Computer Algebra and SAT for Mathematical Search

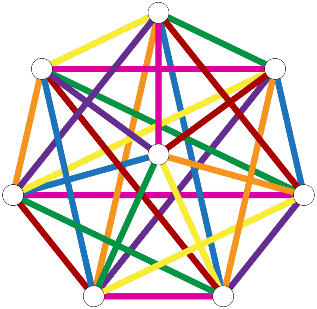
Curtis Bright
University of Windsor

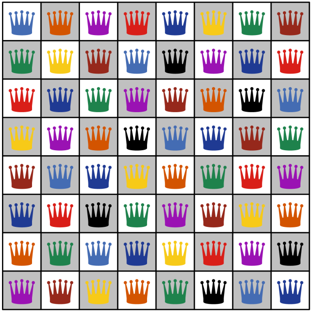
Joint work with
Kevin Cheung, Brett Stevens, Ilias Kotsireas, Vijay Ganesh

Theoretical Foundations of SAT/SMT Solving
Simons Institute
April 21, 2021

Motivation

Mathematicians have long been fascinated with searching for structures that satisfy elegant properties.

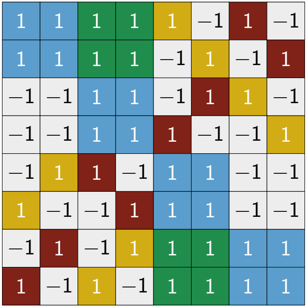




Motivation

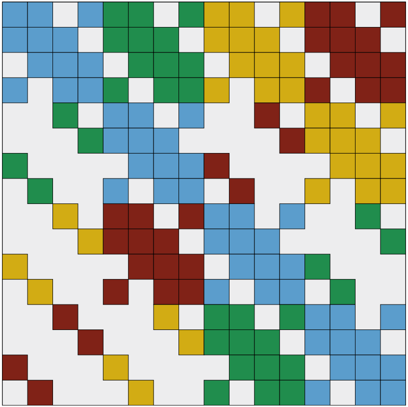
Hadamard matrices are square matrices with ±1 entries whose rows are mutually orthogonal.

In 1944, Williamson found a number of such matrices like this 8×8 example:



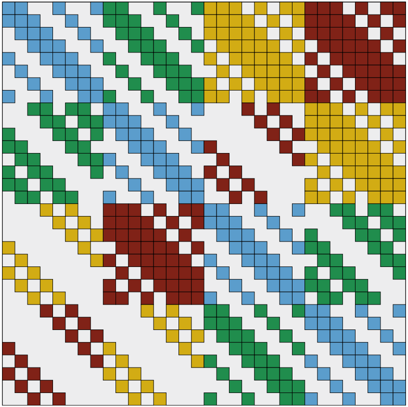
$$\begin{array}{|c|c|c|c|c|c|c|c|}
\hline
1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 \\
\hline
1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 \\
\hline
-1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 \\
\hline
-1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 \\
\hline
-1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 \\
\hline
1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 \\
\hline
-1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 \\
\hline
1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 \\
\hline
\end{array}$$

Hadamard matrix found by Williamson



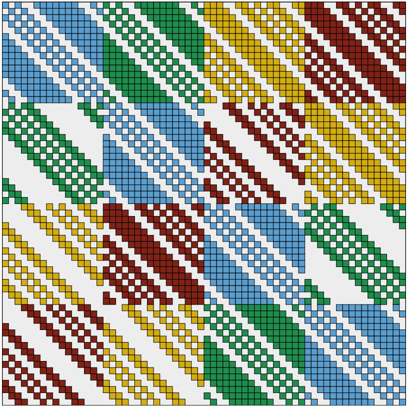
Using Williamson submatrices of order $n = 2^2 = 4$.

