Nonexistence Certificates for Ovals in a Projective Plane of Order Ten

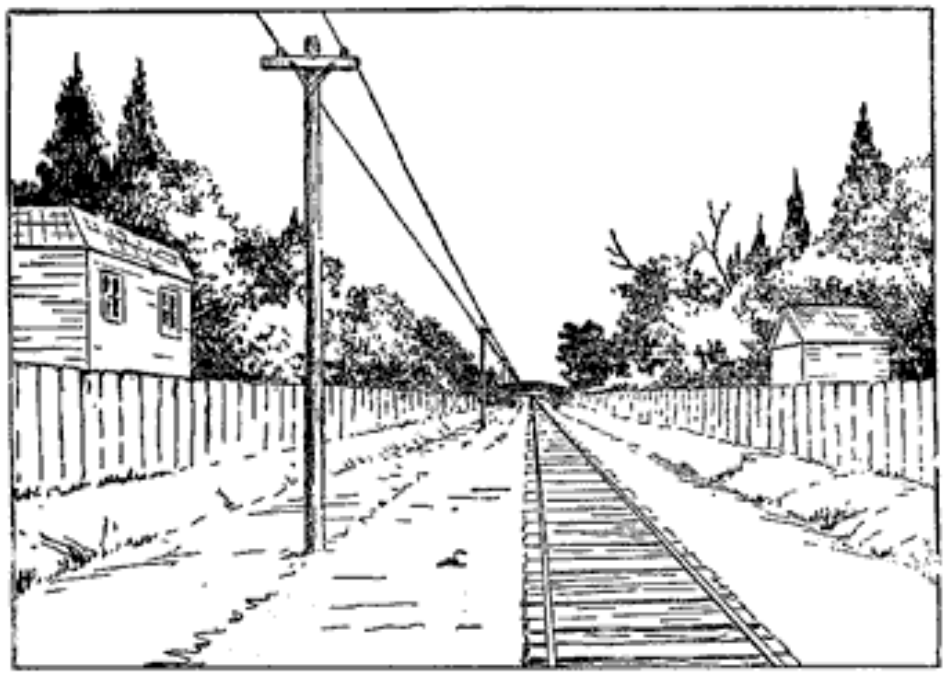
Curtis Bright[1,2] Kevin Cheung[1]
Brett Stevens[1] Ilias Kotsireas[3]
Vijay Ganesh[2]

[1]Discrete Mathematics Group, Carleton University
[2]Computer Aided Reasoning Group, University of Waterloo
[3]Computer Algebra Research Group, Wilfrid Laurier University

June 8, 2020

Overview

We use a tool called MathCheck (based on satisfiability solvers and computer algebra) to generate certificates proving the nonexistence of ovals in Lam's problem from projective geometry.



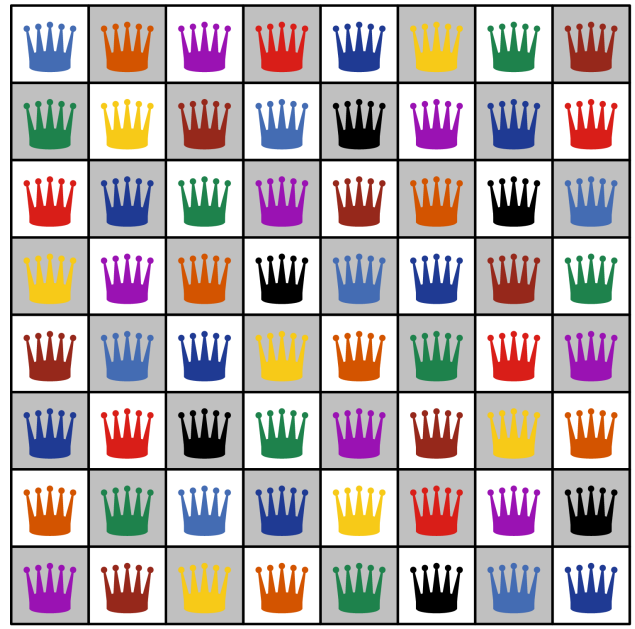
SAT:

Boolean satisfiability problem

Effectiveness of SAT solvers

Surprisingly, many problems that have nothing to do with logic can be effectively solved by translating them into Boolean logic and using a SAT solver:

- Discrete optimization
- Hardware and software verification
- Proving/disproving conjectures



Additionally, SAT solvers produce unsatisfiability certificates when no solutions exist.

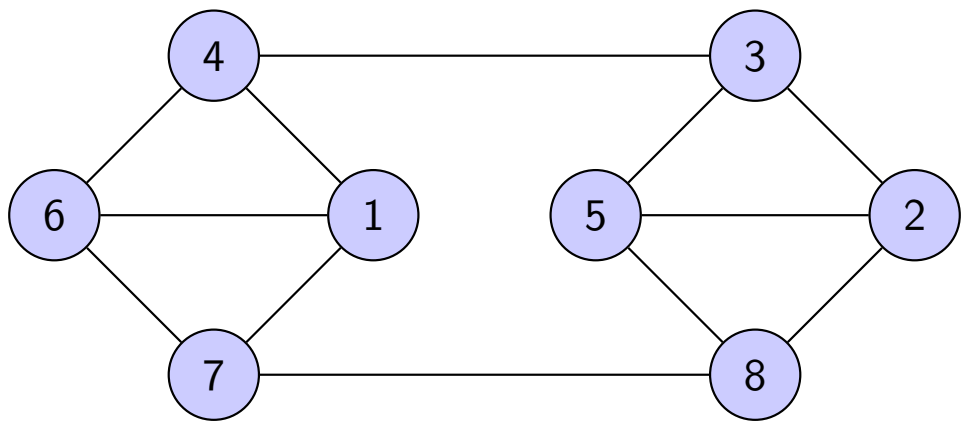
CAS:

Computer algebra system

Effectiveness of CASs

Computer algebra systems can perform calculations and manipulate expressions from many branches of mathematics:

- Determining if graphs are isomorphic
- Row reducing a matrix
- Detecting symmetries of combinatorial objects



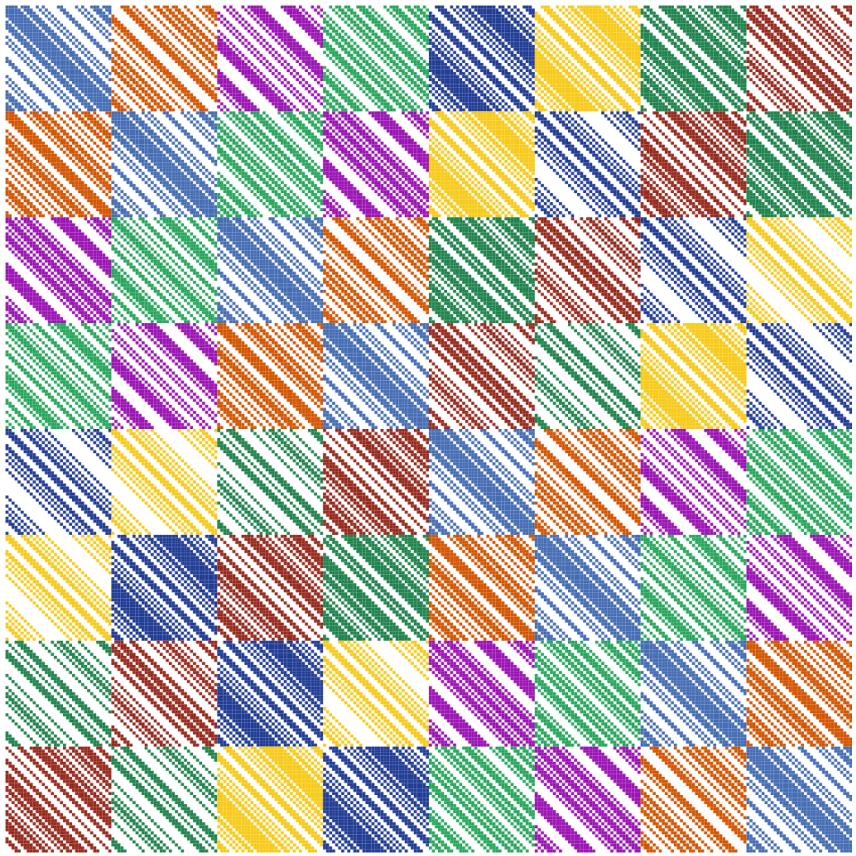
For example, the symmetry group of this graph has generators $(2\ 5)$, $(3\ 8)(4\ 7)$, and $(1\ 2)(3\ 4)(5\ 6)(7\ 8)$.

