# A Verifiable Search for Projective Planes of Order Ten

**Curtis Bright**[1] , **Kevin Cheung**[2] , **Brett Stevens**[2] ,
**Dominique Roy**[3] , **Ilias Kotsireas**[4] and **Vijay Ganesh**[1]
[1]University of Waterloo
[2]Carleton University
[3]Canada Revenue Agency
[4]Wilfrid Laurier University

## Abstract

Using techniques from the field of satisfiability checking we verify one of the cases used in the landmark result that projective planes of order ten do not exist. In particular, we show that if such a projective plane does exist then it does not generate any codewords of weight fifteen, a result first shown in 1973 via an exhaustive computer search. We provide a simple SAT instance and a certificate of unsatisfiability that can be used to automatically verify this result for the first time. All previous demonstrations of this result have relied on search programs that are difficult or impossible to verify—in fact, our study uncovered a bug in a prior search.

## 1 Introduction

A projective plane is a generalization of the Euclidean plane where parallel lines do not exist. In other words, any two lines in a projective plane must meet at some point. The existence of non-Euclidean planes is initially counterintuitive but they have been widely studied since the beginning of the 18th century. As a simple example of this phenomenon, consider the case of geometry on a sphere. In this case the lines on a sphere are the "great circles" of the sphere and any two distinct lines intersect in exactly two antipodal points.

A more exotic type of geometry known as *finite geometry* occurs when only a finite number of points exist. In this article we are concerned with finite projective geometry, i.e., geometry that include axioms that say that only a finite number of points exist and that parallel lines do not exist. A *finite projective plane* is a model of the finite projective geometry axioms (see Section 2 for the complete list). In particular, a finite projective plane is said to be of order $n$ if there are $n+1$ points on every line.

The biggest open question in finite geometry concerns the orders $n$ for which finite planes exist. Finite planes of order $n$ can be constructed whenever $n$ is a prime power but it is unknown if any exist when $n$ is not a prime power. Despite a significant amount of effort no one has ever been able to construct a finite plane in an order $n$ that is not a prime power and it has been widely conjectured that such a plane cannot exist [Colbourn and Dinitz, 2006].

A partial result was proven by Bruck and Ryser [1949] who showed that $n$ must be the sum of two integer squares if a finite plane of order $n$ exists with $n$ congruent to 1 or 2 $(\mathrm{mod}\ 4)$. Bruck and Ryser's result implies that a projective plane of order six cannot exist. Every other $n < 10$ is a prime power and therefore a finite plane of order $n$ does exist; the smallest order that is not a prime power and not covered by the Bruck–Ryser theorem is ten.

A first step towards solving the existence question in order ten was completed by MacWilliams, Sloane, and Thompson [1973]. In this paper the error-correcting code generated by a hypothetical projective plane of order ten was studied. In particular, they showed that the search could be reduced to four cases that they called the weight 12, 15, 16, and 19 cases (see Section 2). Furthermore, they used a computer search to show that the weight 15 case did not lead to a projective plane of order ten.

In the 1980s a number of extensive computer searches were performed to settle the question of existence of a projective plane of order ten. In particular, the weight 12 case was solved by Lam, Thiel, Swiercz, and McKay [1983], the weight 16 case was solved by Lam, Thiel, and Swiercz [1986] (continuing work by Carter [1974]) and the weight 19 case was solved by Lam, Thiel, and Swiercz [1989], finally showing that a projective plane of order ten does not in fact exist.

Each of these cases required a significant amount of computational resources to solve, including about 2.7 months of computing time on a CRAY-1A supercomputer to solve the weight 19 case. More recently, Roy [2011] performed a verification of the non-existence of the projective plane of order ten and required 3.2 months of computing time using 15 CPU cores running at 2.4 GHz. The recent works [Casiello *et al.*, 2010] and [Perrott, 2016] have also performed verifications of the weight 15 case using custom-written code for the computer algebra systems GAP and Mathematica. Additionally Bruen and Fisher [1973] showed that the weight 15 case is a consequence of a result of Denniston [1969] but this was also obtained via a computer search.

In this paper we perform a verification of the weight 15 case using the properties derived by MacWilliams, Sloane, and Thompson [1973]. Our verification is unique in that we translate the properties of a projective plane into Boolean logic and then perform the search using a SAT solver. SAT solvers are known to be some of the best tools to perform

combinatorial searches; for example, Heule, Kullmann, and Marek [2017] state that today they are the "best solution" for most kinds of combinatorial searches. Even so, they mention that there are some problems that SAT solvers have not yet been successfully applied to. In fact, they explicitly list the search for a projective plane of order ten as one of these problems:

> An example where only a solution by [special purpose solvers] is known is the determination that there is no projective plane of order 10 [...] To the best of our knowledge the effort has not been replicated, and there is definitely no formal proof.