Hadamard matrix found by Williamson



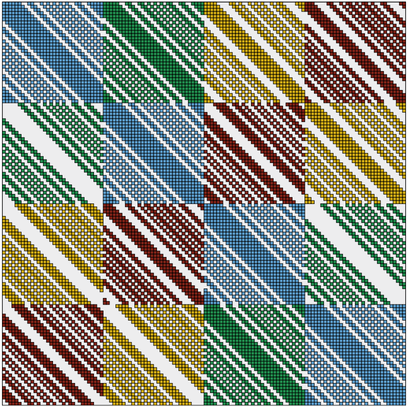
Using Williamson submatrices of order $n = 2^3 = 8$.

Hadamard matrix found by Williamson



Using Williamson submatrices of order $n = 2^4 = 16$.

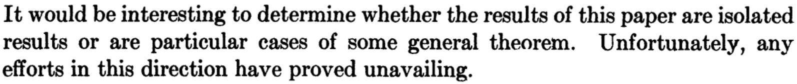
Hadamard matrix found by Williamson



Using Williamson submatrices of order $n = 2^5 = 32$.

Does this continue?

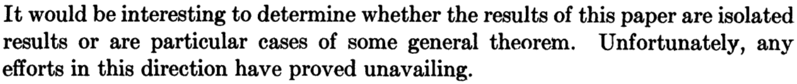
It’s unclear if this pattern extends to orders $n = 2^k$ for $k > 5 \ldots$



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.

Does this continue?

It's unclear if this pattern extends to orders $n = 2^k$ for $k > 5\ldots$



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.

It does!

In 2019, we found all Williamson matrices in even orders $n \leq 70$.[1] The patterns uncovered by these searches show that Williamson's method works for **all** orders that are powers of two.[2]

[1] C. Bright, I. Kotsireas, V. Ganesh. Applying computer algebra systems with SAT solvers to the Williamson conjecture. *Journal of Symbolic Computation*, 2019.

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

Moral of the story

Sometimes the only feasible way of discovering "large" examples of mathematical structures is through computational search.

Previous search methods for Williamson matrices came from fields such as *satisfiability solving* and *computer algebra*.

Previous searches

In 2006, a computer algebra approach found Williamson matrices up to order $n \leq 22$.

In 2016, a satisfiability approach found Williamson matrices up to order $n \leq 30$.

The search space for order $n = 70$ is twenty-five orders of magnitude larger than the search space for order $n = 30$—yet it is possible to search *exhaustively* with a approach.

SAT:

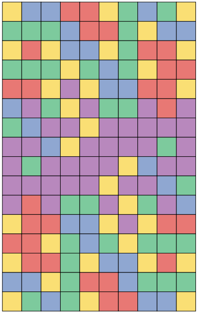
Boolean satisfiability problem

SAT solvers use clever trial-and-error to find solutions

Effectiveness of SAT solvers

SAT solvers are incredibly effective at solving some kinds of search problems that have nothing to do with logic.

- Discrete optimization
- Hardware and software verification
- Solving math problems like colouring as many integers as possible so that *a*, *b*, and $a + b$ are never the same colour[3]



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

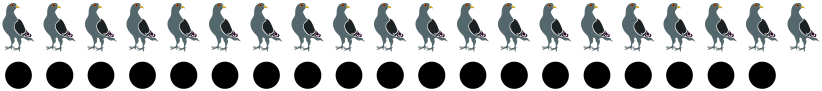
[3] M. J. H. Heule. Schur Number Five. *AAAI 2018*.

Limitations of SAT solvers

SAT solvers lack mathematical understanding beyond the most basic logical inferences and will fail on some trivial tiny problems.

