SAT Solving and Computer Algebra for Combinatorics

Curtis Bright

University of Windsor

Tutte Colloquium
Combinatorics and Optimization
University of Waterloo

April 1, 2022

SAT:

Boolean satisfiability problem

Is $(x \vee y) \wedge (\neg x \vee \neg y)$ satisfiable?

SAT:

Boolean satisfiability problem

Is $(\boxed{x} \lor \boxed{y}) \land (\boxed{\neg x} \lor \boxed{\neg y})$ satisfiable?

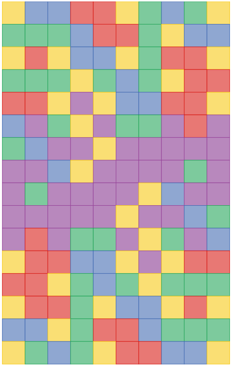
Yes $(x = \boxed{\text{T}}, y = \boxed{\text{F}})$

SAT solvers use clever trial-and-error to search for solutions

Effectiveness of SAT solvers

SAT solvers can be freakishly effective at solving problems that have nothing to do with logic.[1]

- Scheduling
- Discrete optimization
- Hardware and software verification
- Combinatorial problems like colouring the positive integers as far as possible so that a, b, and $a + b$ are never all the same colour[2]



SAT solvers also produce verifiable *certificates* when problems have no solutions.

[1] C. Bright, J. Gerhard, I. Kotsireas, V. Ganesh. Effective Problem Solving Using SAT Solvers. *Maple in Mathematics Education and Research*, 2019.

[2] M. Heule. Schur Number Five. *AAAI 2018*.

CAS:

Computer algebra system

Is 5915587277 prime?

CAS:

Computer algebra system

Is 5915587277 prime?

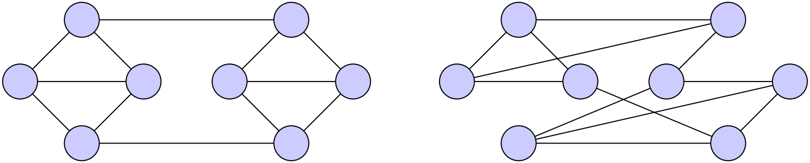
`isprime(5915587277);` $\Rightarrow$ `true`

CASs use clever algorithms to solve many mathematical problems

Effectiveness of CASs

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

- Evaluating sums, integrals, and transforms
- Finding the shortest path between two vertices in a graph
- Computing symmetries of combinatorial objects

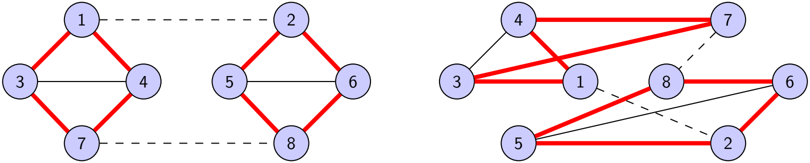


For example, are these two graphs isomorphic?

Effectiveness of CASs

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

- Evaluating sums, integrals, and transforms
- Finding the shortest path between two vertices in a graph
- Computing symmetries of combinatorial objects



Yes—and a computer algebra system can determine this.

The MathCheck system

Since 2016, I've led the development of the first SAT+CAS system *MathCheck*. It has been used at Waterloo, Toronto, Windsor, Carleton, and Wilfrid Laurier.

I will now discuss some successful applications of MathCheck from the last 2 years:

- Answering a 75-year-old open problem about the existence of Williamson matrices and disproving a conjecture about perfect quaternion sequences.
- Providing the first verifiable solution to the centuries-old *Lam's Problem* from finite geometry.[3]

[3] Best Paper Award in Memory of Jacques Calmet, *Applicable Algebra in Engineering, Communication and Computing*, 2021.

Application I: Williamson Matrices

Hadamard matrices

Hadamard matrices are square matrices with ± 1 entries whose rows are mutually orthogonal.

1	1	1	1
-1	1	-1	1
-1	1	1	-1
-1	-1	1	1

In 1893, Jacques Hadamard studied these matrices. They have applications in error-correcting codes and many other areas.

Order 92 example

In 1961, scientists from NASA searched for Hadamard matrices while developing codes for communicating with spacecraft and they found the first known Hadamard matrix of order 92.[4]

[4] L. Baumert, S. Golomb, M. Hall. Discovery of an Hadamard matrix of order 92. *Bulletin of the American Mathematical Society*, 1962.