The fact that we perform our search using a SAT solver means that we can produce a formally verifiable *certificate* that the weight 15 case does not lead to a solution. In contrast to all previous searches that have been completed, one can formally verify our results without needing to trust the particular choice of hardware, compiler, or search algorithms that we happened to use in our verification. Instead, one merely needs to trust our encoding of the problem into SAT (see Section 3).

Although we do not have a machine-verifiable formal proof that our encoding is bug-free we believe that our SAT instance and resulting certificate of unsatisfiability is valuable because it reduces the amount of code that needs to be trusted. In particular, it is not necessary to trust code that implements a search algorithm. It also greatly simplifies the code that needs to be trusted—this is especially important considering that search code often needs to be written in a convoluted way to obtain optimum performance. In fact, while verifying that our SAT encoding was producing correct results we uncovered a bug in the code of a previous search (see Section 4).

Our result is also a first step towards a formal verification. The SAT encoding is deliberately chosen to be as simple as possible so that (1) the possibility of an encoding bug is less likely, and (2) it will be as simple as possible to formally generate the SAT clauses directly from the axioms that define a projective plane of order ten. This approach of reducing a problem to SAT, solving the resulting SAT instance, and then formally verifying the encoding in a theorem prover has recently successfully formally verified the Boolean Pythagorean triples conjecture [Heule *et al.*, 2016; Cruz-Filipe *et al.*, 2018].

## 2 Preliminaries

A finite projective plane of order $n$ consists of a set of lines and a set of points that satisfy the following axioms:

1. There are $n + 1$ points on every line and there are $n + 1$ lines through every point.
2. There is exactly one line between every two distinct points and every two distinct lines intersect in exactly one point.

A consequence of these axioms is that a finite projective plane of order $n$ contains exactly $n^2 + n + 1$ points and exactly $n^2 + n + 1$ lines. One way of representing a finite projective plane is by an incidence matrix that encodes the points that lie on each line. This matrix has a 1 in the $(i, j)$th entry if and only if point $j$ is on line $i$. For example, a finite projective plane of order ten is equivalent to a $111 \times 111$ matrix with entries in $\{0, 1\}$ such that:

1. Every row and column contains exactly eleven 1s.
2. The inner product of any two distinct rows or two distinct columns is exactly 1.

The ordering of the rows and columns of the incidence matrix of a projective plane is arbitrary and we say that two matrices are *isomorphic* if one matrix can be transformed into the other by a reordering of the rows and columns.

Throughout this paper we let $M$ denote the incidence matrix of a hypothetical projective plane of order ten. The elements of the row space of $M$ over the finite field $\mathbb{F}_2$ are known as the *codewords* of $M$ and the number of 1s in a codeword is known as the *weight* of the codeword. Let $w_k$ denote the number of codewords of $M$ of weight $k$. For example, $w_0 = 1$ because the zero vector is in the row space of $M$ and no other codeword has a weight of zero. Also, it was shown by Assmus and Mattson [1970] that the values of all $w_k$ can be determined from just the values of $w_{12}$, $w_{15}$, and $w_{16}$.

The relationships between the values of $w_k$ are what ultimately lead to the contradiction that showed that a projective plane of order ten cannot exist. In particular, $w_{12} = w_{15} = w_{16} = 0$ imply that $w_{19} = 24{,}675$. But a number of exhaustive computer searches [MacWilliams *et al.*, 1973; Carter, 1974; Lam *et al.*, 1983; Lam *et al.*, 1986; Lam *et al.*, 1989] have found no codewords of $M$ of weights 12, 15, 16, or 19.

In fact, it was shown by Hall [1980] that if $w_{15}$ and $w_{16}$ are zero then $w_{19}$ must be positive. Thus, to show that a projective plane of order ten does not exist it suffices to show that there exists no codewords of $M$ of weights 15, 16, or 19. In the remainder of this paper we describe the construction of a SAT instance that has a solution only if a codeword of $M$ of weight 15 exists. We then provide a certificate that this SAT instance is unsatisfiable and therefore solve one of the three cases necessary to prove the nonexistence of a projective plane of order ten.

### 2.1 Incidence matrix structure

Let $w$ be a codeword of $M$ of weight 15. We now describe the known structure of $M$ on the assumption that $w$ exists.