Example

Have a SAT solver try to find a way to put 20 pigeons into 19 holes such that no hole contains more than one pigeon…



CAS:

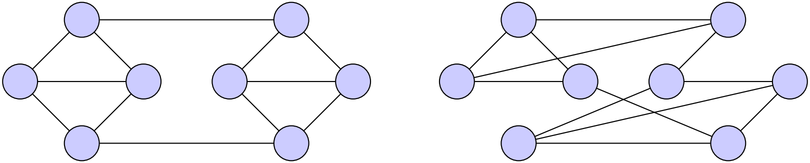
Computer algebra system

“Executing” mathematics on a computer

Effectiveness of CASs

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

- Row reducing a matrix
- Evaluating sums, integrals, and transforms
- Computing symmetries of combinatorial objects

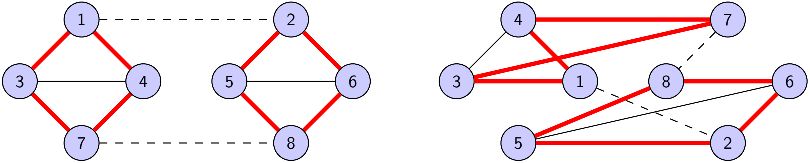


For example, are these two graphs isomorphic?

Effectiveness of CASs

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

- Row reducing a matrix
- Evaluating sums, integrals, and transforms
- Computing symmetries of combinatorial objects



Yes—and a computer algebra system can determine this.

Limitations

CASs are not optimized to do large searches (in an exponential-sized space).

SAT + CAS

Search + Math

The SC^2 project

In November 2015, researchers from both satisfiability checking and symbolic computation (SC^2) came together for the first time in a seminar in Dagstuhl, Germany. . .

This led to the creation of the SC-square project which now has associates from over 40 universities and 15 companies.

MathCheck: The first SAT+CAS system

In 2015, I started developing MathCheck and applied it to various mathematical conjectures.

Over 100,000 new Hadamard matrices were found (one shown on the right).

MathCheck has since won several awards such as a €4,000 prize for the best paper to appear in *Applicable Algebra in Engineering, Communication and Computing* in the year of 2020.[4]

[4] C. Bright et al. A Nonexistence Certificate for Projective Planes of Order Ten with Weight 15 Codewords. *AAECC 2020*.

MathCheck results (see uwaterloo.ca/mathcheck)

Finite Geometry:
Fastest and first certifiable solution of Lam's problem (1800s).

Combinatorics:
Found the smallest counterexample of the Williamson conjecture (1944) and the first examples of Williamson matrices in orders such as 70.
Found three new counterexamples of the good matrix conjecture (1971).
Current best result in the best matrix conjecture (2001).

Graph Theory:
Current best result in the Ruskey–Savage conjecture (1993).
Current best result in the Norin conjecture (2008).

Number Theory:
Verified a conjecture of Craigen, Holzmann, and Kharaghani (2002) on complex Golay sequences.

History of Lam's Problem

Since 300 BC, mathematicians tried to derive Euclid's "parallel postulate" from his other axioms for geometry.

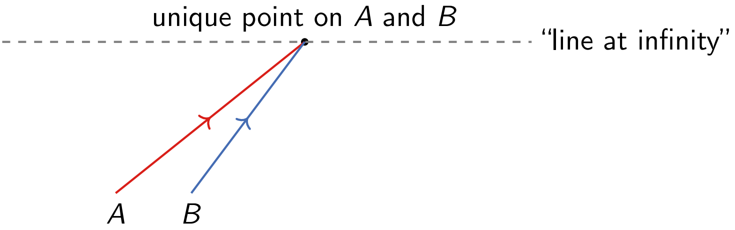
History of Lam's Problem

Since 300 BC, mathematicians tried to derive Euclid's "parallel postulate" from his other axioms for geometry.

The discovery of alternative geometries in the 1800s showed this is impossible!

Projective planes

Parallel lines do not exist in projective planes—instead, any pair of lines will meet at a unique point.

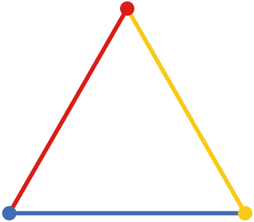


A complete classification of projective planes is still unknown (in particular in the case when there are a finite number of points).

