SAT Solving with Computer Algebra: A Powerful Combinatorial Search Method

Curtis Bright
University of Waterloo

UBC Discrete Mathematics Seminar
September 10, 2019

SAT:

Boolean satisfiability problem

SAT:

Boolean satisfiability problem

SAT solvers: Clever brute force

Effectiveness of SAT solvers

Many problems that have nothing to do with logic can be effectively solved by reducing them to Boolean logic and using a SAT solver.

Effectiveness of SAT solvers

Many problems that have nothing to do with logic can be effectively solved by reducing them to Boolean logic and using a SAT solver.

Examples

- Hardware and software verification
- Scheduling subject to constraints
- Finding or disproving the existence of combinatorial objects

Limitations of SAT solvers

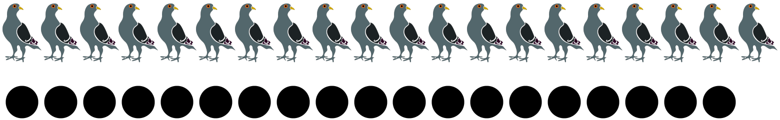
SAT solvers lack mathematical understanding beyond the most basic logical inferences and will fail on some trivial tiny problems.

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 to 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

CAS:

Computer algebra system

Symbolic mathematical computing

Effectiveness of CAS

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

Effectiveness of CAS

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

Example

What is the value of

$$\sum_{n=1}^{\infty} \frac{1}{n^2}\,?$$

Effectiveness of CAS

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

Example

What is the value of

$$\sum_{n=1}^{\infty} \frac{1}{n^2}\,?$$

Maple returns $\pi^2/6$.

Effectiveness of CAS

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

Example

What is the value of

$$\sum_{n=1}^{\infty} \frac{1}{n^2}\,?$$

Maple returns $\pi^2/6$ . . . *not* 1.64493406685.

Limitations

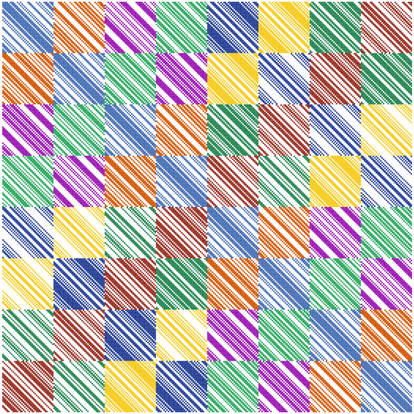
CASs are not optimized to do large (i.e., exponential) searches.

SAT + CAS

Brute force + Knowledge

MathCheck

Our SAT+CAS system MathCheck has constructed over 100,000 various combinatorial objects. For example, this $\{\pm 1\}$-matrix with pairwise orthogonal rows:



uwaterloo.ca/mathcheck

Results of MathCheck

Found the smallest counterexample of the Williamson conjecture.

Verified the even Williamson conjecture up to order 70.

Found three new counterexamples to the good matrix conjecture.

Verified the best matrix conjecture up to order seven.

Verified the Ruskey–Savage conjecture up to order five.

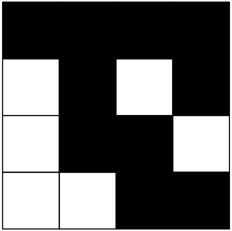
Verified the Norine conjecture up to order six.

Enumerated all quaternary Golay sequences up to length 28.

Verified the nonexistence of weight 15 and 16 codewords in a projective plane of order ten.

Hadamard matrices

In 1893, Hadamard defined what are now known as *Hadamard matrices*: square matrices with ± 1 entries and pairwise orthogonal rows.



The Hadamard conjecture

The *Hadamard conjecture* says that Hadamard matrices exist in order $4n$ for all $n \geq 1$.

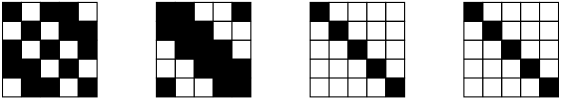
Strongly expected to hold but still open after 125 years.

Williamson matrices

Williamson matrices are symmetric and circulant (each row a cyclic shift of the previous row) $\{\pm 1\}$-matrices A, B, C, D such that

$$A^2 + B^2 + C^2 + D^2$$

is a scalar matrix.



Williamson's theorem

If A, B, C, D are Williamson matrices of order n then

$$\begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix}$$

is a Hadamard matrix of order $4n$.

The Williamson conjecture

It does, however, seem quite likely that not merely Hadamard matrices, but Hadamard matrices of the Williamsom type, "always exist,"...