Let $A$ be the set of points corresponding to the 1s in $w$. MacWilliams et al. [1973] show that $M$ consists of 6 lines that contain five points of $A$, 15 lines that contain three points of $A$, and 90 lines that contain a single point of $A$. We call these lines the *heavy*, *medium*, and *light* lines, respectively. Furthermore, they show that any two heavy lines intersect at a point in $A$. Since each line contains exactly eleven points each heavy line must contain six points not in $A$; all these points are distinct (otherwise there would be heavy lines that intersect in more than one point) so there are $6 \times 6 = 36$ of them. We let $B$ be the set of these 36 points and $C$ be the remaining $111 - 15 - 36 = 60$ points.

Without loss of generality the columns of $M$ are ordered so that the points of $A$ appear first and the points of $B$ appear last. Similarly, the rows of $M$ are ordered so that the heavy lines appear first, followed by the medium lines and finally the light lines. MacWilliams et al. [1973] also determine that

each medium line contains 8 points of $C$ and each light line contains 6 points of $C$. In summary, we know that $M$ can be partitioned into a $3 \times 3$ grid of submatrices as follows:

$$\begin{array}{rrc} & & \begin{array}{ccc} A & C & B \\ 15 & 60 & 36 \end{array} \\ \begin{array}{r} \text{heavy} \\ \text{medium} \\ \text{light} \end{array} & \begin{array}{r} 6 \\ 15 \\ 90 \end{array} & \left( \begin{array}{ccc} 6 & 0 & 5 \\ 3 & 8 & 0 \\ 1 & 6 & 4 \end{array} \right) \end{array}$$

Here the numbers outside the matrix denote the number of rows or columns in that part of $M$ and the numbers inside the matrix are the number of 1s that appear in each row of the submatrix in that part of $M$.

MacWilliams et al. [1973] also show that up to isomorphism there is exactly one way of assigning the 1s in each submatrix except for the last two submatrices of the last row. Furthermore they provide an explicit representation of the unique assignment up to isomorphism. In other words, we can assume that the first 21 rows and 15 columns are explicitly given.

### 2.2 Initial entries

As mentioned in Section 2.1 we can assume that the first 21 rows and 15 columns of $M$ are fully specified. We explicitly give the instantiation of $M$ that we used in our SAT instance (up to row 43) in Figure 1. We now show that this instantiation is correct.

**Theorem 1.** *Assume that a finite projective plane of order ten generates a codeword of weight* 15*. Then the matrix given in Figure 1 can be extended into the incidence matrix of a finite projective plane of order ten.*

*Proof.* As proven by MacWilliams et al. [1973] the heavy and medium lines (the first 21 rows of $M$) have a single representation up to isomorphism. It is straightforward to check that the first 21 rows of Figure 1 do specify heavy and medium lines and do satisfy the axioms of a finite projective plane and are therefore isomorphic to the representation of MacWilliams et al. [1973]. (We applied a column permutation to their representation to more clearly explain how we assign the 1s in the later lines.)

The first 15 columns are also specified to be equivalent to the representation given by MacWilliams et al. [1973]; they choose to order the rows so that the light lines containing point 1 appear first, followed by the light lines containing points 10, 15, and 11 (in that order).

This leaves the lower-right $22 \times 96$ submatrix of Figure 1. The zeros in that appear in this submatrix are easily determined; if they were 1s the row that they are on would have more than one point of intersection with a heavy or medium line.

Next we show that the diagonal line of 1s that appears on the left of the $22 \times 96$ submatrix can be assumed without loss of generality (ignoring for now the other 1s). For example, consider the light lines through point 1 (rows 22–27). These lines must share a point of intersection with the fourth medium line (row 10). There are exactly six possibilities for this point of intersection (points 16–21). Each of the six lines 22–27 must intersect a different point (since any two lines must intersect in a exactly one point). It follows that the submatrix given by rows 22–27 and columns 16–21 is a permutation matrix and by reordering its rows we can assume without loss of generality it is the identity matrix. The lines 28–43 are handled similarly.

Finally, consider the 1s that appear in the lower-right $22 \times 36$ submatrix of $M$. For example, consider the last 6 columns. Each light line through the point 1 must intersect line 6 and by inspection we see that the intersection must be on the six points 106–111. Since there are six lines that intersect six points and each point of intersection must be distinct the submatrix given by rows 22–27 and columns 106–111 is a permutation matrix. By reordering its columns we can assume without loss of generality it is the identity matrix. The other columns 76–105 are handled similarly. □

Note that once the 1s in the lower-right submatrix of $M$ have been assigned some previously undetermined entries of $M$ can be set to 0 but for simplicity we ignore these for now.