SAT + CAS

Search + Math

MathCheck: A SAT+CAS system

We've used MathCheck to explicitly construct examples (or to produce nonexistence certificates) of combinatorial objects like Hadamard matrices.



Lam's Problem and Projective Geometry

History

Since 300 BC, mathematicians tried to derive Euclid's "parallel postulate" from his first four postulates for geometry.

The existence of projective geometries shows this is impossible! These geometries satisfy a "projective axiom" that any two lines meet in a unique point.

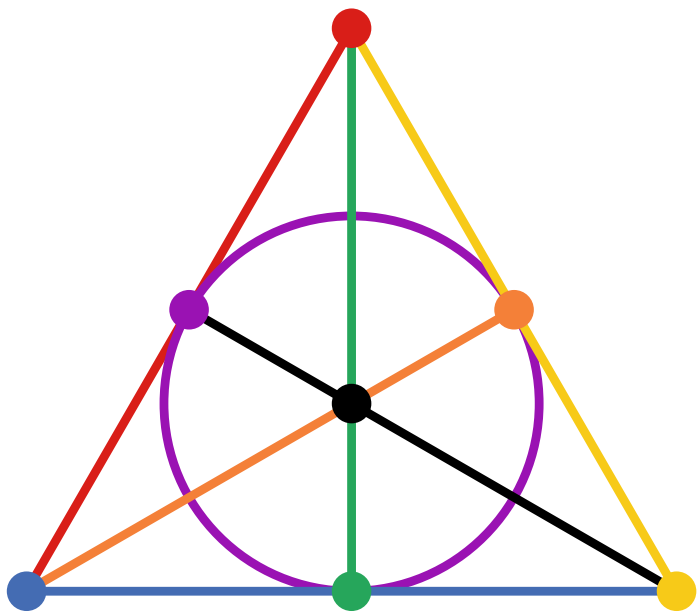
Finite geometries

A geometry is *finite* if it contains a finite number of points.

All finite projective geometries have been classified except for those with two dimensions (the *projective planes*).

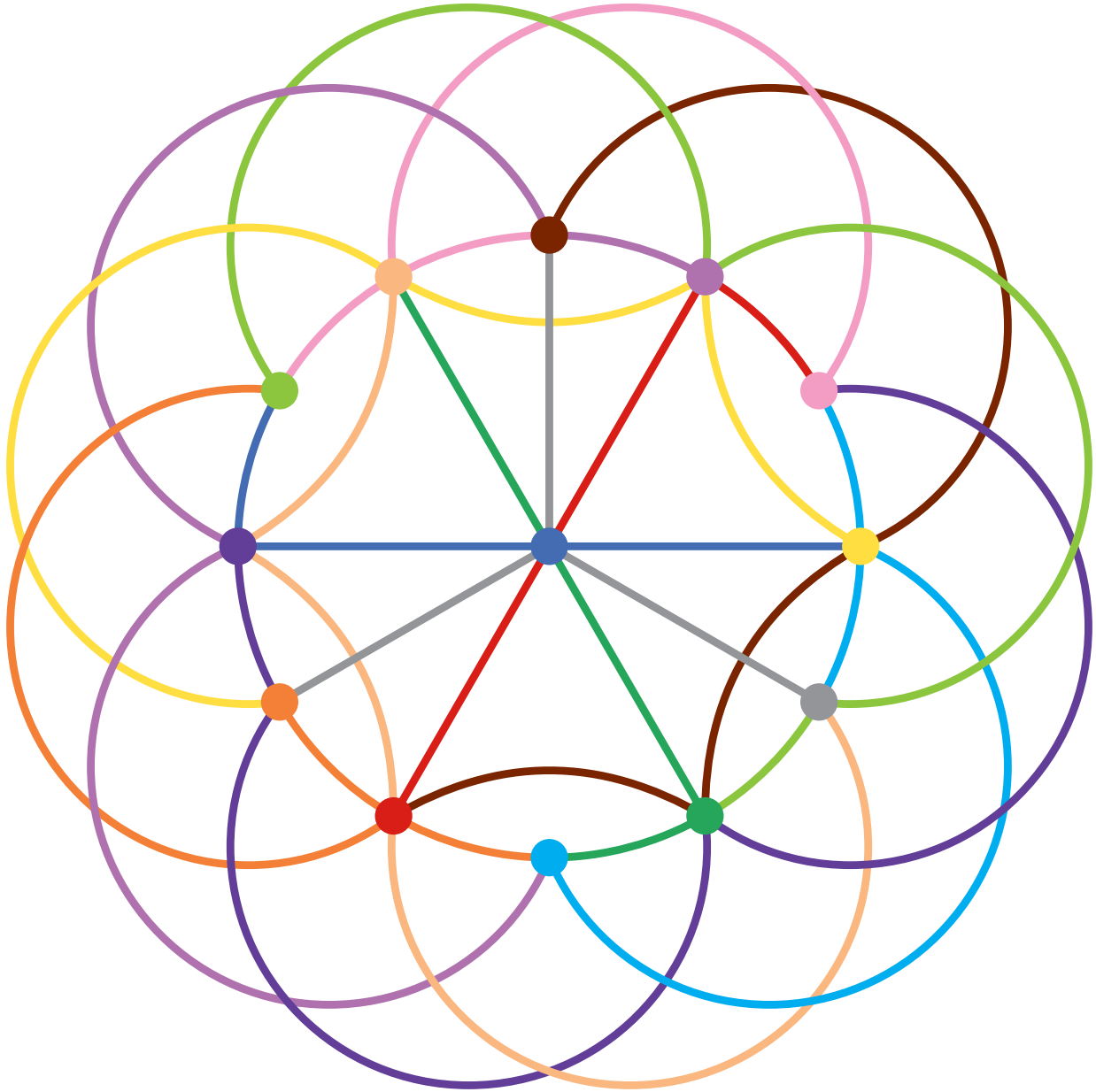
Projective plane of order 2

A projective plane is of *order n* if all lines contain $n + 1$ points.



point 1 line 1
point 2 line 2
point 3 line 3
point 4 line 4
point 5 line 5
point 6 line 6
point 7 line 7

Projective plane of order 3



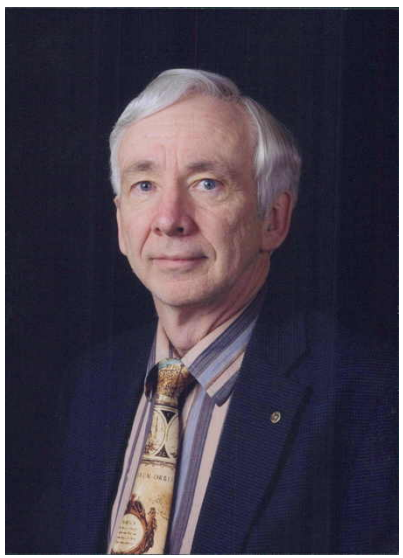
Lam's problem

The first order for which it is theoretically uncertain if projective planes exist is $n = 10$.

Lam's problem

The first order for which it is theoretically uncertain if projective planes exist is $n = 10$.