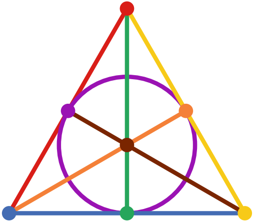
Finite projective planes

Finite projective planes satisfy the following axioms:

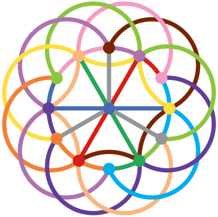
- Every pair of lines meet at a unique point.
- Every pair of points define a unique line.
- Every line contains $n + 1$ points for some *order* n.



order 1



order 2



order 3

Projective planes of small orders

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

Projective planes of small orders

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

Theoretical obstruction

Projective planes of small orders

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

No such plane known

No theoretical obstruction known

Projective planes of small orders

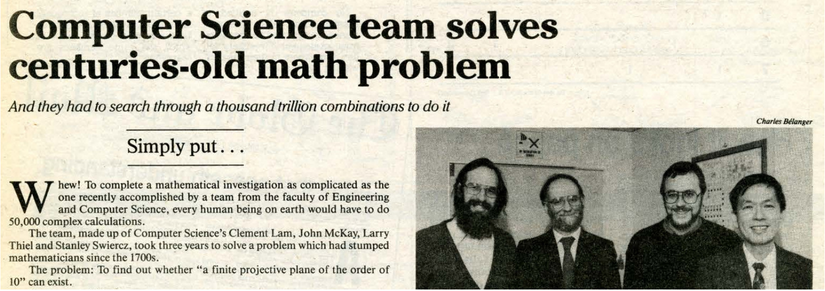
1	2	3	4	5	6	7	8	9	10
✓	✓	✓	✓	✓	✗	✓	✓	✓	?

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
✓	✓	✓	✓	✓	✗	✓	✓	✓	✗



Computer Science team solves centuries-old math problem

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

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.

Charles Bélanger

Correctness of the result

Lam's search used custom-written software run once on a single piece of hardware. We must trust the searches ran to completion.

This is a lot of trust—the authors were upfront that mistakes were a real possibility. Ever since then, mathematicians have dreamt of a proof whose correctness could be formally verified.

The first verifiable proof

We use MathCheck to generate certificates that an independent party can use to verify the solution of Lam's problem.[5]

We encode Lam's problem in SAT and solve the resulting instance using a cube-and-conquer[6] method.

This alone is not sufficient to solve Lam's problem—it does not exploit the theorems that make an exhaustive search feasible.

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

[6] M. J. H. Heule, O. Kullmann, V. W. Marek. Solving Very Hard Problems: Cube-and-Conquer, a Hybrid SAT Solving Method. *IJCAI 2017*.

Incidence matrix encoding

The *incidence matrix* of a projective plane is a $\{0, 1\}$ matrix encoding which lines (rows) contain which points (columns):

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

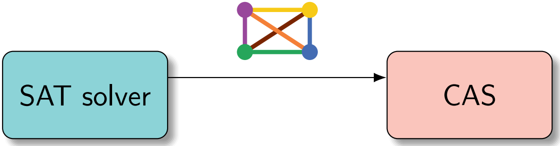
1	0	0	0	1	0	0	0	1	1	0	0	0
0	0	1	1	0	0	0	1	0	1	0	0	0
0	1	0	0	0	1	1	0	0	1	0	0	0
1	0	0	0	0	1	0	1	0	0	1	0	0
0	1	0	1	0	0	0	0	1	0	1	0	0
0	0	1	0	1	0	1	0	0	0	1	0	0
1	0	0	1	0	0	1	0	0	0	0	1	0
0	1	0	0	1	0	0	1	0	0	0	1	0
0	0	1	0	0	1	0	0	1	0	0	1	0
0	0	0	1	1	1	0	0	0	0	0	0	1
0	0	0	0	0	0	1	1	1	0	0	0	1
1	1	1	0	0	0	0	0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

order 3

SAT encoding: use a Boolean variable for every entry in the matrix, with false representing 0 and true representing 1.

