When Computer Algebra Meets Satisfiability

A New Approach to Combinatorial Mathematics

Vijay Ganesh
University of Waterloo, Canada
&
Curtis Bright
University of Windsor, Canada

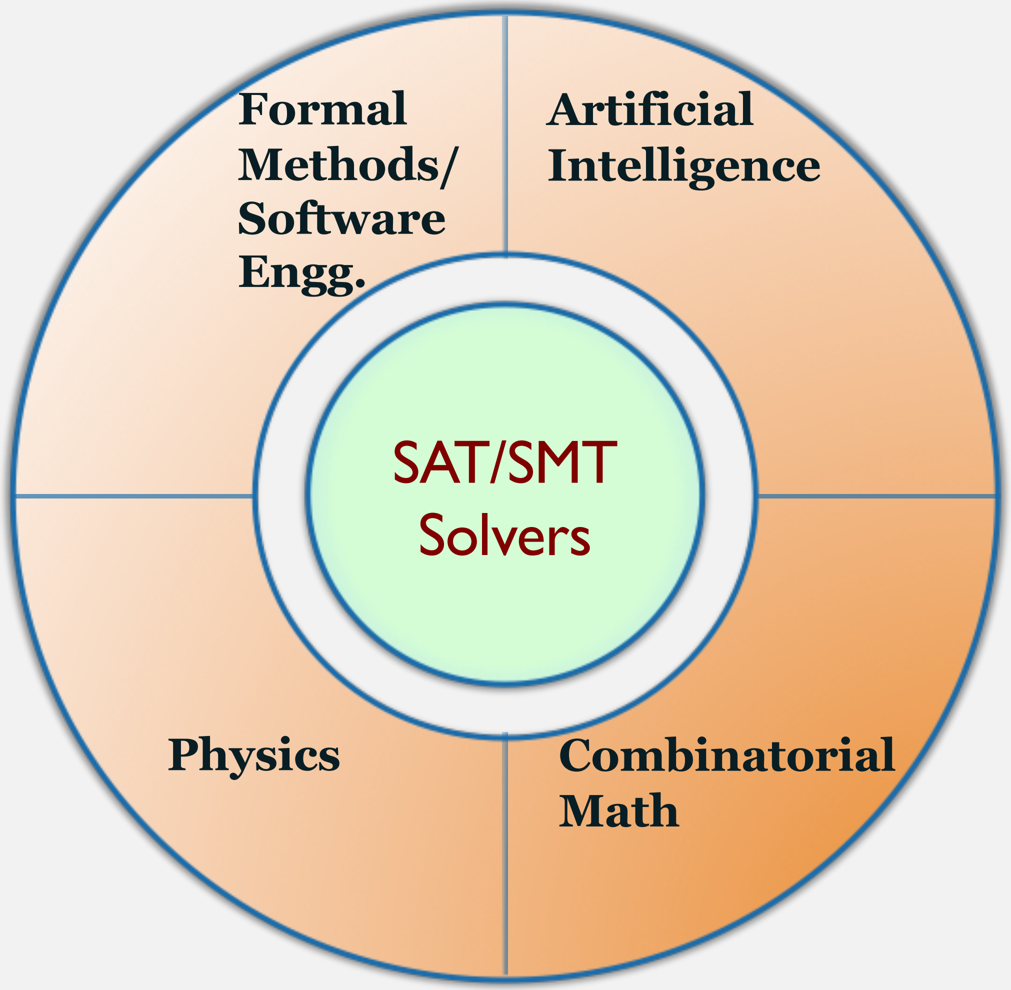
Harvard Math
Nov 3, 2021

PART I

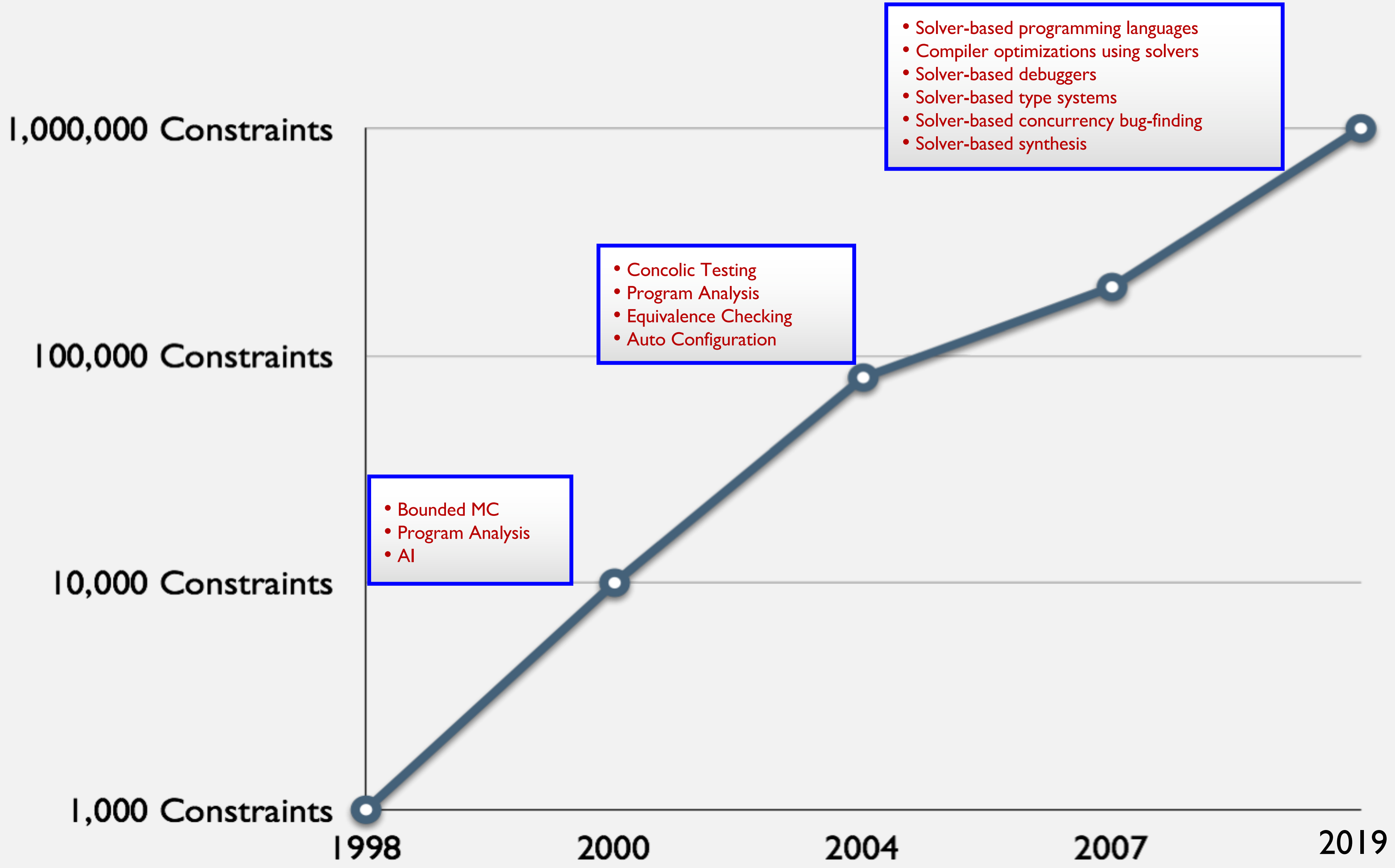
Context and Motivation

Why should you care about SAT Solvers?