## 3 SAT encoding

Our encoding will use the Boolean variables $p_{ij}$ where $i$ and $j$ are between 1 and 111. When $p_{ij}$ is true it represents that the $(i, j)$th entry of $M$ is 1 and when $p_{ij}$ is false it represents that the $(i, j)$th entry of $M$ is 0.

We found that only two properties were necessary to show that the initial entries of $M$ given in Section 2.2 cannot be extended into a projective plane. In particular, it was only necessary to encode the following two properties:

1. Any two lines do not intersect twice.
2. Every light line intersects every heavy and medium line.

We discuss our encoding of these properties in Sections 3.1 and 3.2. Additionally, it was only necessary to consider the lines up to row 43 and it was not possible to decrease this number. In other words, we were able to fill in the missing entries of the first 42 rows of Figure 1 to form a partial projective plane (see Figure 2).

### 3.1 Any two lines do not intersect twice

Consider lines $i$ and $j$ for arbitrary $1 \leq i, j \leq 43$ with $i \neq j$. To enforce that these lines do not intersect twice we must enforce that there do not exist points $k$ and $l$ (where $1 \leq k, l \leq 111$ and $k \neq l$) such that

$$M_{i,k} = M_{i,l} = M_{j,k} = M_{j,l} = 1.$$

As clauses in conjunctive normal form we encode this as

$$\bigwedge_{i<j} \bigwedge_{k<l} (\neg p_{i,k} \vee \neg p_{i,l} \vee \neg p_{j,k} \vee \neg p_{j,l}).$$

### 3.2 Light line intersections

Consider the intersection of line $i$ where $1 \leq i \leq 21$ (a heavy or medium line) with line $j$ where $22 \leq j \leq 43$ (a light line). The axioms of a projective plane specify that line $i$ and line $j$ must intersect at some point. In certain cases (e.g., $i = 1$ and $j = 22$) this happens in the first 15 columns of $M$ that are already known so those cases can be ignored.