Solomon Golomb and Leonard Baumert, 1963

Williamson matrices: A history

In 1944, Williamson found Williamson matrices in the orders

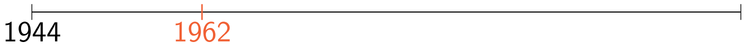
$$3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 25, 37, 43,$$

twice each number on this list, as well as 12, 20, and the powers of two up to 32.

1944

Williamson matrices: A history

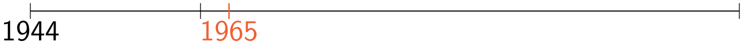
In 1962, Baumert, Golomb, and Hall found one in order 23.



S. Golomb, L. Baumert, M. Hall, 1962.

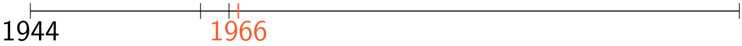
Williamson matrices: A history

In 1965, Baumert and Hall found seventeen sets of Williamson matrices in the orders 15, 17, 19, 21, 25, and 27.



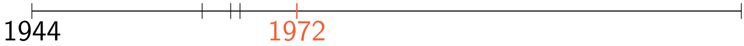
Williamson matrices: A history

The next year Baumert found one in order 29.



Williamson matrices: A history

In 1972, Turyn found an infinite class of them, including one in each order 27, 31, 37, 41, 45, 49, 51, 55, 57, 61, 63, and 69.

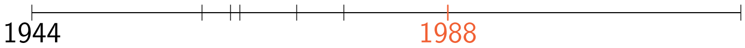


Williamson matrices: A history

In 1977, Sawade found four in order 25 and four in order 27 and Yamada found one in order 37.

Williamson matrices: A history

In 1988, Koukouvinos and Kounias found four in order 33.

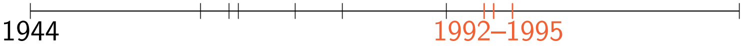


Williamson matrices: A history

In 1992, Đoković found one in order 31.

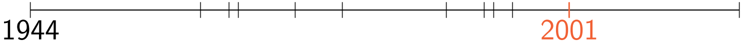
The next year he found one in order 33 and one in order 39.

Two years later he found two in order 25 and one in order 37.



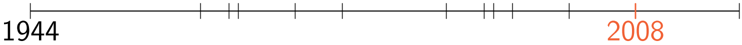
Williamson matrices: A history

In 2001, van Vliet found one in order 51.



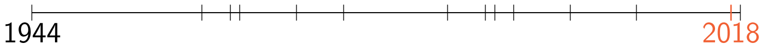
Williamson matrices: A history

In 2008, Holzmann, Kharaghani, and Tayfeh-Rezaie found one in order 43.

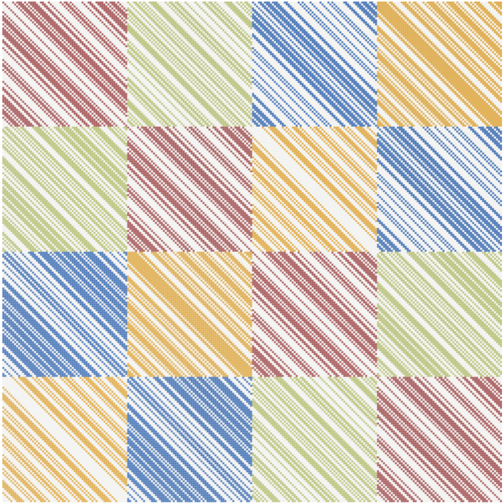


Williamson matrices: A history

In 2018, Bright, Kotsireas, and Ganesh found one in order 63.



A Hadamard matrix of order $4 \cdot 63 = 252$



Counterexamples

In 1993, the counterexample 35 was found by Đoković.

In 2008, the counterexamples 47, 53, and 59 were found by Holzmann, Kharaghani, and Tayfeh-Rezaie.

Đoković noted that 35 was the smallest *odd* counterexample but left open the question if it was the smallest counterexample.

Even orders

In 2006, Kotsireas and Koukouvinos found Williamson matrices in all even orders $n \leq 22$ using a CAS.

In 2016, Bright et al. found Williamson matrices in all even orders $n \leq 30$ using a SAT solver.

Even orders

In 2006, Kotsireas and Koukouvinos found Williamson matrices in all even orders $n \leq 22$ using a CAS.