> *The structure of ovals is likely to be important to the attempt to settle the case 10 existence question. . .*

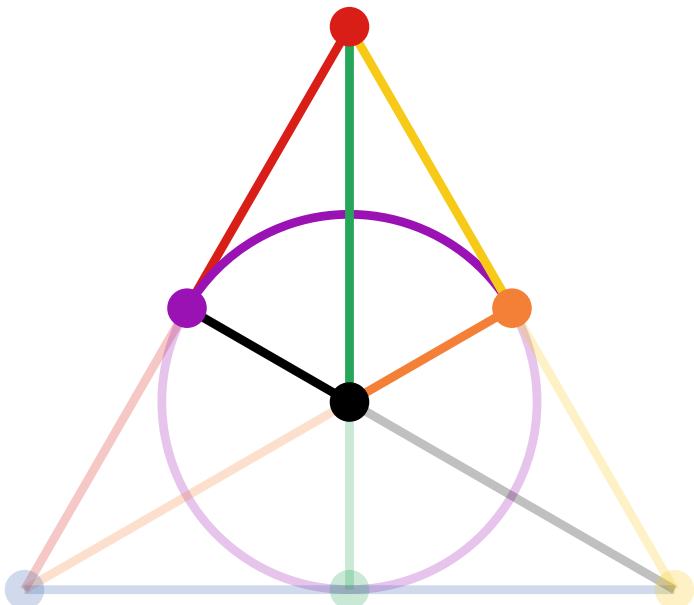


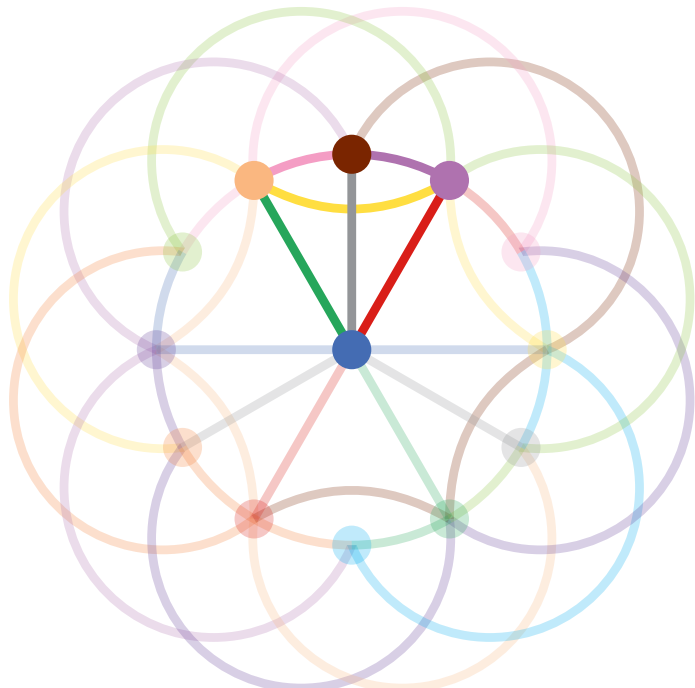
D. W. Erbach (1976)
The non-existence of a certain finite projective plane

Ovals

An *oval* is a set of points such that no three lie on the same line and is of the largest possible size: $n + 2$ points (even orders n) or $n + 1$ points (odd orders n).

All *known* projective planes contain ovals.





Ovals in order 10

Recently the search was finally finished without finding such a structure . . . we are confident that there are no ovals in a plane of order 10.

Lam, Thiel, Swiercz, McKay (1983)

Left to right: Swiercz, McKay, Lam, Thiel

Verification

Their search used custom-written software run once on a single piece of hardware. We must simply trust that it ran to completion.

Lam et al. requested an independent search to verify the result. Apparently this had never been done.

Nonexistence Certificates

Nonexistence certificates

We provide certificates that an independent party can use to verify Lam et al.'s nonexistence result.

The certificates rely on an encoding of the existence problem into Boolean logic.

Incidence matrices

1	1	0	1	0	0	0
0	1	1	0	1	0	0
0	0	1	1	0	1	0
0	0	0	1	1	0	1
1	0	0	0	1	1	0
0	1	0	0	0	1	1
1	0	1	0	0	0	1

Boolean matrix where (i, j)th entry is 1 exactly when the ith line contains the jth point.

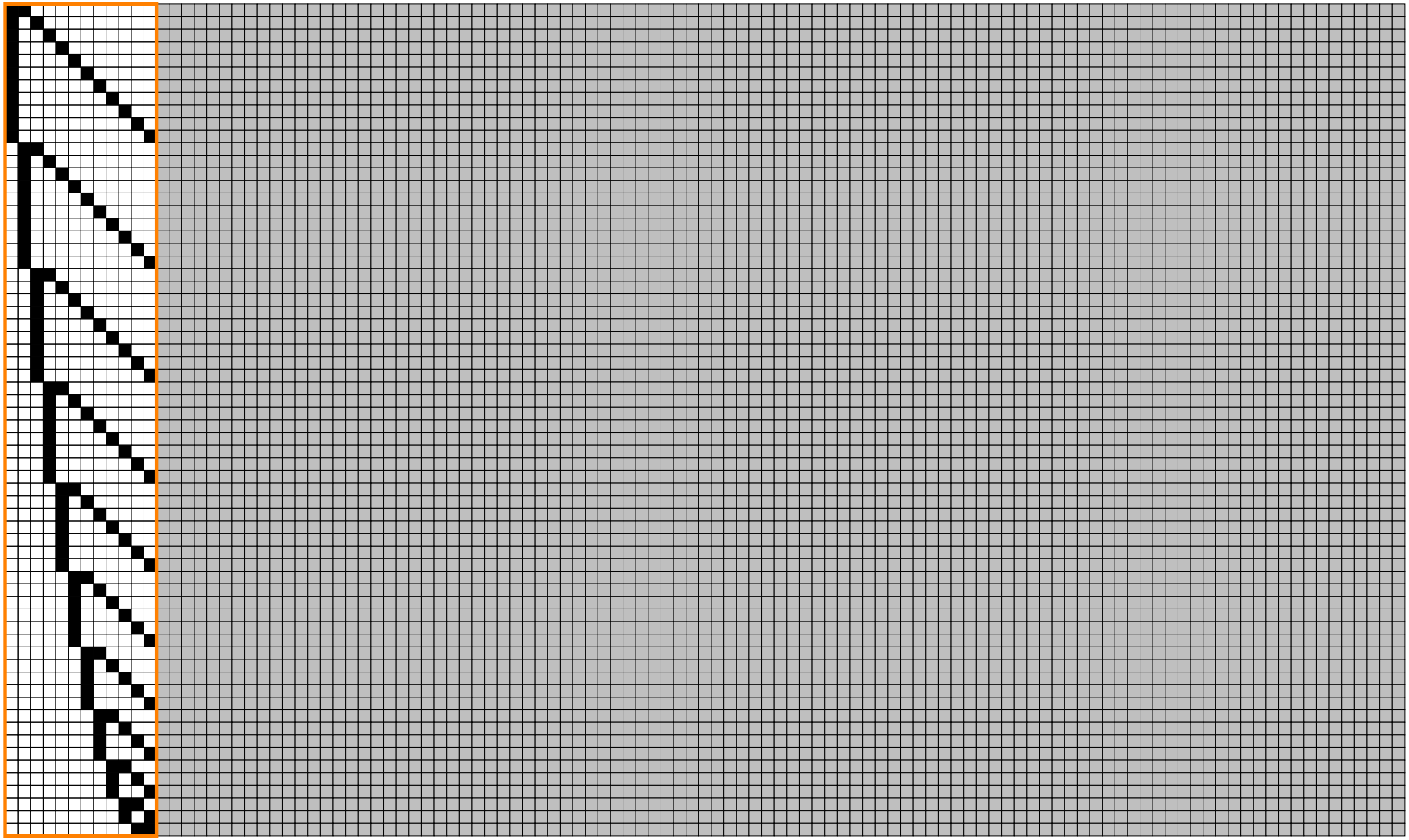
SAT encoding: false $\equiv 0$, true $\equiv 1$