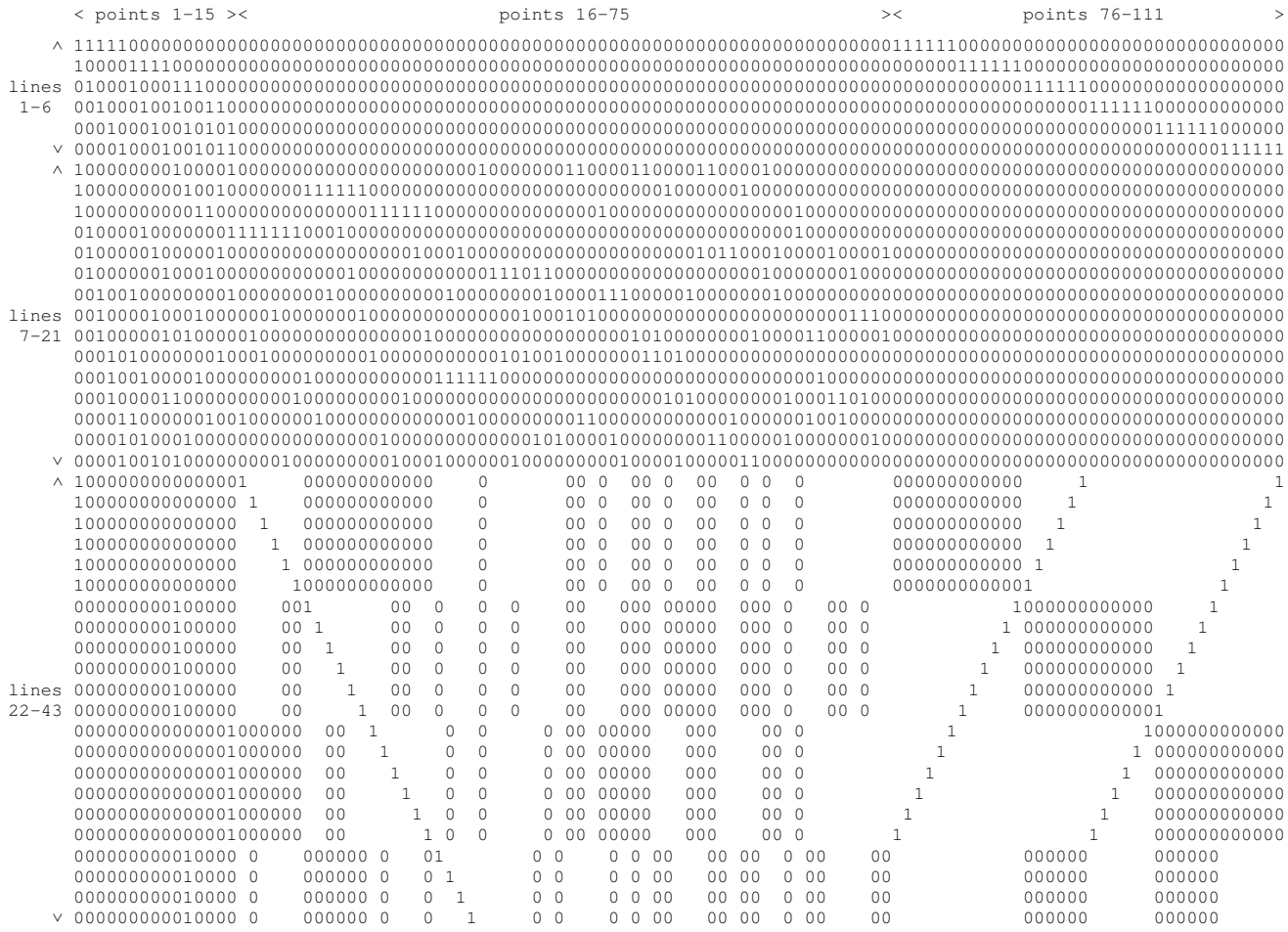


Figure 1: Our initial instantiation of the first 43 rows of $M$ where blank spaces represent unknown entries.

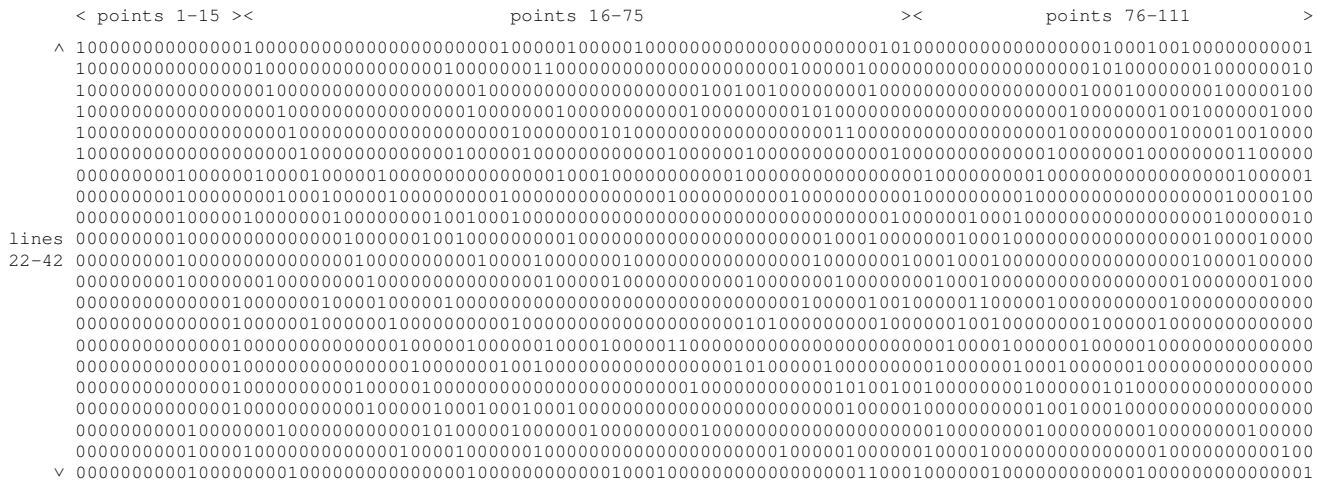


Figure 2: An assignment to rows 22–42 of $M$ that produces a partial projective plane of order ten containing 42 rows.

By an examination of Figure 1 we see that in each of the remaining cases there are exactly six possible points $k$ with $16 \leq k \leq 111$ where this could happen. In other words, the set

$$S(i,j) \coloneqq \{\, k : M_{i,k} = 1 \text{ and } M_{j,k} \text{ not initialized to } 0 \,\}$$

has exactly six elements. Then the conjunctive normal form clause

$$\bigvee_{k \in S(i,j)} p_{j,k}$$

specifies that line $i$ and $j$ intersect.

### 3.3 Optional clauses

Although not strictly necessary there are some additional clauses that can be used to improve the performance of the SAT solver. In particular, we describe clauses that encode the property that says that for any two points there must be some line that they both lie on. Since we only are using the first $43$ rows of $M$ we only encode the cases where we can show this line is one of the first $43$.

For example, consider point $1$ and point $k$ with $16 \leq k \leq 111$. In certain cases both of these points lie on a line in the known part of $M$ so we can ignore these cases. In particular, $M_{22,k}$ is initialized to zero exactly when there is a line in the first $21$ rows that point $1$ and $k$ are both on.

