SAT Solvers and Computer Algebra Systems: A Powerful Combination for Mathematics

Curtis Bright[1] Ilias Kotsireas[2] Vijay Ganesh[1]

[1]University of Waterloo
[2]Wilfrid Laurier University

The 29th International Conference on
Computer Science and Software Engineering

November 4, 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.

Limitations of SAT solvers

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

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.

Limitations of CAS

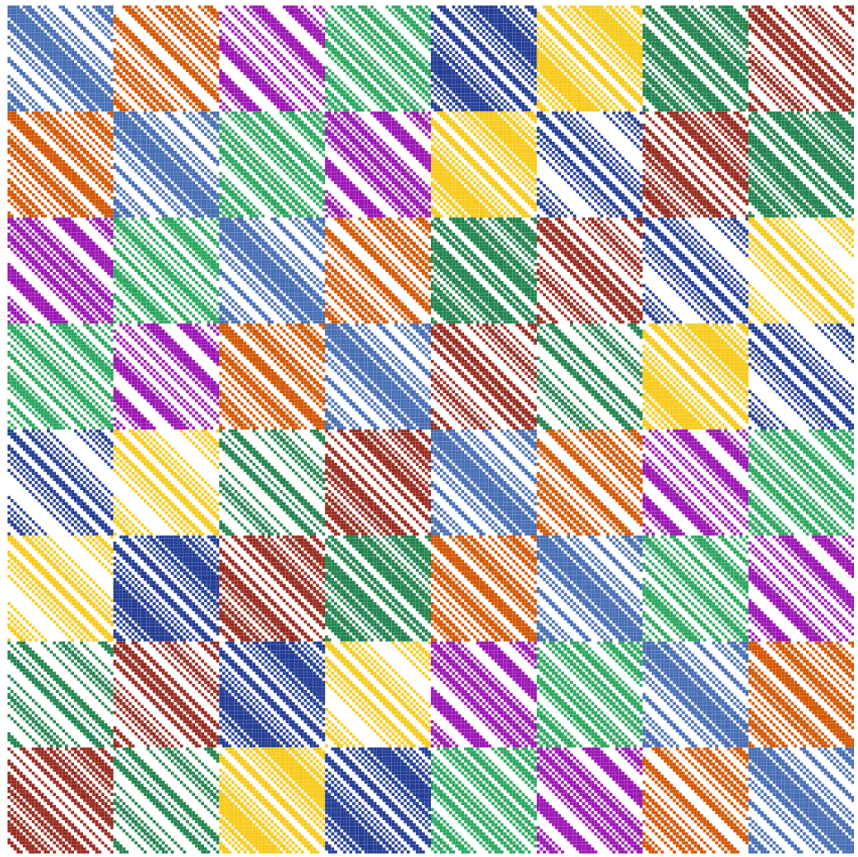
CASs are not optimized to do large (i.e., exponential) searches.

SAT + CAS

Search + 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

Verified the even Williamson conjecture up to order 70.

Found the smallest counterexample of the Williamson conjecture.

Found three new counterexamples to the good matrix conjecture.

Verified the best matrix conjecture up to order 57.

Verified conjectures about complex Golay sequences up to length 28.

Verified the Ruskey–Savage conjecture up to order five.

Verified the Norine conjecture up to order six.

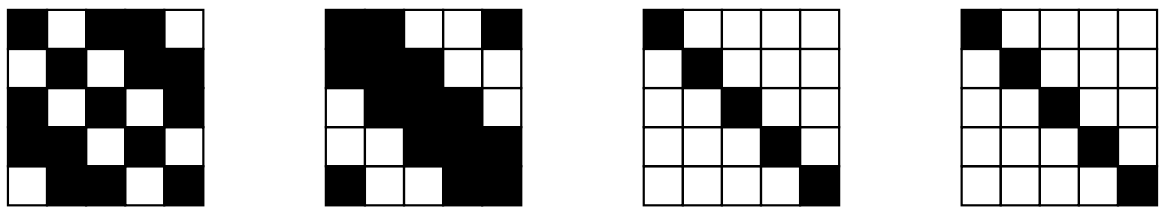
Verified the nonexistence of weight 15 and 16 codewords in a projective plane of order ten.

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.