Starting structure

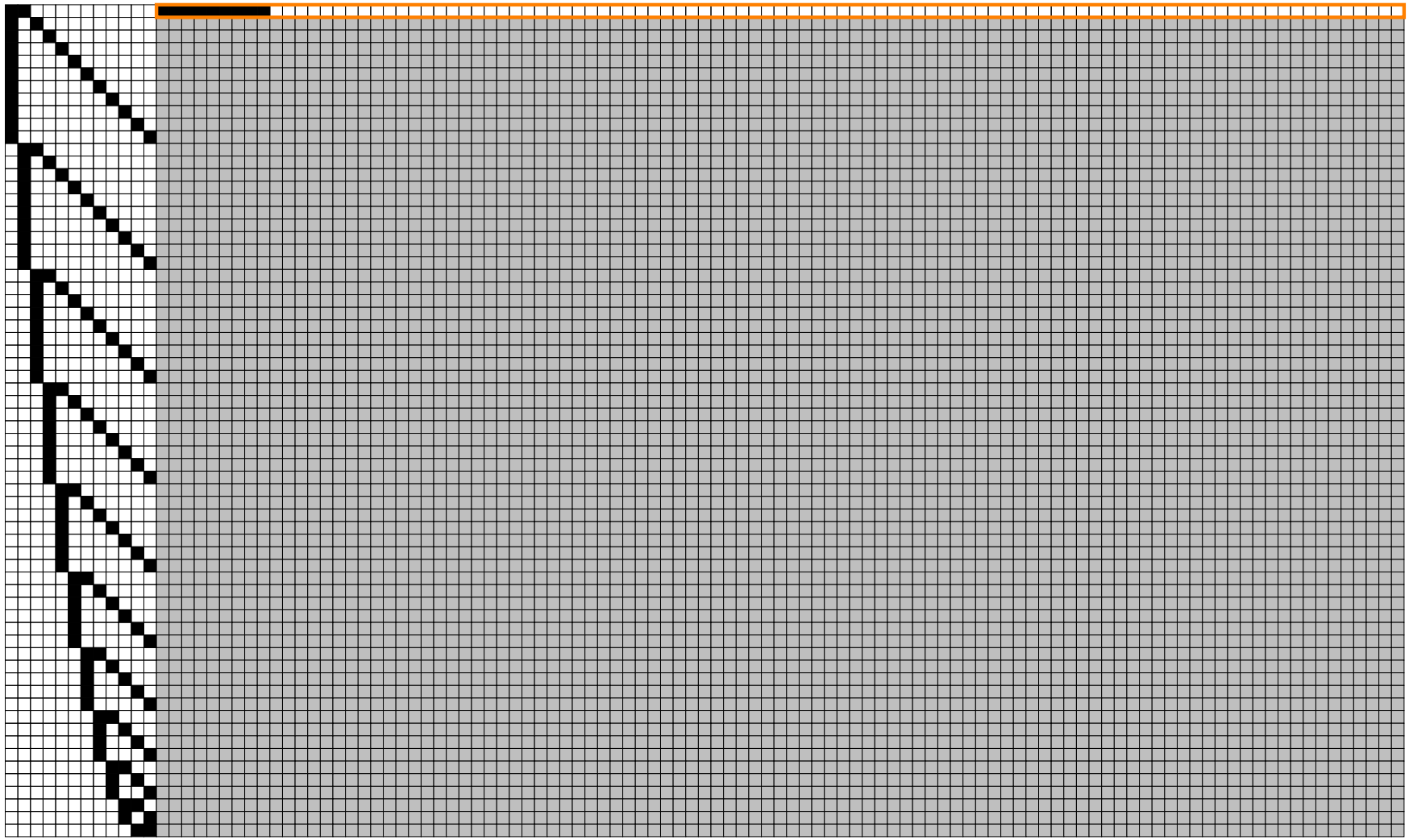
Suppose an oval in a projective plane of order ten exists and consists of its first twelve points.

Each pair of points in the oval define a unique line, and therefore there are $\binom{12}{2} = 66$ lines incident to the oval.

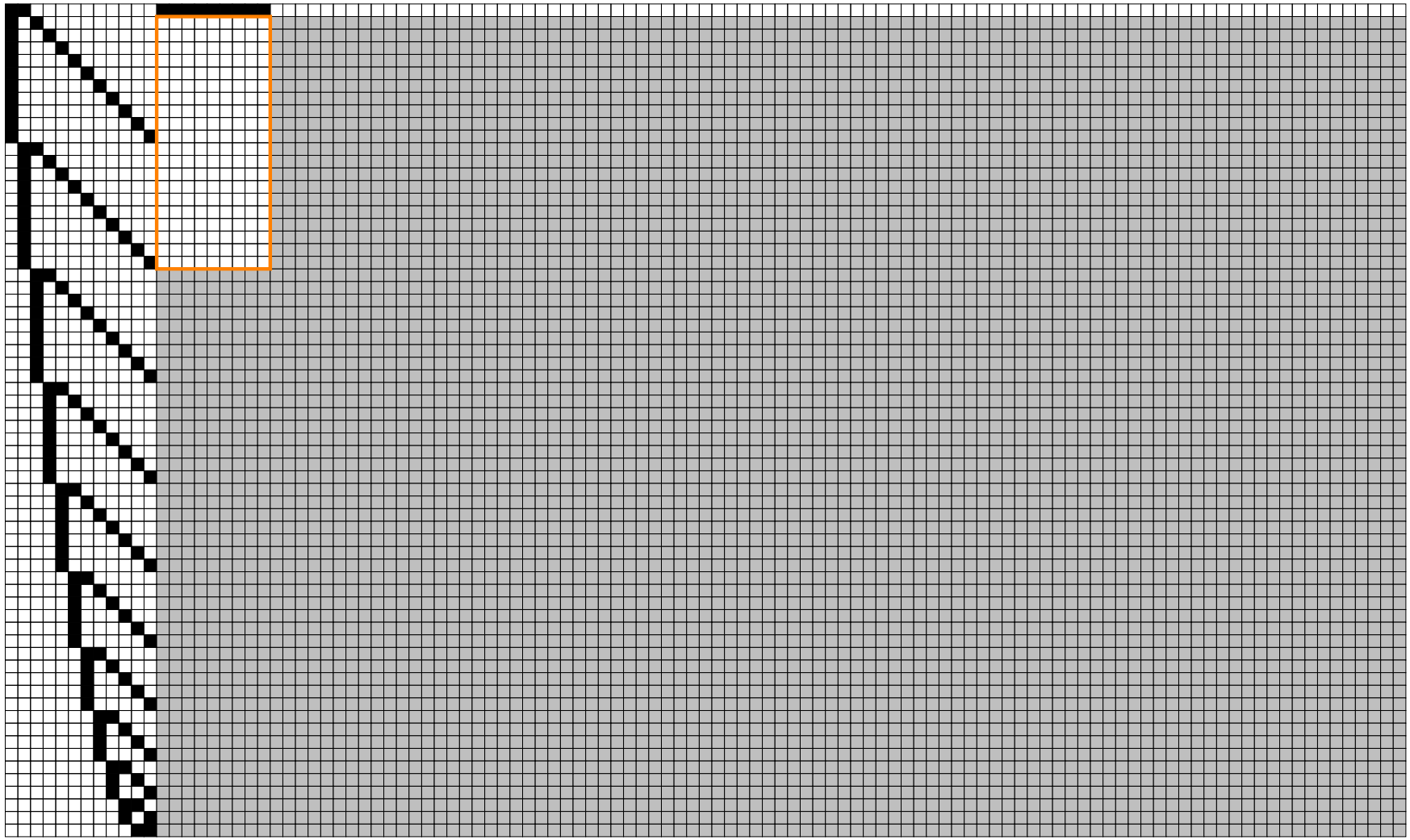
Lexicographically ordering the first 66 rows...