If $M_{22,k}$ is not initialized to $0$ there is no line in the first $21$ rows that point $1$ and $k$ are both on and an examination of $M$ shows that the only remaining lines that could contain both points $1$ and $k$ are the lines $22$–$27$. Thus, we can include the clauses

$$\bigvee_{22 \leq j \leq 27} p_{j,k}$$

where $16 \leq k \leq 111$ is any index such that $M_{22,k}$ is not initialized to $0$. Similar reasoning can be applied to point $10$ (with lines $28$–$33$) and point $15$ (with lines $34$–$39$) as well. Note that this reasoning does *not* work with point $11$ (with lines $40$–$45$) unless you extend $M$ to row $45$.

## 4 Implementation and results

A Python script[1] of about 100 lines was written to generate a SAT instance containing the clauses described in Section 3. After preprocessing the instance contains 844 variables and 24,127 clauses and could be solved in around 9 minutes using MapleSAT [Liang *et al.*, 2018] on a single core running at 2.7GHz. A DRUP certificate of unsatisfiability was also produced. The certificate is approximately 2.5 gigabytes in size and will be made available on an open data repository so that it may be publicly verified. Without the optional clauses described in Section 3.3 the SAT instance generated required a running time of about 25% longer to solve.

Also note that the SAT instance generated using the first $42$ rows of $M$ was found to be satisfiable after 8 seconds of computation time (see Figure 2). The satisfying assignment was then manually verified to satisfy the axioms of a partial projective plane (i.e., every row has exactly eleven $1$s and every two distinct rows have exactly a single $1$ in common).

[1] Available at https://pastebin.com/ZmEysihg.

Note that this contradicts the search of Casiello, Indaco, and Nagy [2010]. They provided some GAP code that searched for ways to fill in $M$ up to the $39$th row and $75$th column and found no solutions. A closer examination of their code revealed incorrect indices were used in a block compatibility check. With the correct indices their program does produce correct results though given the complexity of the program we are still not entirely sure it is bug-free.

We also cannot be 100% sure our code is bug-free. However, our code is much less complex than any previous code available that solves this problem because we only need to generate some simple SAT constraints as described in Section 3. Furthermore, the certificate of unsatisfiability that we produce can be checked in a formally verified proof checker [Lammich, 2017]. We also wrote a program to generate and solve the SAT clauses using the Logic package of the computer algebra system Maple. The same results were derived, further increasing the confidence in our result.

We also tried various methods of symmetry breaking; for example, by using clauses that lexicographically order the light lines or clauses that lexicographically order the columns $76$–$81$, $82$–$87$, etc. The symmetry breaking described in Theorem 1 was experimentally found to give the best performance for the SAT solver. Our initial SAT instances using lexicographic constraints (instead of preassigning $1$s in the lower-right $22 \times 96$ submatrix of Figure 1) required several hours to solve.

## 5 Related work

As recounted in the introduction SAT solvers have been used to perform searches in many different combinatorial problems. Some of the first successes were computing van der Waerden numbers by Kouril and Paul [2008] and Ahmed, Kullmann, and Snevily [2014], computing Green–Tao numbers by Kullmann [2010], as well as solving a special case of the Erdős discrepancy conjecture by Konev and Lisitsa [2015]. Other more recent combinatorial applications include proving the Boolean Pythagorean triples conjecture [Heule *et al.*, 2016] and a new case of the Ruskey–Savage conjecture [Zulkoski *et al.*, 2017], as well as computing Ramsey numbers [Codish *et al.*, 2016], Williamson matrices [Bright *et al.*, 2018a], complex Golay sequences [Bright *et al.*, 2018b], and Schur numbers [Heule, 2018].

We are not aware of any previous work searching for projective planes using SAT solvers. However, there has been work formalizing the axioms of projective planes in the theorem prover Coq by Magaud, Narboux, and Schreck [2008] and Braun, Magaud, and Schreck [2018].

## 6 Conclusion

In this paper we have performed a verification of one of the first nonexistence results that was crucial in the renowned proof that a projective plane of order ten does not exist. In particular, we showed that a projective plane of order ten does not generate codewords of weight fifteen. There have been a number of exhaustive searches for such a codeword but all previous searches are difficult to verify.

In particular, the works [Denniston, 1969; MacWilliams *et al.*, 1973; Roy, 2011] provide no source code. The paper [Casiello *et al.*, 2010] provides source code but as described in Section 4 their code has a bug that caused them to assert the nonexistence of a partial projective plane that we found actually exists. The paper [Perrott, 2016] verifies the same result that we verified in this paper but does so using about ten pages of sophisticated Mathematica code.