Williamson's construction

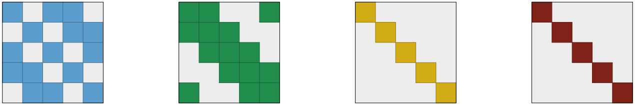
In 1944, John Williamson discovered a method of constructing Hadamard matrices in many orders like this order 8 example:

1	1	1	1	1	−1	1	−1
1	1	1	1	−1	1	−1	1
−1	−1	1	1	−1	1	1	−1
−1	−1	1	1	1	−1	−1	1
−1	1	1	−1	1	1	−1	−1
1	−1	−1	1	1	1	−1	−1
−1	1	−1	1	1	1	1	1
1	−1	1	−1	1	1	1	1

Williamson matrices

Williamson's construction relies on finding a quadruple $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \boldsymbol{D})$ of $\{\pm 1\}$-matrices for which all of the off-diagonal entries of $\boldsymbol{A}^2 + \boldsymbol{B}^2 + \boldsymbol{C}^2 + \boldsymbol{D}^2$ are zero.

The matrices are said to be *Williamson matrices* if they are symmetric and each row is a cyclic shift of the previous row; the first rows are known as *Williamson sequences*.



Williamson matrices of order 5.

The Williamson conjecture

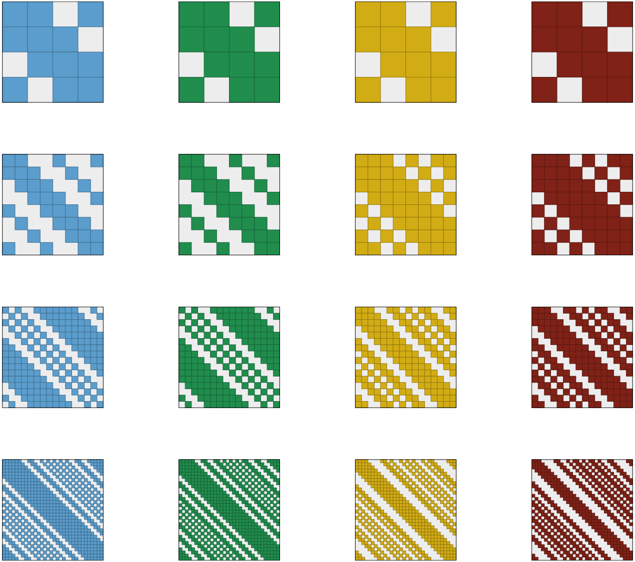
Researchers in the field expected Williamson matrices to exist in all orders[5] and this became known as the *Williamson conjecture*.

Williamson found examples in orders $n = 2^k$ for $k \leq 5$ and he expressed interest in if this could be generalized:

> **It would be interesting to determine whether the results of this paper are isolated results or are particular cases of some general theorem. Unfortunately, any efforts in this direction have proved unavailing.**

[5] S. Golomb, L. Baumert. The Search for Hadamard Matrices. *American Mathematical Monthly*, 1963.

Williamson matrices of order 2^k for $2 \leq k \leq 5$



Williamson matrices of order 2^k

The question of if Williamson matrices exist in all orders 2^k was open for 75 years.

We ran exhaustive searches for Williamson matrices in all even orders $n \leq 70$. We found that Williamson matrices **do** exist for $n = 70$ and *many* Williamson matrices exist in order 64.[6]

The search results showed that Williamson's method generalizes to all orders 2^k.[7]

---

[6] C. Bright, I. Kotsireas, V. Ganesh. Applying computer algebra systems with SAT solvers to the Williamson conjecture. *Journal of Symbolic Computation*, 2020.

[7] ——. New Infinite Families of Perfect Quaternion Sequences and Williamson Sequences. *IEEE Transactions on Information Theory*, 2020.

Construction

If A, B are sequences of even length n, A is a Williamson sequence, and B is an antipalindromic nega Williamson sequence, then the perfect shuffle of

$$[A; A] \text{ and } [B; -B]$$

is a Williamson sequence of length $4n$.

The construction applies recursively to generate Williamson sequences of all orders 2^k.

It also generates perfect sequences over the quaternion group Q_8. A sequence $(a_0, \ldots, a_{n-1})$ is *perfect* if $\sum_{i=0}^{n-1} a_i a_{i+k}^* = 0$ for all $k \not\equiv 0 \pmod{n}$.

