}\big(\#\{c \in D \cap E : c \text{ contributes to } \mathrm{dinv}^E_D\} + \#\{c \in D \cap E : c \text{ contributes to } \mathrm{dinv}^D_E\}\big)$. When $D = E$, this recovers the classical Gorsky–Mazin $\mathrm{dinv}(D)$ statistic.

Main Statement(s)

Theorem 1.2. Let a, b be coprime positive integers with $a < b$. Let G, B, and $\mathrm{dinv}(D, E)$ be as in Definitions 1–4 above. For any two subdiagrams $D, E \subseteq G$, $B(\mathbf{1}_D, \mathbf{1}_E) = \mathrm{dinv}(D, E)$, where $\mathbf{1}_D, \mathbf{1}_E \in \mathbb{R}^G$ denote the indicator vectors of D and E respectively.

Context and Significance

Auto-formalization of Theorem 1.2 by AxiomMath

AI-generated problem file in Lean

```
import Mathlib

open Finset

namespace RationalDinv

-- Definition: Value function $g : \mathbb{Z}^2 \to \mathbb{Z}$
-- $g(x,y) = ab - ax - by$
def gVal (a b : ℕ) (p : ℤ × ℤ) : ℤ :=
  (a : ℤ) * (b : ℤ) - (a : ℤ) * p.1 - (b : ℤ) * p.2

-- The gap set $G$ as a predicate on $\mathbb{Z}^2$:
-- $G = \{(x,y) \in \mathbb{Z}_{\geq 1}^2 : g(x,y) > 0\}$
def GapSet (a b : ℕ) : Set (ℤ × ℤ) :=
  {p | 1 ≤ p.1 ∧ 1 ≤ p.2 ∧ 0 < gVal a b p}
```

```
-- Indicator function for a subdiagram (as a vector in $\mathbb{R}^G$)
noncomputable def indicatorVec (D : Finset (ℤ × ℤ)) : ℤ × ℤ → ℝ :=
  fun p => if p ∈ D then (1 : ℝ) else 0

/-
## Main Theorem

For any subdiagrams $D, E \subseteq G$:
$$B(\mathbf{1}_D, \mathbf{1}_E) = \mathbf{dinv}(D, E).$$
-/
theorem bilinForm_eq_crossDinv (a b : ℕ) (ha : 0 < a) (hb : 0 < b) (hab : a < b)
    (hcop : Nat.Coprime a b) (D E : Finset (ℤ × ℤ))
    (hD : IsSubdiagram a b D) (hE : IsSubdiagram a b E) :
    bilinForm a b (indicatorVec D) (indicatorVec E) = crossDinv a b D E := by
  sorry

end RationalDinv
```

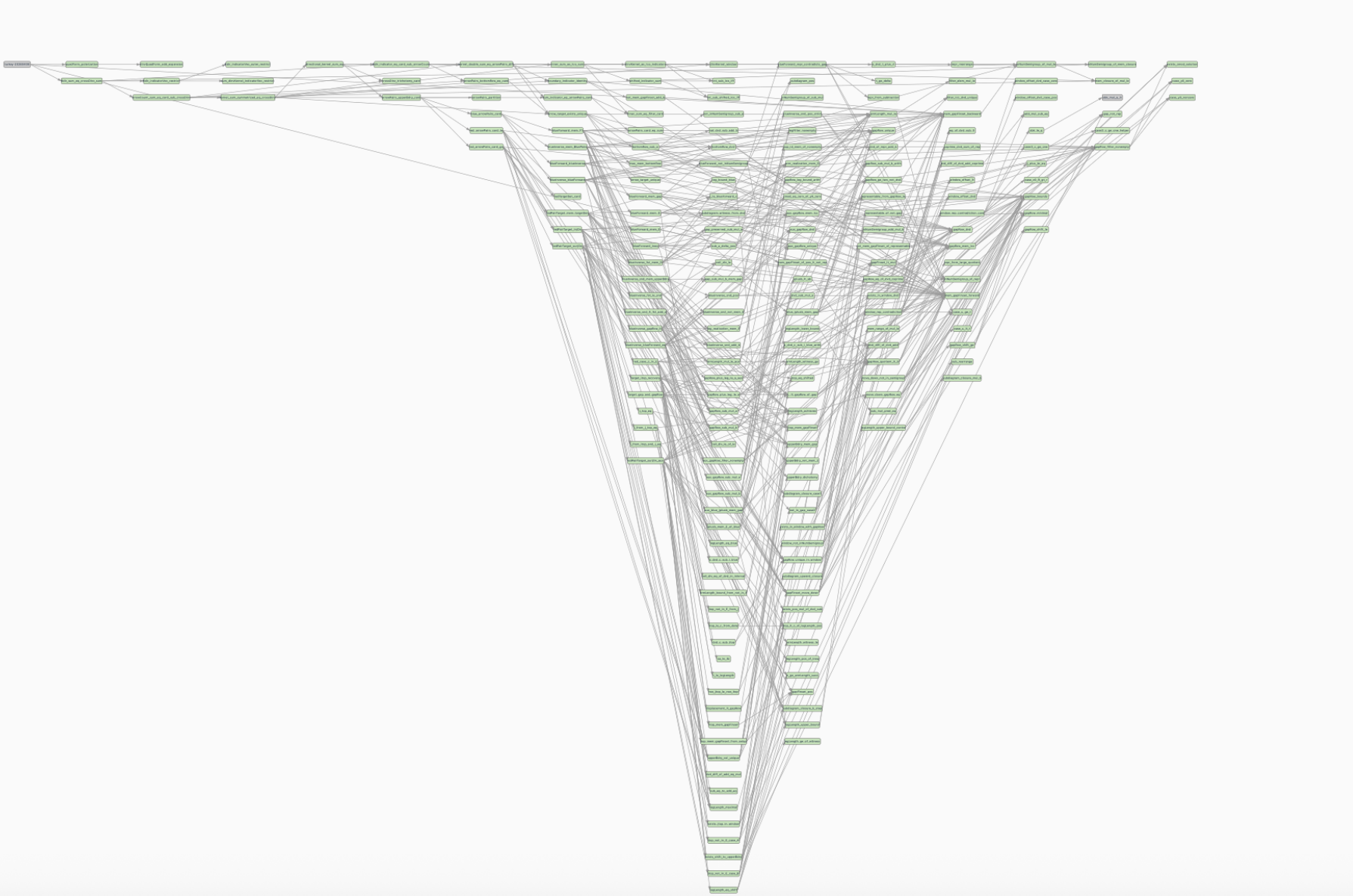
Auto-formalization of Theorem 1.2 by AxiomMath