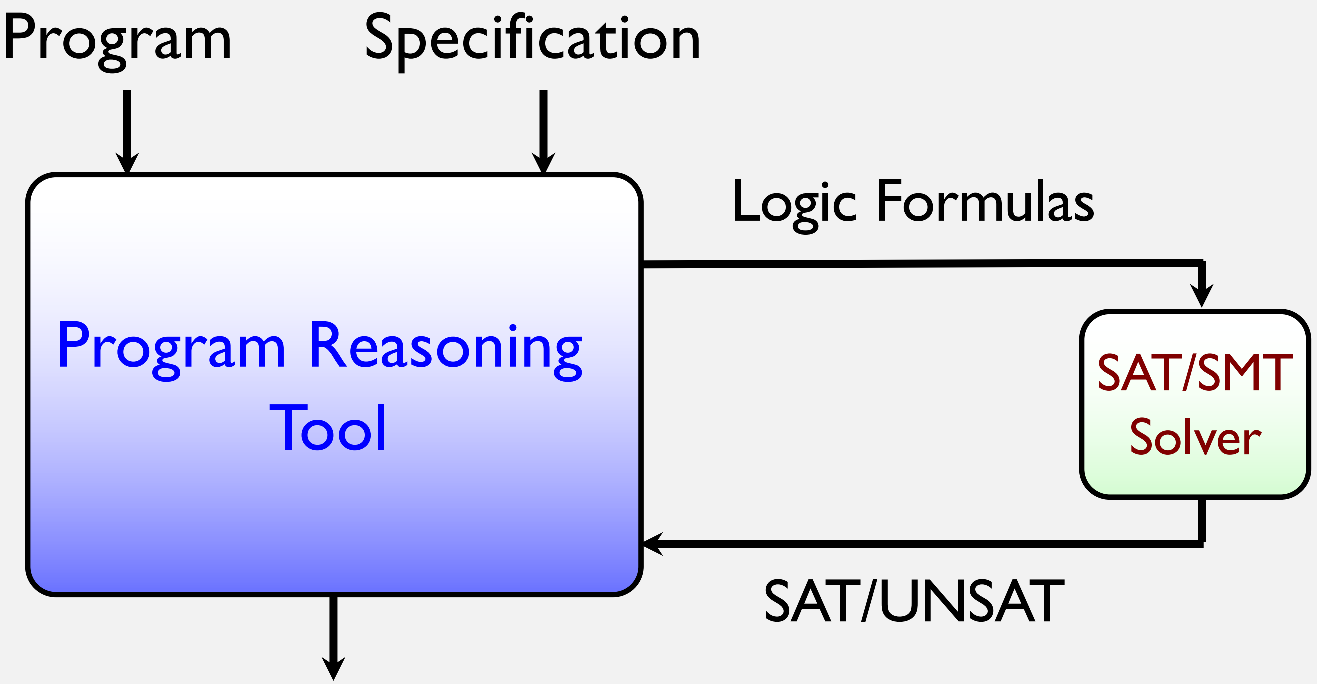
Combinatorial Math and SAT/SMT Solvers
An Indispensable Tool for many Strategies



SAT/SMT Solver Research Story
A 1000x+ Improvement



Solvers in Software Engineering and Security
Better Engineering, Usability, Novelty



Program is correct?
or Generate Counterexamples (test cases)

Research Questions

- How can we leverage the search capabilities of SAT solvers to counter-example math conjectures?
  - Pros: Solvers can easily search very large combinatorial spaces
  - Cons: Solvers lack domain-specific knowledge

- How do we compensate for the weaknesses of SAT?
  - Computer Algebra Systems (CAS) are repositories of domain-specific knowledge about many areas of mathematics, but lack the search capabilities of SAT

- Answer: Combine SAT and CAS

PART II

SAT Solver Background

The Boolean Satisfiability (SAT) Problem
Basic Definitions

- The Boolean SAT problem: Given Boolean formulas in Conjunctive Normal Form (CNF), decide whether they are satisfiable. A SAT solver is a program that takes as input CNF formulas, and decides whether they are satisfiable.