In contrast, we have given a simple translation of properties of a weight fifteen codeword into Boolean logic and have shown that these properties are sufficient to prove that such a codeword cannot exist. This was done by a simple Python script that generates a SAT instance that encodes the necessary properties in conjunctive normal form. Lastly, we solved the resulting SAT instance and provide a 2.5GB formally verifiable certificate that the SAT instance indeed has no solution.

Our work shows for the first time that SAT solvers can effectively be used in the search for finite projective planes—our code is some of the fastest available that can verify the weight 15 nonexistence result. We generated our SAT instance in a second and solved it in nine minutes and this time can be improved using more sophisticated SAT solving techniques. Using the cube-and-conquer method [Heule *et al.*, 2017] we finished the cubing in about two minutes using March_cu [Heule *et al.*, 2011] and finished the conquering in about five minutes using Glucose 3.0 [Audemard and Simon, 2009]. Conversely, the code of [Perrott, 2016] runs in about an hour and the corrected code of [Casiello *et al.*, 2010] runs in about seven minutes.

Although we do not provide a machine-checkable formal proof directly from the axioms of a projective plane we have performed the most rigorous verification of this nonexistence result to date. In particular, our code is much simpler than the code used in any previous approach to this problem. We were able to simplify the code by relying on a SAT solver to do the hard exhaustive search work. As a bonus this also produces a nonexistence certificate that can be formally independently verified.

## References


[Ahmed *et al.*, 2014] Tanbir Ahmed, Oliver Kullmann, and Hunter Snevily. On the van der Waerden numbers $w(2;3,t)$. *Discrete Applied Mathematics*, 174:27–51, 2014.

[Assmus and Mattson, 1970] Edward Ferdinand Assmus, Jr. and Harold Frazyer Mattson, Jr. On the possibility of a projective plane of order 10. *Algebraic Theory of Codes II, Air Force Cambridge Research Laboratories Report AFCRL-71-0013, Sylvania Electronic Systems, Needham Heights, Mass*, 1970.

[Audemard and Simon, 2009] Gilles Audemard and Laurent Simon. Predicting learnt clauses quality in modern SAT solvers. In Craig Boutilier, editor, *IJCAI-09: Proceedings of the Twenty-First International Joint Conference on Artificial Intelligence*, pages 399–404. 2009.

[Braun *et al.*, 2018] David Braun, Nicolas Magaud, and Pascal Schreck. Formalizing some "small" finite models of projective geometry in Coq. In *International Conference on Artificial Intelligence and Symbolic Computation*, pages 54–69. Springer, 2018.

[Bright *et al.*, 2018a] Curtis Bright, Ilias Kotsireas, and Vijay Ganesh. A SAT+CAS method for enumerating Williamson matrices of even order. In Sheila A. McIlraith and Kilian Q. Weinberger, editors, *Proceedings of the Thirty-Second AAAI Conference on Artificial Intelligence (AAAI-18)*, pages 6573–6580. AAAI Press, 2018.

[Bright *et al.*, 2018b] Curtis Bright, Ilias Kotsireas, Albert Heinle, and Vijay Ganesh. Enumeration of complex Golay pairs via programmatic SAT. In *Proceedings of the 2018 ACM International Symposium on Symbolic and Algebraic Computation*, ISSAC '18, pages 111–118, New York, NY, USA, 2018.

[Bruck and Ryser, 1949] Richard H Bruck and Herbert J Ryser. The nonexistence of certain finite projective planes. *Canad. J. Math*, 1(191):9, 1949.

[Bruen and Fisher, 1973] A Bruen and John Chris Fisher. Blocking sets, $k$-arcs and nets of order ten. *Advances in Mathematics*, 10(2):317–320, 1973.

[Carter, 1974] John Lawrence Carter. *On the existence of a projective plane of order ten*. University of California, Berkeley, 1974.

[Casiello *et al.*, 2010] D Casiello, L Indaco, and Gábor Péter Nagy. Sull'approccio computazionale al problema dell'esistenza di un piano proiettivo d'ordine 10. *Atti del Seminario matematico e fisico dell'Università di Modena e Reggio Emilia*, 57:69–88, 2010.

[Codish *et al.*, 2016] Michael Codish, Michael Frank, Avraham Itzhakov, and Alice Miller. Computing the Ramsey number $R(4,3,3)$ using abstraction and symmetry breaking. *Constraints*, 21(3):375–393, 2016.

[Colbourn and Dinitz, 2006] Charles J Colbourn and Jeffrey H Dinitz. *Handbook of combinatorial designs*. CRC press, 2006.