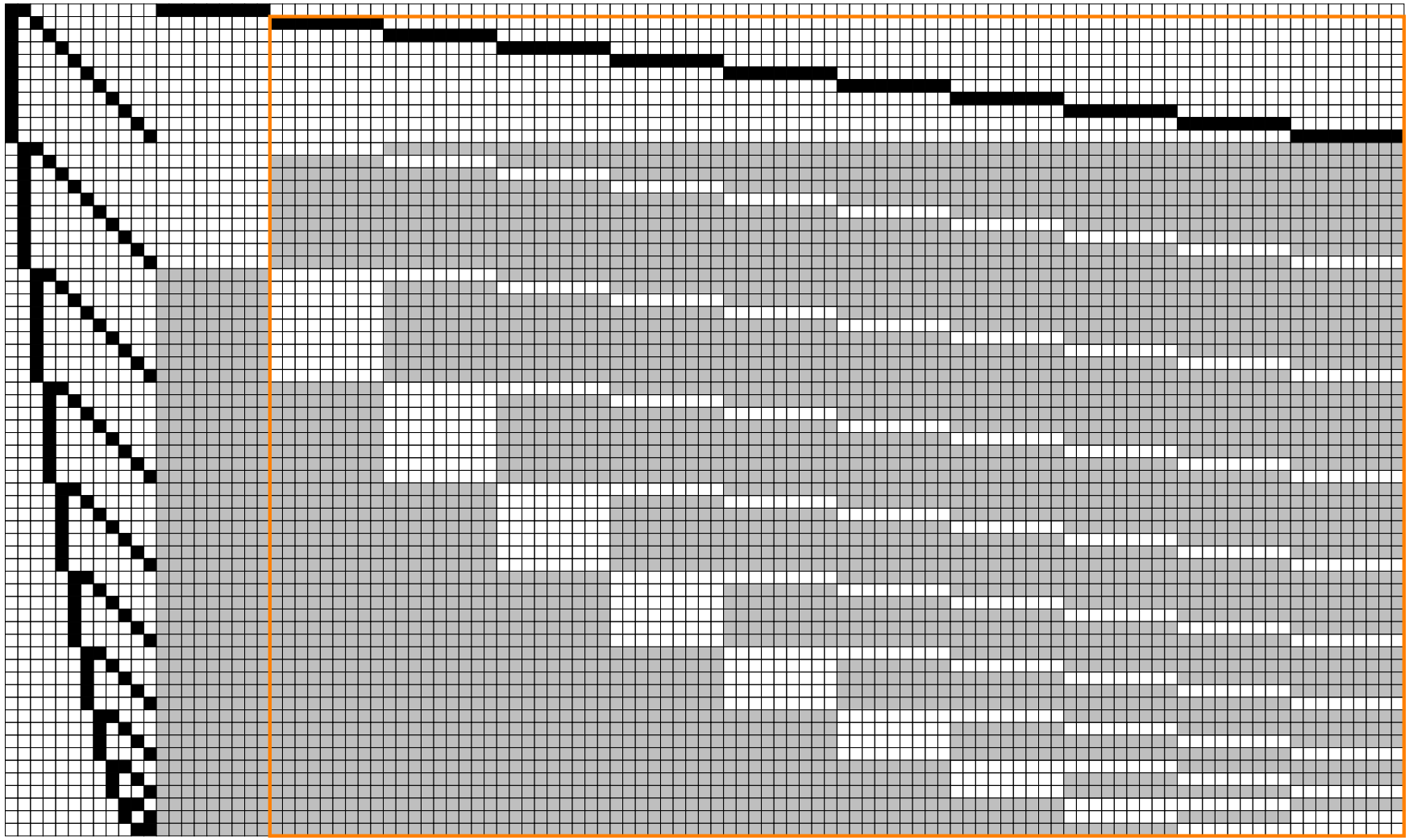
The first line must contain another nine points...



The lines 2–21 cannot intersect the first line again...



Similarly, each of the lines 2–11 contain nine more points...



SAT constraints

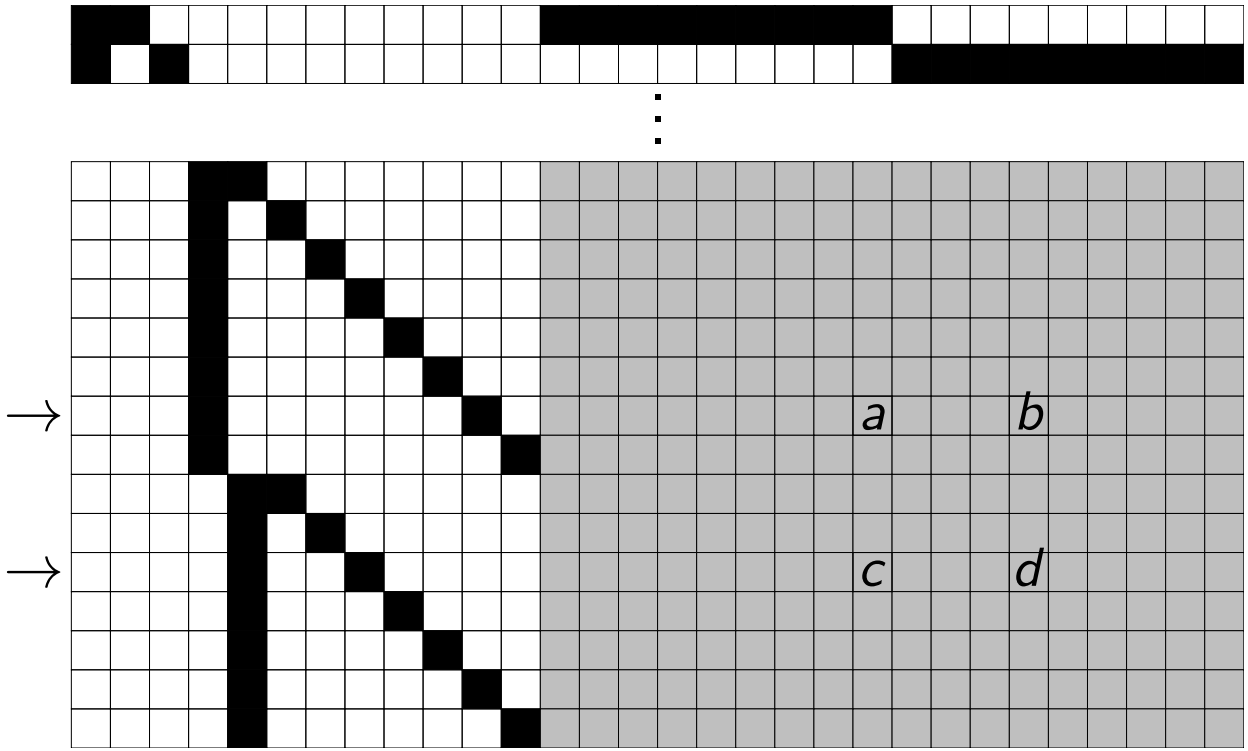
How should the projective axiom be encoded in Boolean logic?

Any two lines meet exactly once, therefore:

1. Any two lines meet *at most* once.
2. Any two lines meet *at least* once.

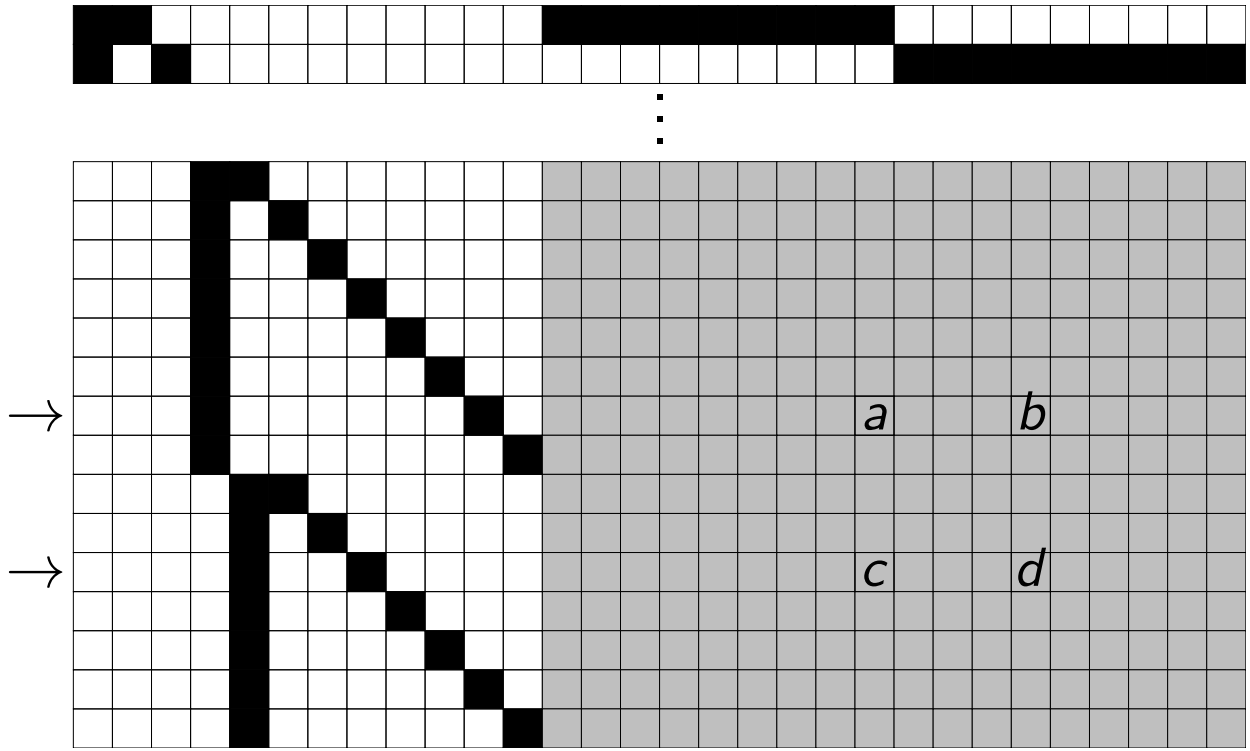
1. Lines meet at most once

In this case the entries a, b, c, d cannot all be simultaneously true:



1. Lines meet at most once

In this case the entries a, b, c, d cannot all be simultaneously true:

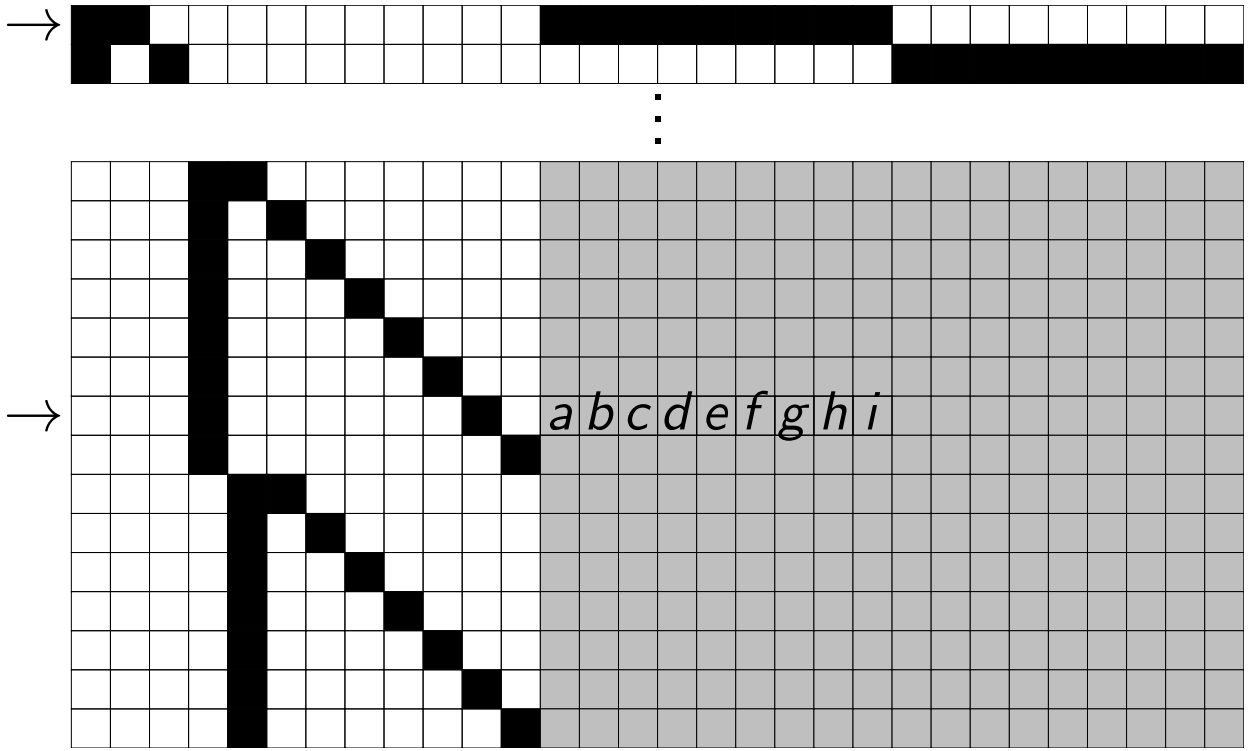


In Boolean logic:

$$\neg a \vee \neg b \vee \neg c \vee \neg d$$

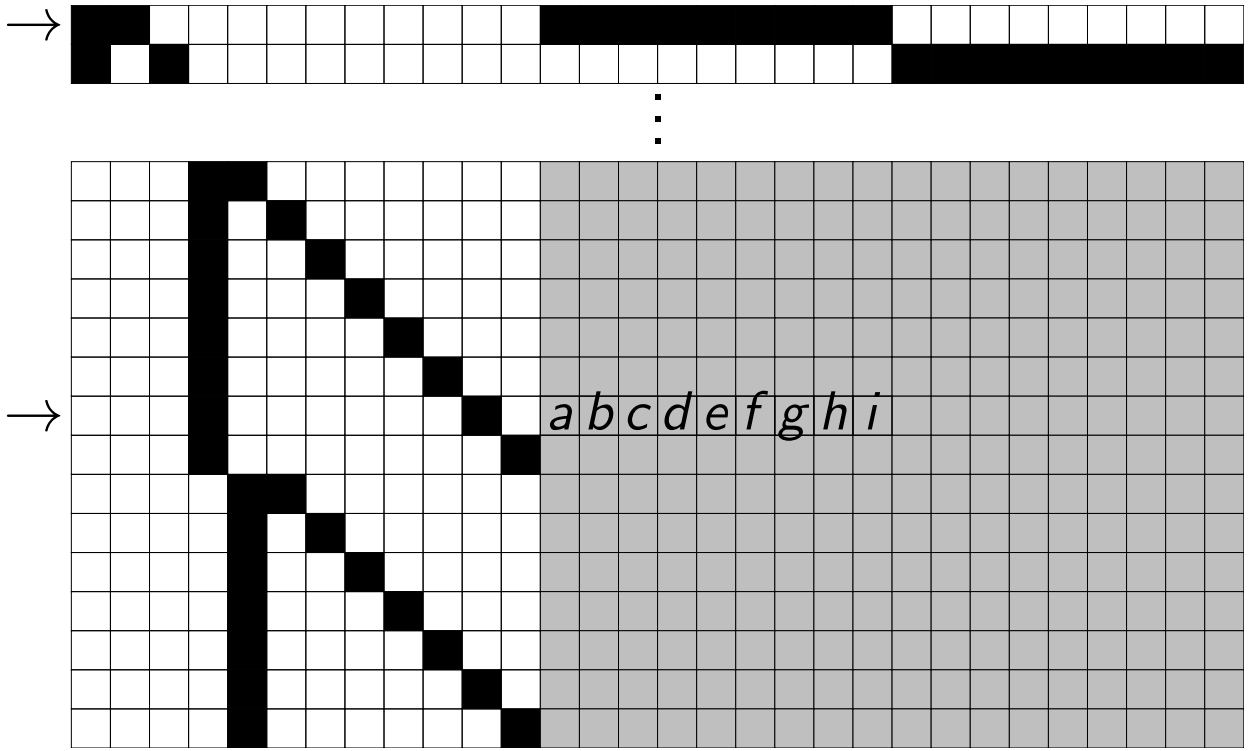
2. Lines meet at least once

In this case at least one entry *a*–*i* must be true:



2. Lines meet at least once

In this case at least one entry a–i must be true:

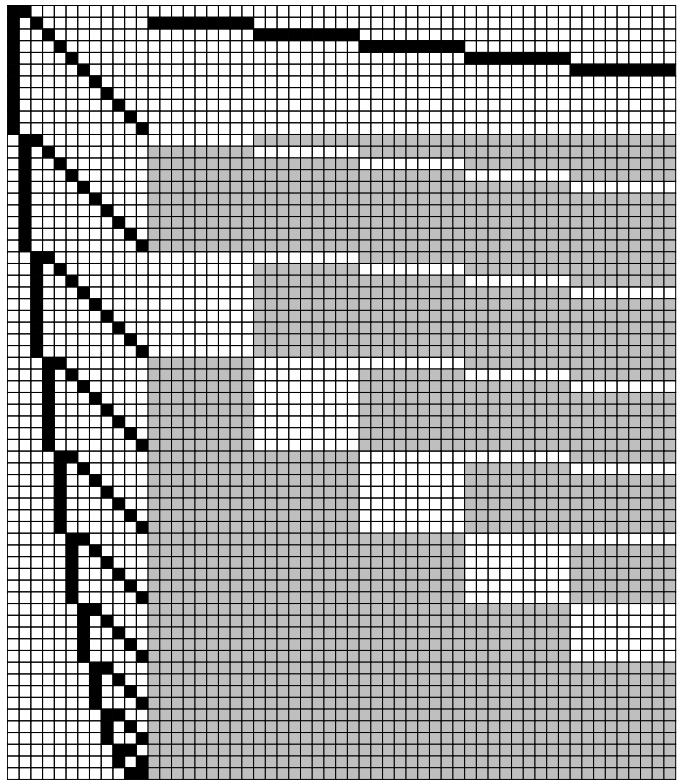


In Boolean logic:

$$a \vee b \vee c \vee d \vee e \vee f \vee h \vee i$$

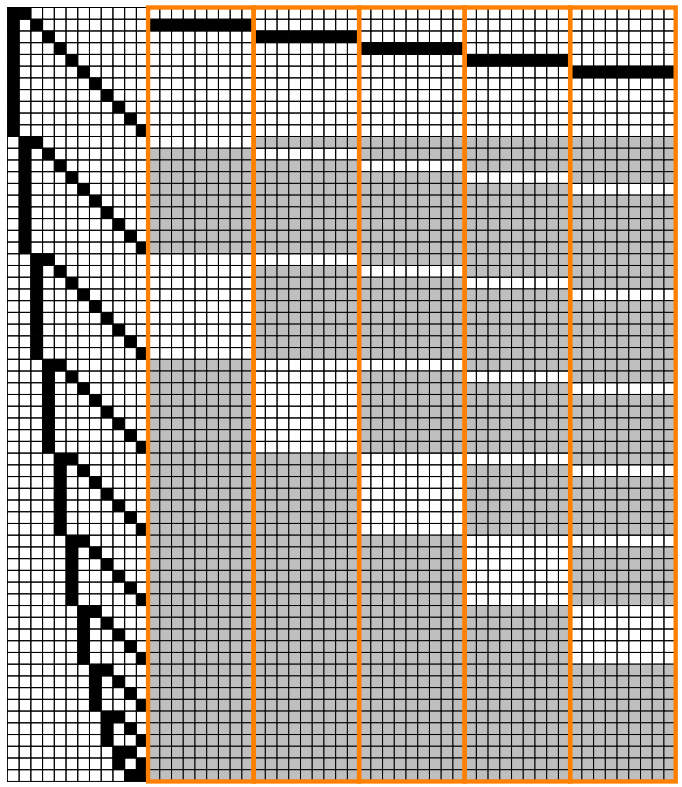
SAT instance

A SAT instance is generated using the entries in this matrix:



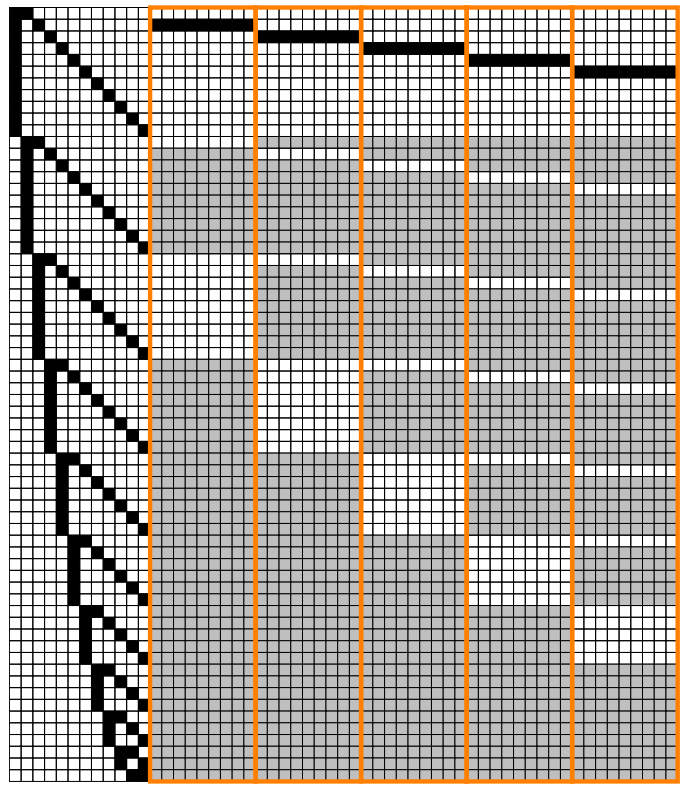
Size of the search

There are over 10^{14} possible ways of completing the entries in each of the five blocks below:



Size of the search

There are over 10^{14} possible ways of completing the entries in each of the five blocks below:



However, up to permuting the rows and columns there are only 396 ways of filling in the entries of the first block.

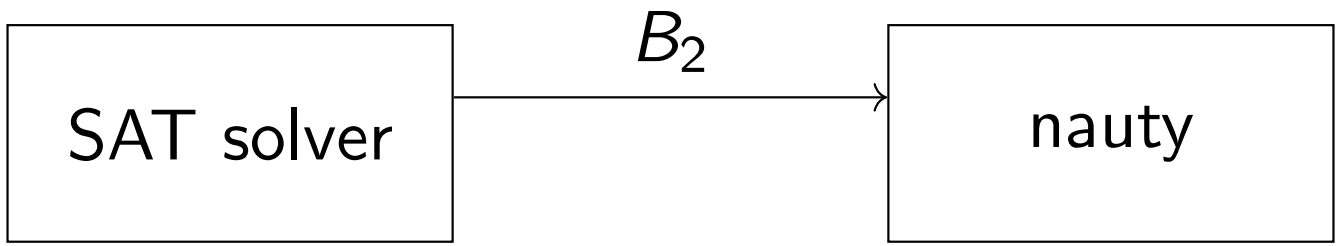
Symmetry blocking

The completions of a block are given a tag in $\{1, \ldots, 396\}$ using the symbolic computation library nauty.

Without loss of generality we suppose the first block's tag is smaller than the tags of the other blocks. We use a SAT+CAS solver that learns this on-the-fly.

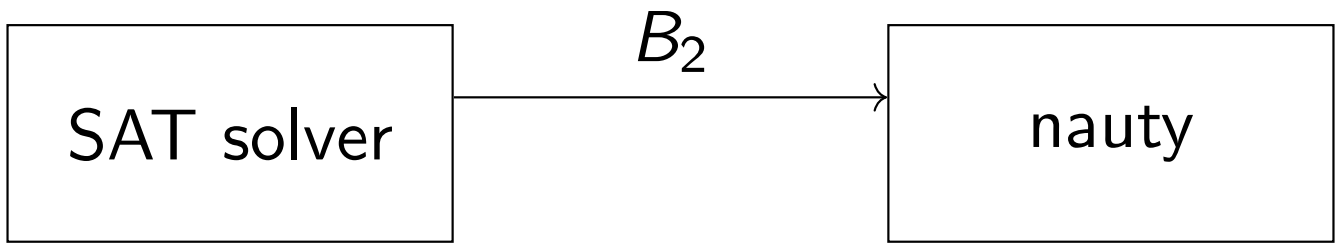
Learning method

Suppose B_2 is a completion of the second block.



Learning method

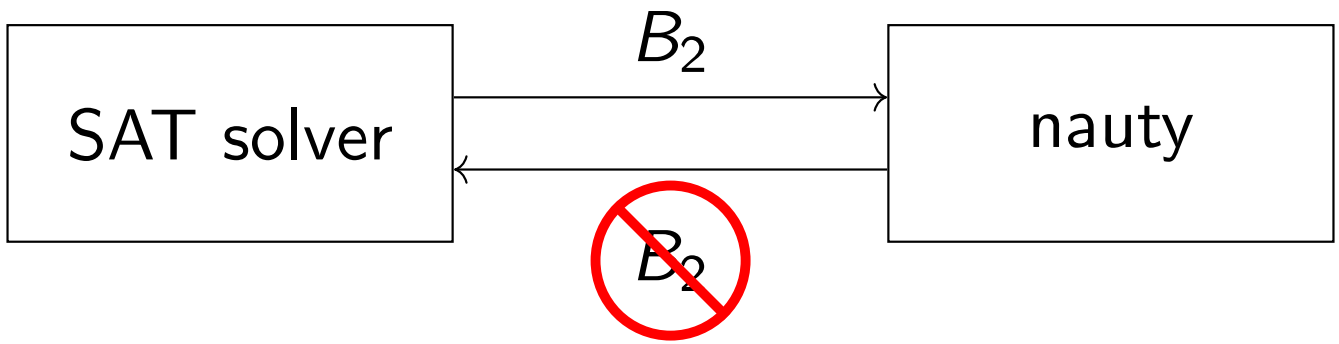
Suppose B_2 is a completion of the second block.