The Williamson conjecture

It does, however, seem quite likely that [. . .] matrices of the Williamsom type, "always exist,". . .

Solomon Golomb and Leonard Baumert, 1963

Counterexample

Williamson matrices do not exist in order 35 and this is the smallest **odd** counterexample (Đoković 1993).

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

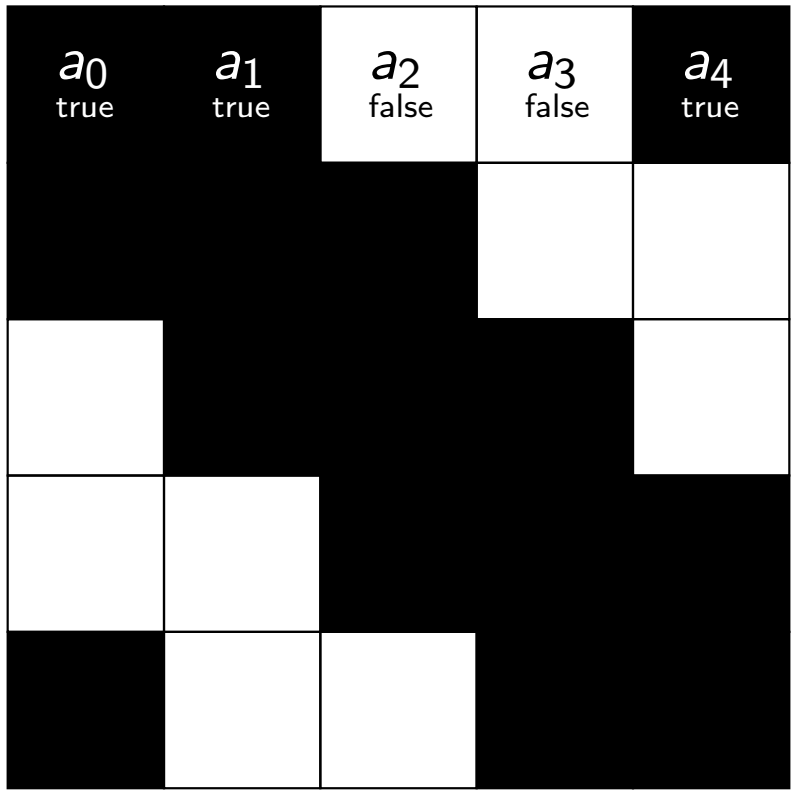
In 2006, Kotsireas and Koukouvinos found Williamson matrices in all even orders $n \leq 22$ using a CAS.

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

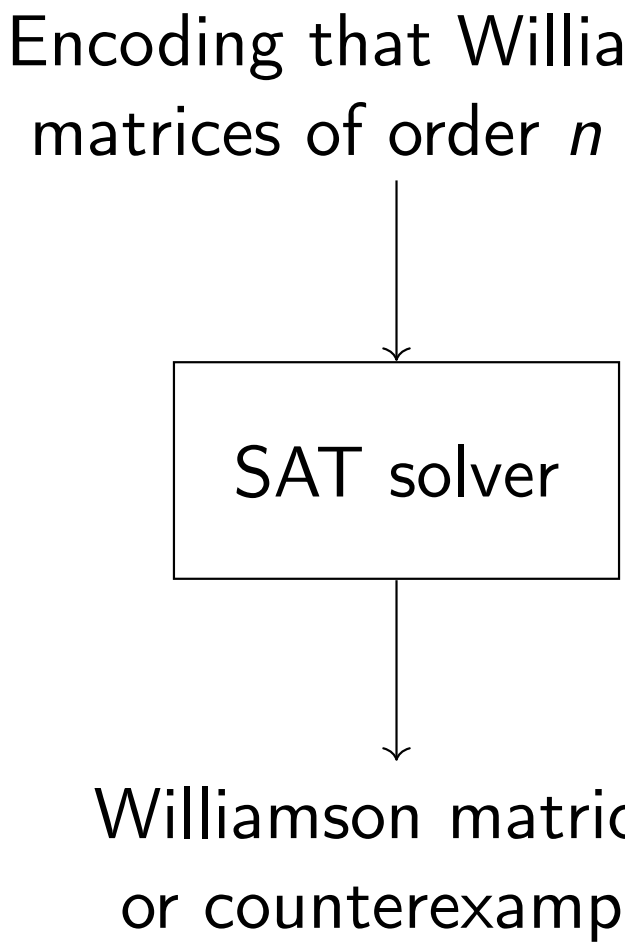
In 2018, Bright, Kotsireas, and Ganesh enumerated all Williamson matrices in all even orders $n \leq 70$ using a SAT+CAS method.