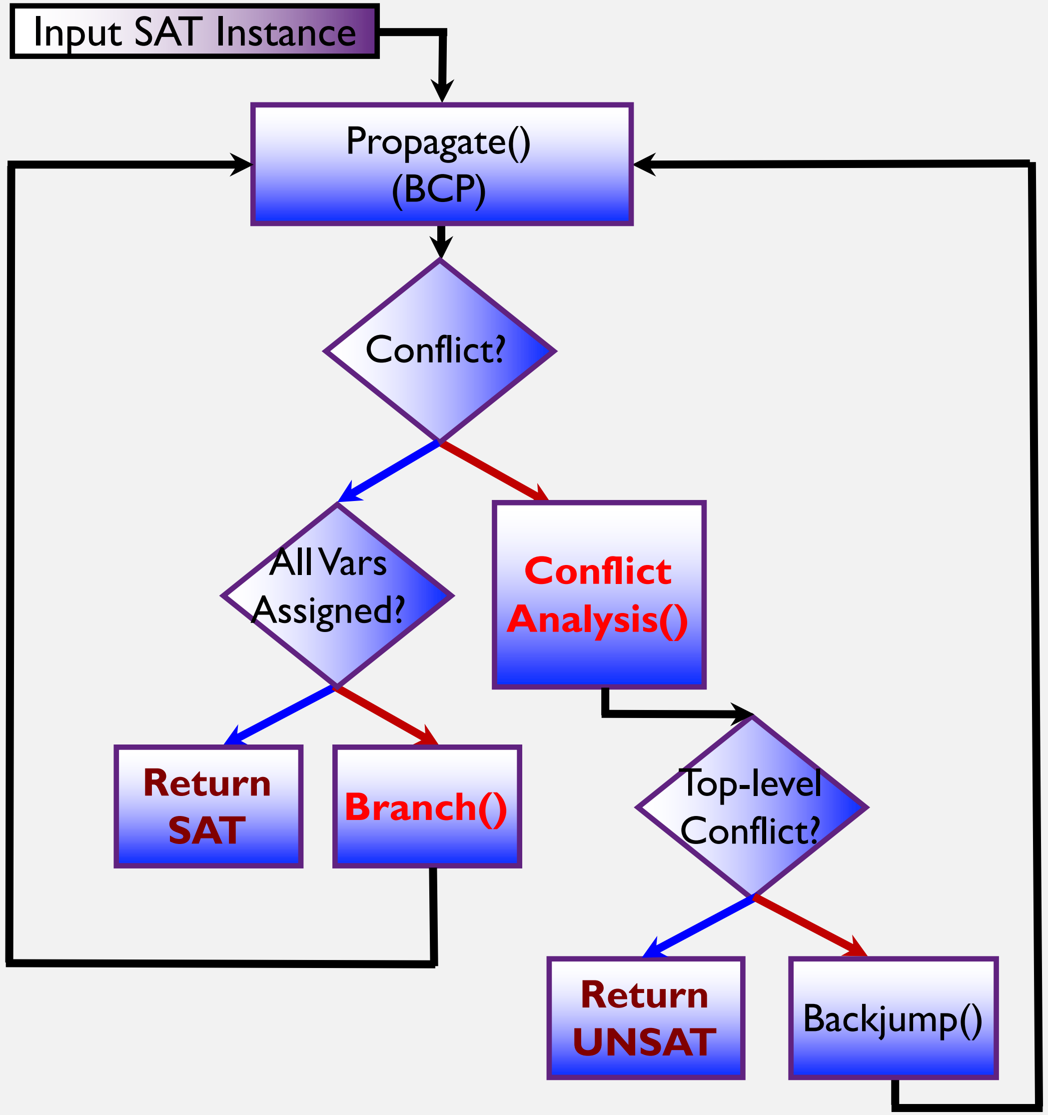
$$(x_1 \lor \neg x_2 \ldots \lor \neg x_n)$$
$$(\neg x_1 \lor \neg x_2 \ldots \lor x_n)$$
$$\ldots$$
$$(\neg x_1 \lor x_2 \ldots \lor \neg x_n)$$

- The SAT problem is known to be NP-complete, believed to be intractable.