If the tag of B_2 is smaller than the tag of the first block...

Learning method

Suppose B_2 is a completion of the second block.

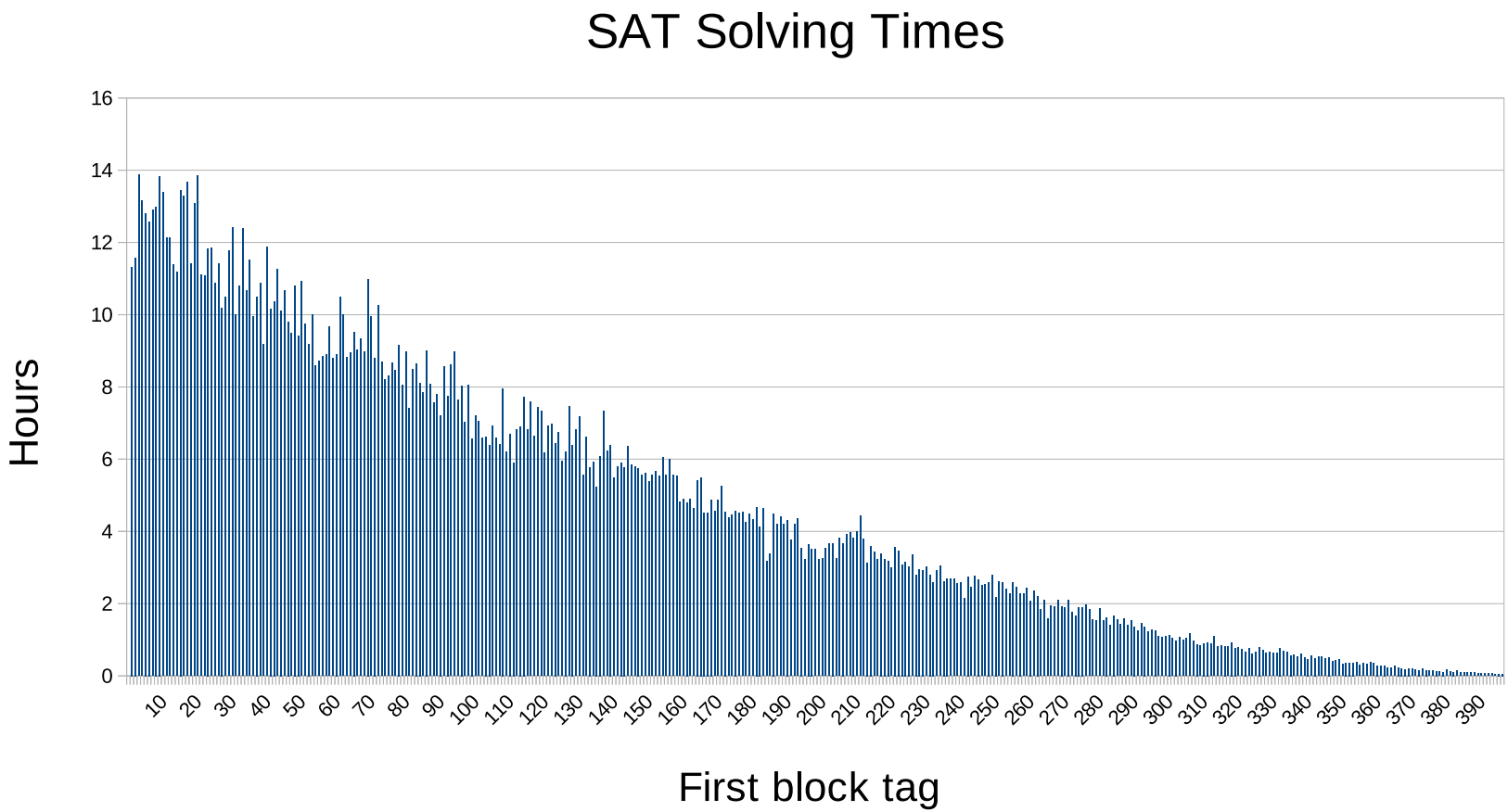


If the tag of B_2 is smaller than the tag of the first block...

...a "symmetry blocking clause" is learned.

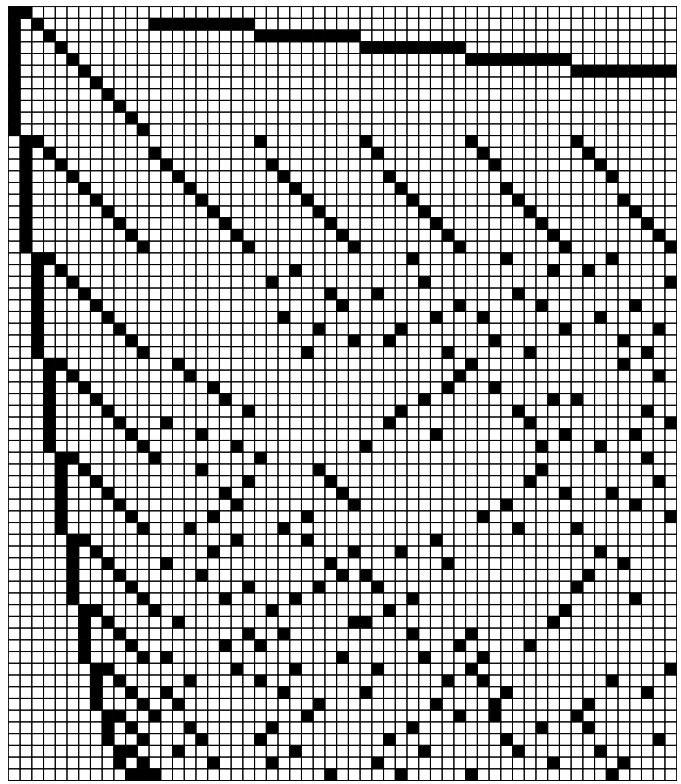
Results

As the tag of the first block increases the SAT instances become easier due to symmetry blocking...



Completions

The solver's exhaustive search found 58 five-block completions.
For example:



None of the completions can be extended to a sixth block.

Certificates

The certificates generated by the SAT solver totalled 33 TiB (and 3 TiB compressed).

To believe this nonexistence result you now need to trust:

- Our SAT encoding and script to generate the SAT instances.
- The proof verifier DRAT-trim.
- The symmetry blocking clauses (whose correctness relies on nauty).

Ongoing work

By solving several other cases we now have a complete SAT-based resolution of Lam's problem—verifying that projective planes of order ten do not exist.

For more detail on the other cases, see:

A Nonexistence Certificate for Projective Planes of Order Ten with Weight 15 Codewords. AAECC 2020.

Unsatisfiability Proofs for Weight 16 Codewords in Lam's Problem. To appear at IJCAI 2020.

Conclusion

The SAT+CAS paradigm is an effective way of searching for combinatorial objects or disproving their existence.

Conclusion

The SAT+CAS paradigm is an effective way of searching for combinatorial objects or disproving their existence.

Wide application: *Many* mathematical problems stand to benefit from fast, powerful, and verifiable search tools.

Conclusion

The SAT+CAS paradigm is an effective way of searching for combinatorial objects or disproving their existence.

Wide application: *Many* mathematical problems stand to benefit from fast, powerful, and verifiable search tools.

Bang for your buck: Requires some knowledge of SAT and CAS, but avoids using special-purpose search code.

Conclusion

The SAT+CAS paradigm is an effective way of searching for combinatorial objects or disproving their existence.

Wide application: *Many* mathematical problems stand to benefit from fast, powerful, and verifiable search tools.

Bang for your buck: Requires some knowledge of SAT and CAS, but avoids using special-purpose search code.

Thank you!

`curtisbright.com`