SAT encoding

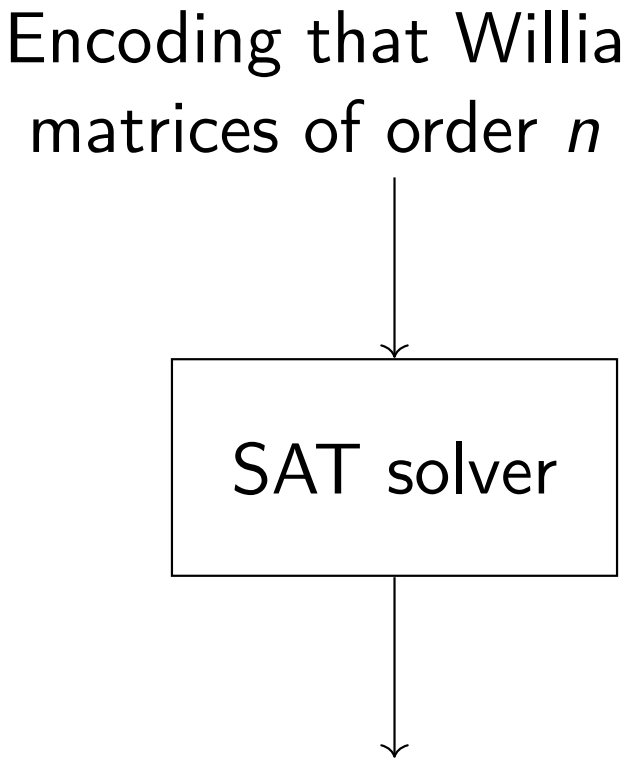
Let the Boolean variables $a_0, \ldots, a_{n-1}$ represent the entries of the first row of the matrix A with true representing 1 and false representing -1.