Previous searches (even orders)

In 2006, a computer algebra approach found Williamson matrices in all even orders $n \leq 22$.[8]

In 2016, a satisfiability approach found Williamson matrices in all even orders $n \leq 30$.[9]

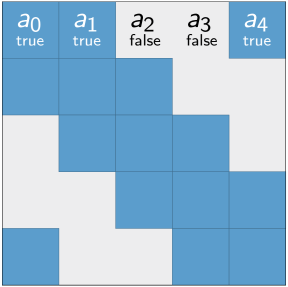
The search space for order $n = 70$ is *twenty-five orders of magnitude* larger than the search space for order $n = 30$.

[8] I. Kotsireas, C. Koukouvinos. Constructions for Hadamard matrices of Williamson type. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 2006.

[9] C. Bright, V. Ganesh, A. Heinle, I. Kotsireas, S. Nejati, K. Czarnecki. MathCheck2: A SAT+CAS verifier for combinatorial conjectures. *CASC 2016*.

SAT encoding

Let the Boolean variable a_i represent the ith entry in the initial row of the matrix $\boldsymbol{A}$ contains a 1.



Using similar variables for $\boldsymbol{B}$, $\boldsymbol{C}$, and $\boldsymbol{D}$, one can express that the off-diagonal entries of $\boldsymbol{A}^2 + \boldsymbol{B}^2 + \boldsymbol{C}^2 + \boldsymbol{D}^2$ are zero using arithmetic circuits (which can be converted into a SAT instance).

Simple setup

Encoding that Williamson
matrices of order n exist

SAT solver

Williamson matrices
or counterexample

However, this does not perform well, since a SAT solver will not exploit mathematical facts about Williamson matrices.

Power spectral density (PSD) filtering

If $\boldsymbol{A}$ is a Williamson sequence of length n then

$$\mathrm{PSD}_{\boldsymbol{A}}(k) \leq 4n$$

where $\mathrm{PSD}_{\boldsymbol{A}}(k)$ is the squared magnitude of the kth entry of the Fourier transform of $\boldsymbol{A} = [a_0, \ldots, a_{n-1}]$.

In other words, $\left|\sum_{j=0}^{n-1} a_j \omega^{kj}\right|^2 \leq 4n$ where ω is a primitive nth root of unity.

Search with PSD filtering

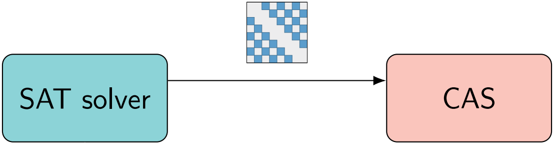
We will structure our search to efficiently

(1) compute PSD values; and
(2) block matrices with large PSD values.

CASs excel at (1) and SAT solvers excel at (2).

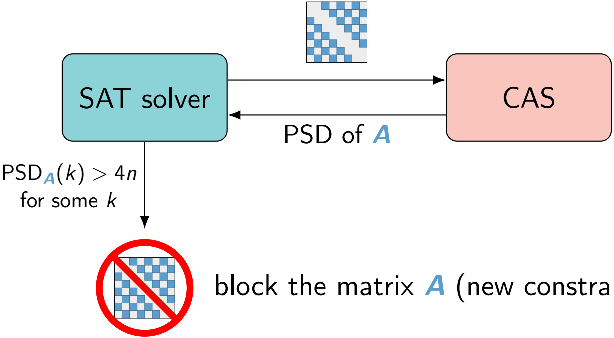
SAT+CAS learning for Williamson matrices

During the search the SAT solver will find partial solutions by finding complete definitions for $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$, or $\boldsymbol{D}$...