SAT+CAS learning method

The SAT solver finds partial solutions and sends them to a CAS. . .

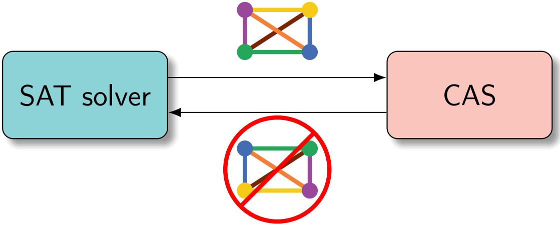


SAT solver

CAS

SAT+CAS learning method

The SAT solver finds partial solutions and sends them to a CAS. . .



. . . and the CAS finds a nontrival isomorphism and blocks it.

Results

The structure of the incidence matrix can be split into three main cases. Each case produced unsatisfiable instances and we generated nonexistence certificates for each:

Case	Compute time	Certificate size	Appearing
1	7 seconds	35 MiB	AAECC 2020
2	30 hours	325 GiB	IJCAI 2020
3	24 months	110 TiB	AAAI 2021

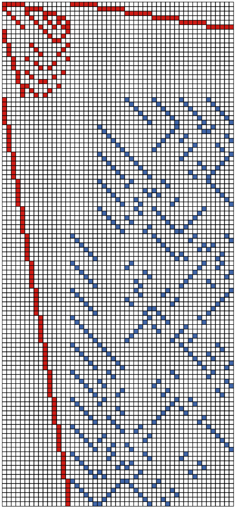
For case 1, a SAT-only cube-and-conquer approach used 5 minutes and previous CAS-only approaches used between 3 and 55 minutes.

The previous verification of case 2 required 16,000 hours.

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.

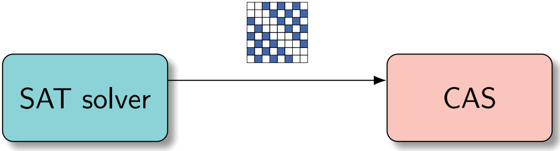
On the right is a 51-point partial projective plane of order ten asserted to not exist in 2011—but discovered by MathCheck.



SAT+CAS learning: Williamson matrices

The submatrices in Williamson's construction define sequences whose Fourier transforms have entries of small magnitude.

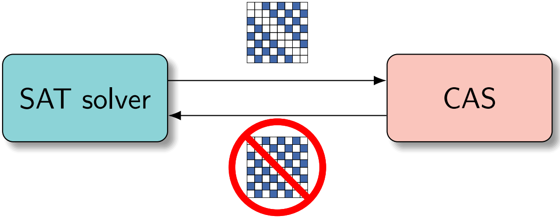
The CAS computes the largest magnitude in the discrete Fourier transform of the first row of a submatrix. . .



SAT+CAS learning: Williamson matrices

The submatrices in Williamson's construction define sequences whose Fourier transforms have entries of small magnitude.

The CAS computes the largest magnitude in the discrete Fourier transform of the first row of a submatrix. . .



. . . if it is too large, the submatrix is blocked.

Conclusion

Many mathematical problems stand to benefit from fast, verifiable, and expressive search tools.

Don't reinvent the wheel!

- It's hard to beat a SAT solver at search.
- It's hard to beat CASs for mathematical computations.

The SAT+CAS method overcomes the lack of expressiveness that results from using a SAT solver.

Future work

SAT+CAS methods are poised to forever change what is considered feasible in mathematical search.

I'm looking for students to extend and apply this paradigm to new applications. See my website for research position postings:

`curtisbright.com`

Upcoming: I'm co-chairing the sixth SC-square workshop taking place virtually on August 19–20, 2021. Participants from diverse backgrounds are explicitly encouraged to attend.