Naive setup


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

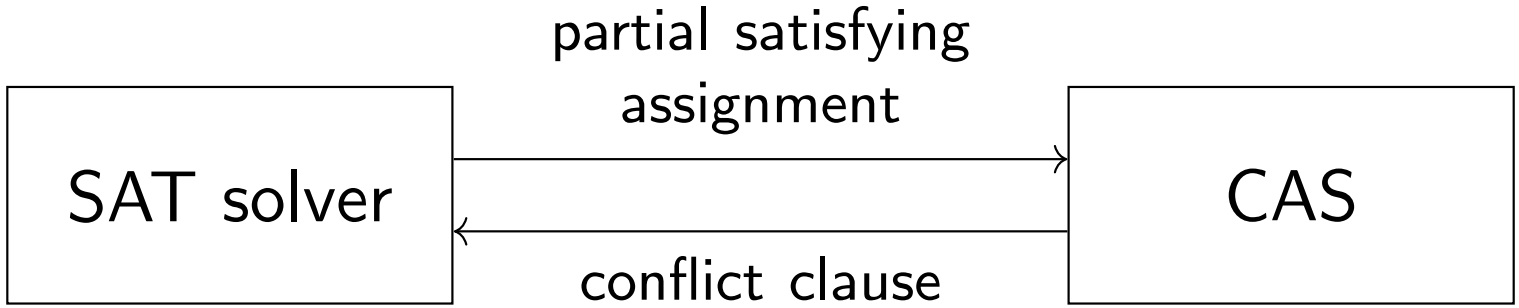
Naive setup



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

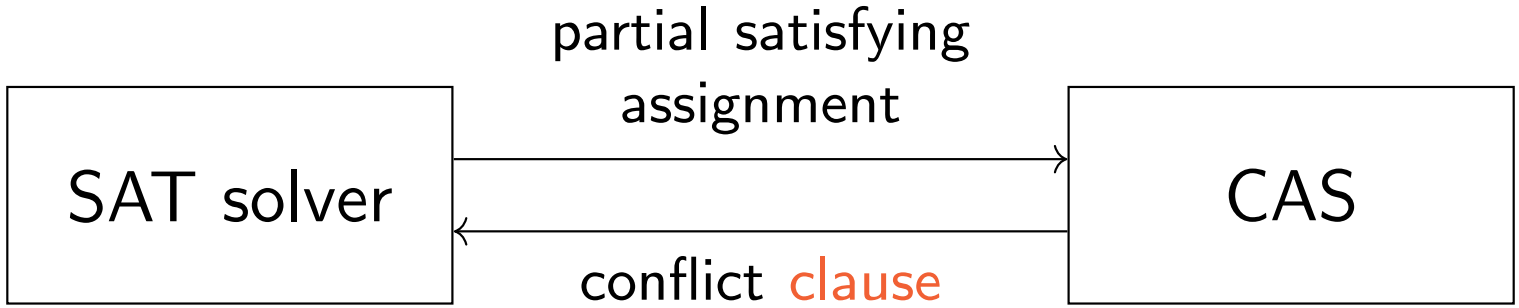
System overview

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

$$\mathrm{PSD}_A \leq 4n$$

where PSD_A is the maximum squared magnitude of the Fourier transform of A.

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

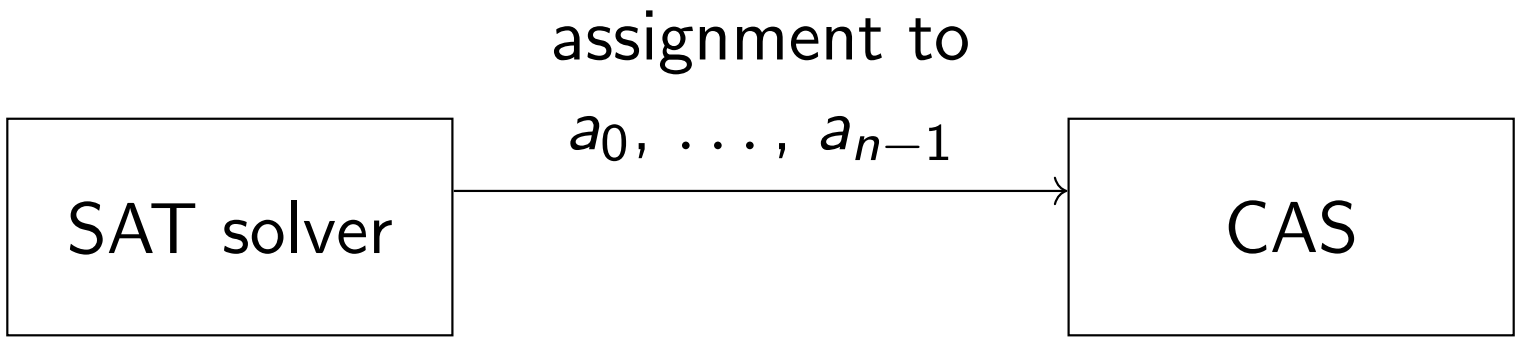
To exploit PSD filtering we need

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

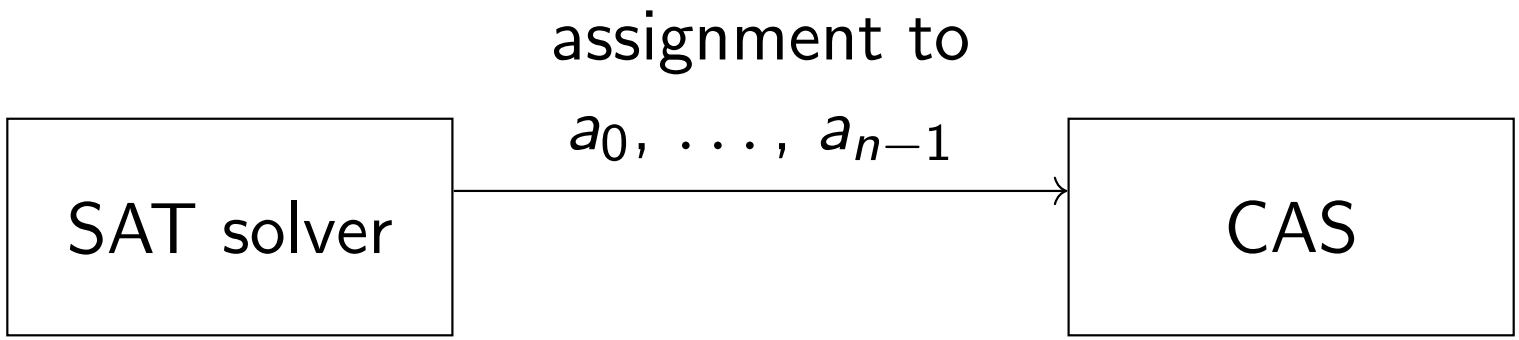
(2) an efficient method of searching while avoiding matrices that fail the filtering criteria.