SAT+CAS learning for Williamson matrices

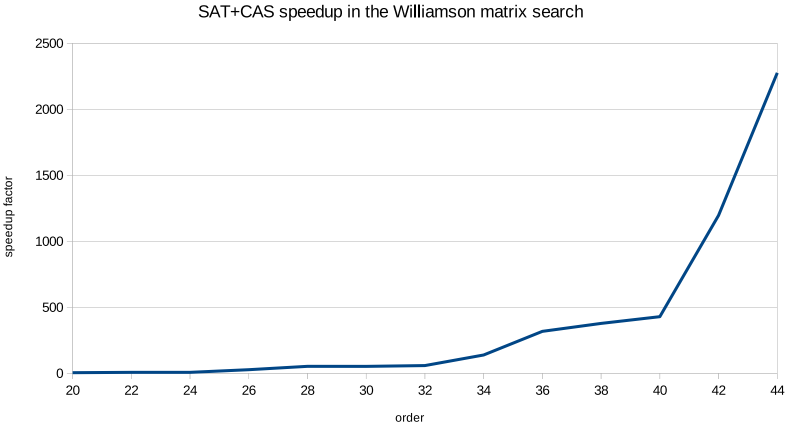
During the search the SAT solver will find partial solutions by finding complete definitions for $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$, or $\boldsymbol{D}$...



block the matrix $\boldsymbol{A}$ (new constraint)

Encoding comparison

The SAT+CAS method was significantly faster than the simple SAT encoding and the speedup improved as the order increased:



Results

MathCheck found over 100,000 new sets of Williamson matrices. Fewer than 200 had previously been found by computers.

MathCheck also proved that $n = 35$ is the minimal counterexample of the Williamson conjecture.[10]

These results lead us to propose the conjecture that Williamson matrices exist in all *even* orders n. This is still open.

[10] Computer search had previously determined the minimal odd counterexample: D. Đoković. Williamson matrices of order $4n$ for $n = 33, 35, 39$. *Discrete Mathematics*, 1993.

Application II: Lam's Problem

History

For over two thousand years, mathematicians tried to derive Euclid's "parallel postulate" from his other axioms for geometry.

History

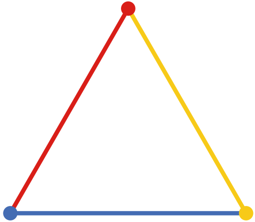
For over two thousand years, mathematicians tried to derive Euclid's "parallel postulate" from his other axioms for geometry.

The discovery of non-Euclidean geometries in the 1800s showed this is impossible!

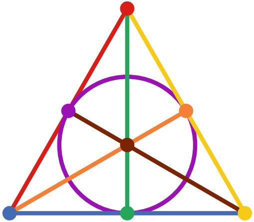
Finite projective planes

Finite projective planes satisfy the following axioms:

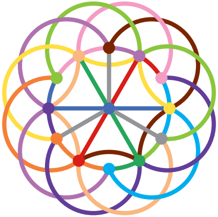
- Every pair of points define a unique line.
- Every pair of lines meet at a unique point.
- Every line contains $n+1$ points for some *order* n.



order 1



order 2



order 3

Projective planes of small orders

1	2	3	4	5	6	7	8	9	10
✓	✓	✓	✓	✓	✗	✓	✓	✓	?

Lam's problem

Somehow, this problem has a beauty that fascinates me as well as many other mathematicians.

Clement Lam

Projective planes of small orders

1	2	3	4	5	6	7	8	9	10
✓	✓	✓	✓	✓	✗	✓	✓	✓	✗

Lam's problem

Computer Science team solves centuries-old math problem

And they had to search through a thousand trillion combinations to do it

Charles Bélanger

Simply put . . .

Whew! To complete a mathematical investigation as complicated as the one recently accomplished by a team from the faculty of Engineering and Computer Science, every human being on earth would have to do 50,000 complex calculations.

The team, made up of Computer Science's Clement Lam, John McKay, Larry Thiel and Stanley Swiercz, took three years to solve a problem which had stumped mathematicians since the 1700s.

The problem: To find out whether "a finite projective plane of the order of 10" can exist.

Resolution of Lam's problem

Lam et al.[11] used custom-written software to show that a projective plane of order ten does not exist.

We must trust the searches ran to completion—the authors were upfront that mistakes were a real possibility.

MathCheck generated the first certifiable resolution of Lam's problem.[12]

[11] C. Lam, L. Thiel, S. Swiercz. The Nonexistence of Finite Projective Planes of Order 10. *Canadian Journal of Mathematics*, 1989.

[12] C. Bright, K. Cheung, B. Stevens, I. Kotsireas, V. Ganesh. A SAT-based Resolution of Lam's Problem. *AAAI 2021*.

SAT encoding

A projective plane of order n is equivalent to a quad-free $(0,1)$-matrix with $n+1$ ones in each row and column. A *quad-free* matrix contains no rectangle with 1s in the corners.