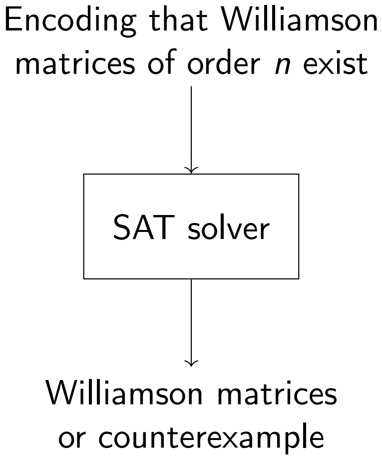
In 2016, Bright et al. found Williamson matrices in all even orders $n \leq 30$ using a SAT solver.

In 2018, Bright, Kotsireas, and Ganesh enumerated all Williamson matrices in all even orders $n \leq 70$ using a SAT+CAS method.

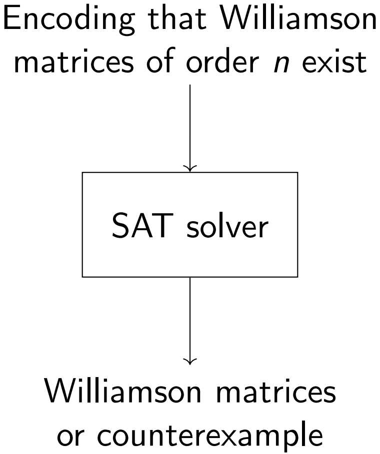
SAT encoding

Let the Boolean variables $a_0, \ldots, a_{n-1}$ represent the entries of the first row of the matrix A with true representing 1 and false representing -1.

Naive setup


Encoding that Williamson
matrices of order n exist
SAT solver
Williamson matrices
or counterexample

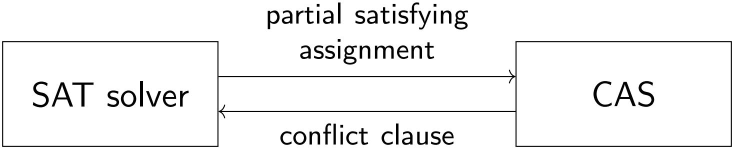
Naive setup



This is suboptimal as SAT solvers alone will not exploit mathematical facts about Williamson matrices.

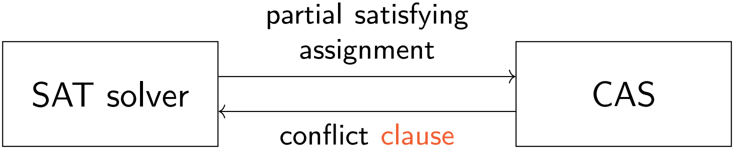
System overview

The SAT solver is augmented with a CAS learning method:



System overview

The SAT solver is augmented with a CAS learning method:



expression of the form $x_1 \vee x_2 \vee \cdots \vee x_n$ where each x_i is a variable or negated variable

Power spectral density (PSD) filtering

If A is a Williamson matrix then

$$\left|\sum_{j=0}^{n-1} a_j \exp(2\pi ijk/n)\right|^2 \leq 4n$$

for all integers k.

Search with PSD filtering

To exploit PSD filtering we need

(1) an efficient method of computing the PSD values; and
(2) an efficient method of searching while avoiding matrices that fail the filtering criteria.

Search with PSD filtering

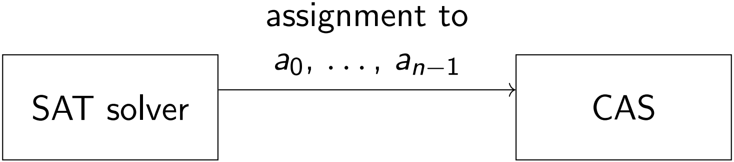
To exploit PSD filtering we need

(1) an efficient method of computing the PSD values; and

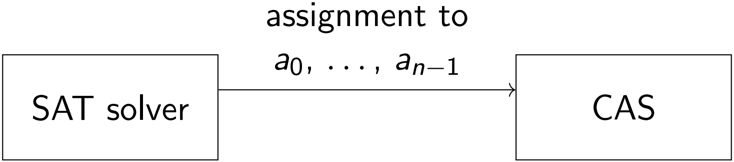
(2) an efficient method of searching while avoiding matrices that fail the filtering criteria.

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

Learning method

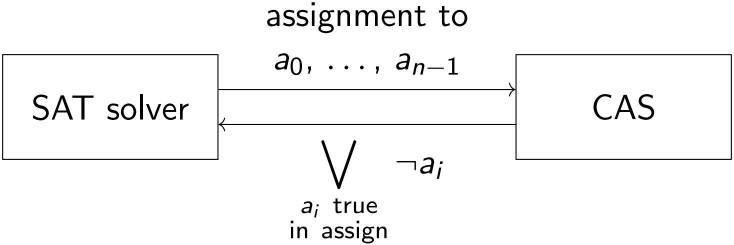


Learning method



The CAS computes the PSD of A. If it is too large...