List of subproblems (when in progress)

- turkey-20260409 (610 subproblems, 6 immediate)
  - mem_gapFinset_forward
  - mem_gapFinset_backward (3 subproblems, 1 immediate)
  - quadForm_polarization (1 subproblems, 1 immediate)
  - Bdir_sum_eq_crossDinv_sum (596 subproblems, 4 immediate)
  - mem_gapFinset_iff (2 subproblems, 2 immediate)
    - [mem_gapFinset_forward]
    - [mem_gapFinset_backward]
  - bilinForm_indicator_eq_crossDinv (2 subproblems, 2 immediate)
    - [quadForm_polarization]
    - [Bdir_sum_eq_crossDinv_sum]

Auto-formalization of Theorem 1.2 by AxiomMath

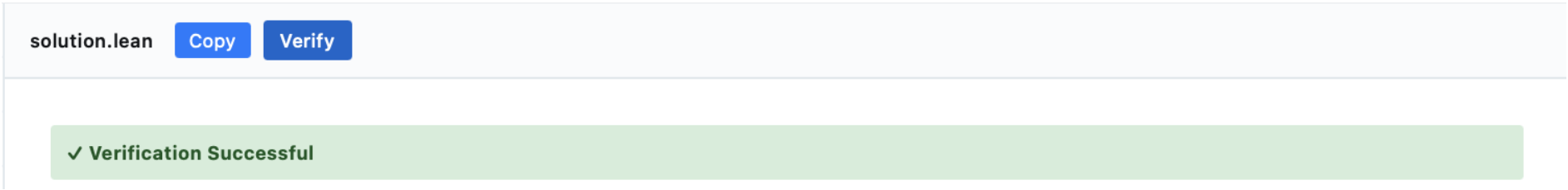
Dependency graph of subproblems (green means verified)



Auto-formalization of Theorem 1.2 by AxiomMath

Final lines of the solution

```
2568  lemma two_bilinForm_eq_dinvAsym_sum (a b : ℕ) (ha : 0 < a) (hb : 0 < b) (hab : a < b)
2569      (hcop : Nat.Coprime a b) (D E : Finset (ℤ × ℤ))
2570      (hD : IsSubdiagram a b D) (hE : IsSubdiagram a b E) :
2571      2 * bilinForm a b (indicatorVec D) (indicatorVec E) =
2572        ((dinvAsym a b D E + dinvAsym a b E D : ℕ) : ℝ) := by
2573    have h1 := two_bilinForm_eq_unsym_sum a b D E hD.1 hE.1
2574    have h2 := bilinFormUnsym_eq a b ha hb hab hcop D E hD hE
2575    have h3 := bilinFormUnsym_eq a b ha hb hab hcop E D hE hD
2576    have h4 := arrowPairs_card_eq a b ha hb hab hcop D E hD hE
2577    have h5 := arrowPairs_card_eq a b ha hb hab hcop E D hE hD
2578    have h6 := blue_plus_red_eq a b ha hb hab hcop D E hD hE
2579    have h7 := blue_plus_red_eq a b ha hb hab hcop E D hE hD
2580    have h4' : ((arrowPairs a b D (upperBoundary a b E)).card : ℝ) =
2581      ((blueCells a b D E).card : ℝ) + ((redCells a b D E).card : ℝ) := by
2582      exact_mod_cast h4
2583    have h5' : ((arrowPairs a b E (upperBoundary a b D)).card : ℝ) =
2584      ((blueCells a b E D).card : ℝ) + ((redCells a b E D).card : ℝ) := by
2585      exact_mod_cast h5
2586    have h6' : ((blueCells a b D E).card : ℝ) + ((redCells a b E D).card : ℝ) +
2587      (dinvAsym a b D E : ℝ) = (E.card : ℝ) := by exact_mod_cast h6
2588    have h7' : ((blueCells a b E D).card : ℝ) + ((redCells a b D E).card : ℝ) +
2589      (dinvAsym a b E D : ℝ) = (D.card : ℝ) := by exact_mod_cast h7
2590    push_cast
2591    linarith
2592
2593  theorem bilinForm_eq_crossDinv (a b : ℕ) (ha : 0 < a) (hb : 0 < b) (hab : a < b)
2594      (hcop : Nat.Coprime a b) (D E : Finset (ℤ × ℤ))
2595      (hD : IsSubdiagram a b D) (hE : IsSubdiagram a b E) :
2596      bilinForm a b (indicatorVec D) (indicatorVec E) = crossDinv a b D E := by
2597    have h := two_bilinForm_eq_dinvAsym_sum a b ha hb hab hcop D E hD hE
2598    unfold crossDinv
2599    linarith
```



Thank You!

Questions?