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

Learning method

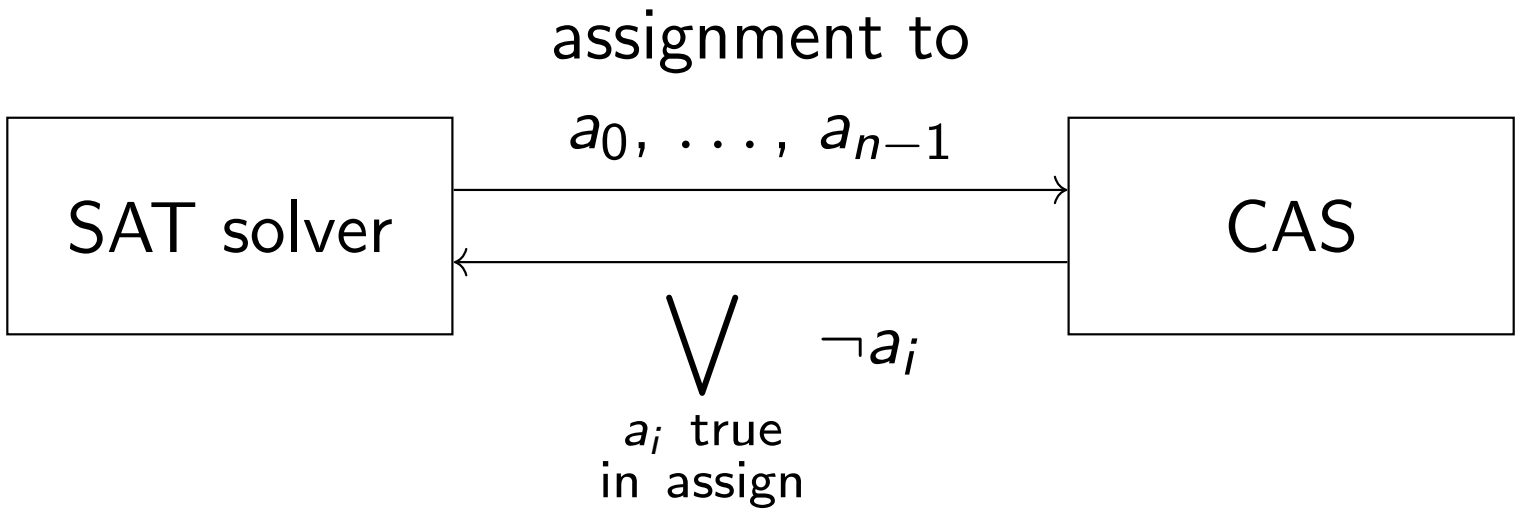


Learning method



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.

Results

Over 100,000 sets of Williamson matrices were found in all even orders up to order 70.

35 is in fact the smallest counterexample of the Williamson conjecture.

Applying Computer Algebra Systems with SAT Solvers to the Williamson Conjecture. *Journal of Symbolic Computation*, 2019.

Recent SAT+CAS Results

Heule, Kauers, and Seidl found many new algorithms for 3×3 matrix multiplication.

A family of schemes for multiplying 3×3 matrices with 23 coefficient multiplications. *ACM Communications in Computer Algebra*, 2019.

Kaufmann, Biere, and Kauers verified Boolean arithmetic circuits.

Verifying Large Multipliers by Combining SAT and Computer Algebra. *Conference on Formal Methods in Computer Aided Design*, 2019.

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.