Learning method



The CAS computes the PSD of A. If it is too large...

...a conflict clause is learned.

Enumeration results

We found over 100,000 new Williamson matrices in all even orders up to 70.

A huge number of Williamson matrices of order 64 were found.

Enumeration results

We found over 100,000 new Williamson matrices in all even orders up to 70.

A huge number of Williamson matrices of order 64 were found.

Interestingly, Williamson matrices in all orders 2^k can be found by generalizing their structure.

Projective planes

A *projective plane* is a square $\{0,1\}$-matrix such that any two columns or rows have an inner product of 1, the matrix has dimension $n^2 + n + 1$, and each column/rowsum is $n + 1$.

Such a projective plane is said to have *order n*.

Projective planes

A *projective plane* is a square $\{0,1\}$-matrix such that any two columns or rows have an inner product of 1, the matrix has dimension n^2+n+1, and each column/rowsum is $n+1$.

Such a projective plane is said to have *order* n.

Explicit constructions are known when n is a prime power.

The first critical value of n is $n = 10$. A thorough investigation of this case is currently beyond the facilities of computing machines.

Marshall Hall Jr.
Finite Projective Planes
1955

Projective planes of order ten: Weight 15 codewords

The simplest case of this search has been verified by at least three different independent implementations on modern desktops:

- Implementation in C, runs in 78 minutes.
- Implementation in GAP, runs in 7 minutes.
- Implementation in Mathematica, runs in 55 minutes.

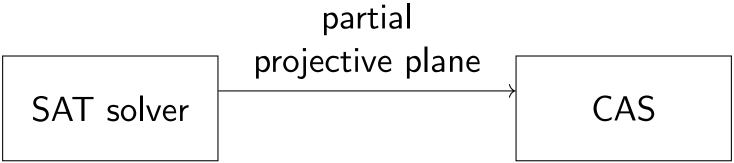
Projective planes of order ten: Weight 15 codewords

The simplest case of this search has been verified by at least three different independent implementations on modern desktops:

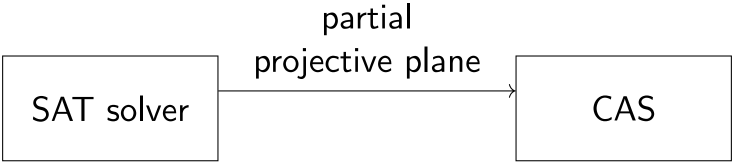
- Implementation in C, runs in 78 minutes.
- Implementation in GAP, runs in 7 minutes.
- Implementation in Mathematica, runs in 55 minutes.

We verified this using a SAT+CAS method in under 10 seconds.

Learning method

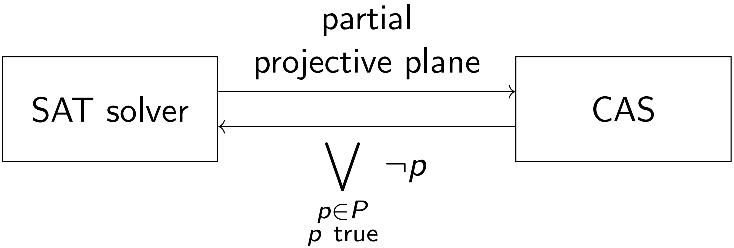


Learning method



The CAS computes a nontrivial symmetry P of the plane...

Learning method



The CAS computes a nontrivial symmetry P of the plane. . .

. . . and a symmetry blocking clause is learned.

Conclusion

The SAT+CAS paradigm is currently the fastest way of performing searches for certain combinatorial objects.

Conclusion

The SAT+CAS paradigm is currently the fastest way of performing searches for certain combinatorial objects.

Moreover, the code tends to be simpler: no need to write and optimize a special-purpose search algorithm.

Conclusion

The SAT+CAS paradigm is currently the fastest way of performing searches for certain combinatorial objects.

Moreover, the code tends to be simpler: no need to write and optimize a special-purpose search algorithm.

The main difficulty lies in setting up and tuning the learning method, requiring expertise in both SAT solvers and the problem domain.

Future work

I have been awarded an NSERC PDF to further develop the SAT+CAS paradigm over the next two years and I'm open to new applications or collaborations!

`curtisbright.com`