1	1	0
1	0	1
0	1	1

order 1

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

order 2

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

order 3

These constraints can be encoded in Boolean logic, but this is not sufficient to solve Lam's problem—it does not exploit the theorems that make an exhaustive search feasible.

Enter coding theory

The *code* generated by a projective plane is the row space of its incidence matrix over $GF(2) = \{0,1\}$. The *weight* of a binary word is the number of 1s it contains.

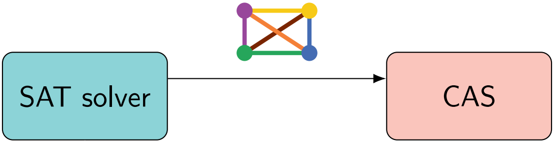
In 1970, properties about how many words of each weight must exist in the code generated by a hypothetical projective plane of order ten were derived.[13]

The code must contain words of weight 15, 16, or 19. These constraints can be reduced to SAT, but the solver still needs help...

[13] E. Assmus. The projective plane of order ten? Combinatorial Aspects of Finite Geometries, 1970.

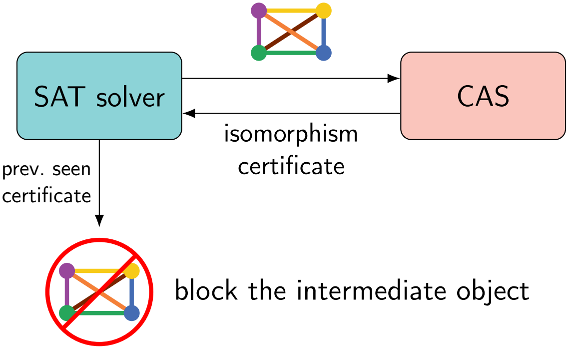
SAT+CAS learning for Lam's problem

During the search the SAT solver will find partial solutions by finding complete definitions for the first few lines of the plane. . .



SAT+CAS learning for Lam's problem

During the search the SAT solver will find partial solutions by finding complete definitions for the first few lines of the plane. . .



Results

Searches for codewords of weight 15, 16, and 19:

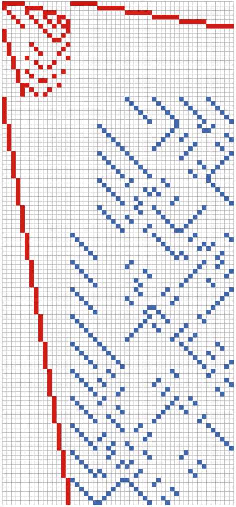
Weight	**SAT-based**	**CAS-based**	**SAT+CAS**
15	5 minutes	3–78 minutes	0.1 minutes
16	–	16,000 hours	30 hours
19	–	20,000 hours	16,000 hours

In the final case, a SAT+CAS search exhaustively generates all possibilities for the first 19 points of the plane **150 times** faster than a pure SAT approach.

Discrepancies

The lack of verifiable certificates has real consequences. We found discrepancies with the intermediate results of both Lam's search and an independent verification from 2011.[14]

On the right is a 51-column partial projective plane determined not to exist in 2011, but found by MathCheck.



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

Other MathCheck results (see uwaterloo.ca/mathcheck)

Problem	**New Result**	**CAS Functionality**
Williamson	Found smallest counterexample	Fourier transform
Even Williamson	First verification in orders $n \leq 70$	Fourier transform
Lam's Problem	First certifiable solution	Graph isomorphism
Good Matrix	Found 3 new counterexamples	Fourier transform
Best Matrix	First solution in order 57	Fourier transform
Complex Golay	Verified lengths up to 28	Nonlinear optimizer
Ruskey–Savage	First verification in order 5	Travelling salesman solver
Norine	First verification in order 6	Shortest path solver
Kochen–Specker	Improved lower bound to order 23	Graph isomorphism

SAT+CAS methods have also been used to find small circuits for matrix multiplication[15] and to verify arithmetic circuits.[16]

[15] M. Heule, M. Kauers, M. Seidl. New ways to multiply 3×3-matrices. *Journal of Symbolic Computation*, 2021.

[16] D. Kaufmann, M. Kauers, A. Biere. SAT, Computer Algebra, Multipliers. *Vampire 2019*.

Conclusion

Searches that were previously out-of-reach have become feasible due to SAT+CAS methods.

There are many problems where they have yet to be used! Perhaps even in your own research area? ⌣̈

We are hiring research assistants—for more details:

`curtisbright.com`