[Cruz-Filipe *et al.*, 2018] Luís Cruz-Filipe, Joao Marques-Silva, and Peter Schneider-Kamp. Formally verifying the solution to the Boolean Pythagorean triples problem. *Journal of Automated Reasoning*, Oct 2018.

[Denniston, 1969] RHF Denniston. Non-existence of a certain projective plane. *Journal of the Australian Mathematical Society*, 10(1-2):214–218, 1969.

[Hall, 1980] Marshall Hall, Jr. Configurations in a plane of order ten. In *Annals of Discrete Mathematics*, volume 6, pages 157–174. Elsevier, 1980.

[Heule *et al.*, 2011] Marijn J H Heule, Oliver Kullmann, Siert Wieringa, and Armin Biere. Cube and conquer: Guiding CDCL SAT solvers by lookaheads. In *Haifa Verification Conference*, pages 50–65. Springer, 2011.

[Heule *et al.*, 2016] Marijn JH Heule, Oliver Kullmann, and Victor W Marek. Solving and verifying the Boolean Pythagorean triples problem via cube-and-conquer. In *International Conference on Theory and Applications of Satisfiability Testing*, pages 228–245. Springer, 2016.

[Heule *et al.*, 2017] Marijn JH Heule, Oliver Kullmann, and Victor W Marek. Solving very hard problems: Cube-and-conquer, a hybrid SAT solving method. In Carles Sierra, editor, *Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence, IJCAI-17*, pages 4864–4868. 2017.

[Heule, 2018] Marijn JH Heule. Schur number five. In Sheila A. McIlraith and Kilian Q. Weinberger, editors, *Proceedings of the Thirty-Second AAAI Conference on Artificial Intelligence (AAAI-18)*, pages 6598–6606. AAAI Press, 2018.

[Konev and Lisitsa, 2015] Boris Konev and Alexei Lisitsa. Computer-aided proof of Erdős discrepancy properties. *Artificial Intelligence*, 224:103–118, 2015.

[Kouril and Paul, 2008] Michal Kouril and Jerome L Paul. The van der Waerden number $W(2, 6)$ is 1132. *Experimental Mathematics*, 17(1):53–61, 2008.

[Kullmann, 2010] Oliver Kullmann. Green-Tao numbers and SAT. In *International Conference on Theory and Applications of Satisfiability Testing*, pages 352–362. Springer, 2010.

[Lam *et al.*, 1983] Clement WH Lam, L Thiel, Stan Swiercz, and John McKay. The nonexistence of ovals in a projective plane of order 10. *Discrete Mathematics*, 45(2-3):319–321, 1983.

[Lam *et al.*, 1986] Clement WH Lam, L Thiel, and Stan Swiercz. The nonexistence of code words of weight 16 in a projective plane of order 10. *Journal of Combinatorial Theory, Series A*, 42(2):207–214, 1986.

[Lam *et al.*, 1989] Clement WH Lam, L Thiel, and Stanley Swiercz. The non-existence of finite projective planes of order 10. *Canad. J. Math*, 41(6):1117–1123, 1989.

[Lammich, 2017] Peter Lammich. Efficient verified (UN)SAT certificate checking. In *International Conference on Automated Deduction*, pages 237–254. Springer, 2017.

[Liang *et al.*, 2018] Jia Liang, Hari Govind V. K., Pascal Poupart, Krzysztof Czarnecki, and Vijay Ganesh. An empirical study of branching heuristics through the lens of global learning rate. In Jérôme Lang, editor, *Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence, IJCAI-18*, pages 5319–5323. 2018.

[MacWilliams *et al.*, 1973] Florence Jessie MacWilliams, Neil James Alexander Sloane, and John G Thompson. On the existence of a projective plane of order 10. *Journal of Combinatorial Theory, Series A*, 14(1):66–78, 1973.

[Magaud *et al.*, 2008] Nicolas Magaud, Julien Narboux, and Pascal Schreck. Formalizing projective plane geometry in Coq. In *International Workshop on Automated Deduction in Geometry*, pages 141–162. Springer, 2008.

[Perrott, 2016] Xander Perrott. Existence of projective planes. *arXiv preprint arXiv:1603.05333*, 2016.

[Roy, 2011] Dominique J Roy. Confirmation of the non-existence of a projective plane of order 10. Master's thesis, Carleton University, 2011.

[Zulkoski *et al.*, 2017] Edward Zulkoski, Curtis Bright, Albert Heinle, Ilias Kotsireas, Krzysztof Czarnecki, and Vijay Ganesh. Combining SAT solvers with computer algebra systems to verify combinatorial conjectures. *Journal of Automated Reasoning*, 58(3):313–339, 2017.