- SAT solvers are required to produce proofs of unsatisfiability for UNSAT instances and satisfying assignments for SAT instances

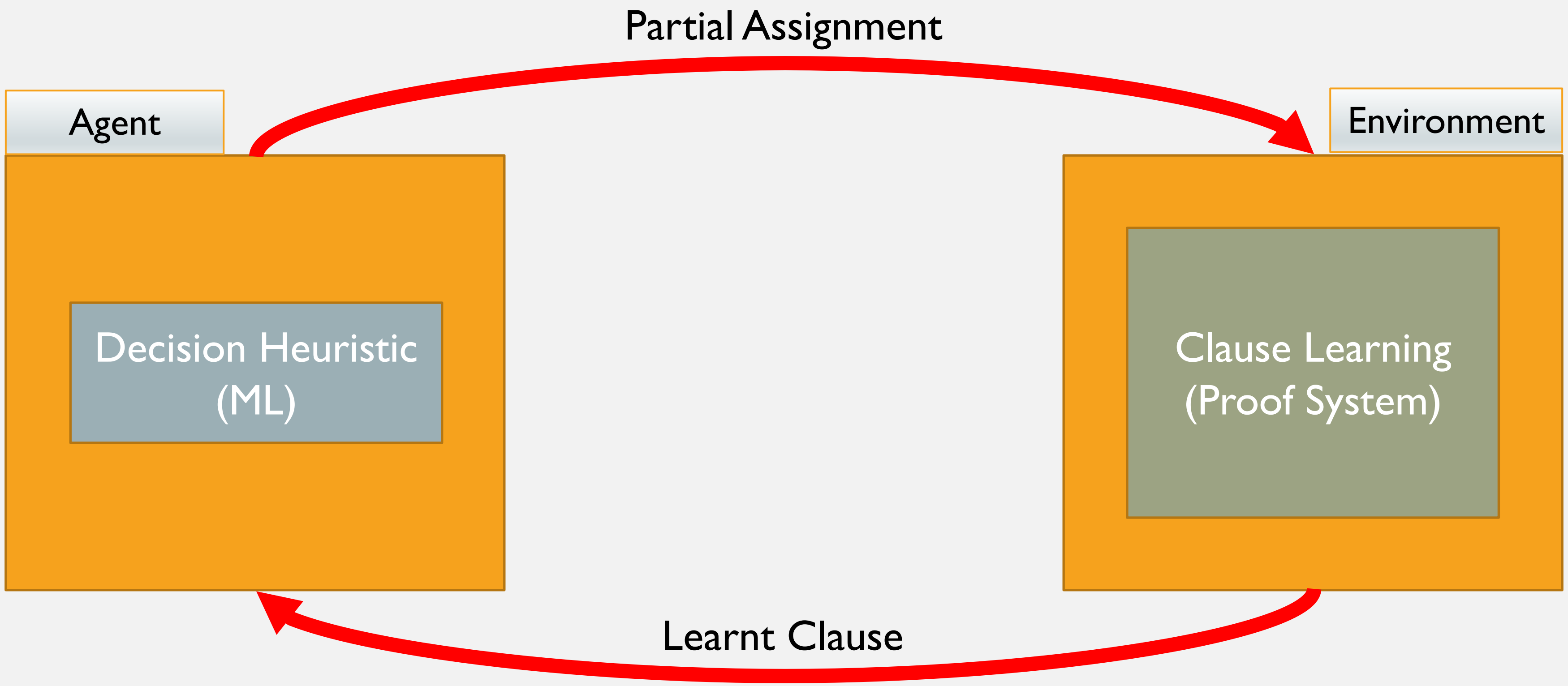
Modern Conflict-Driven Clause-Learning (CDCL) SAT Solver

Overview



GRASP Solver: [MS96]
ZChaff Solver: [MMZZM01]

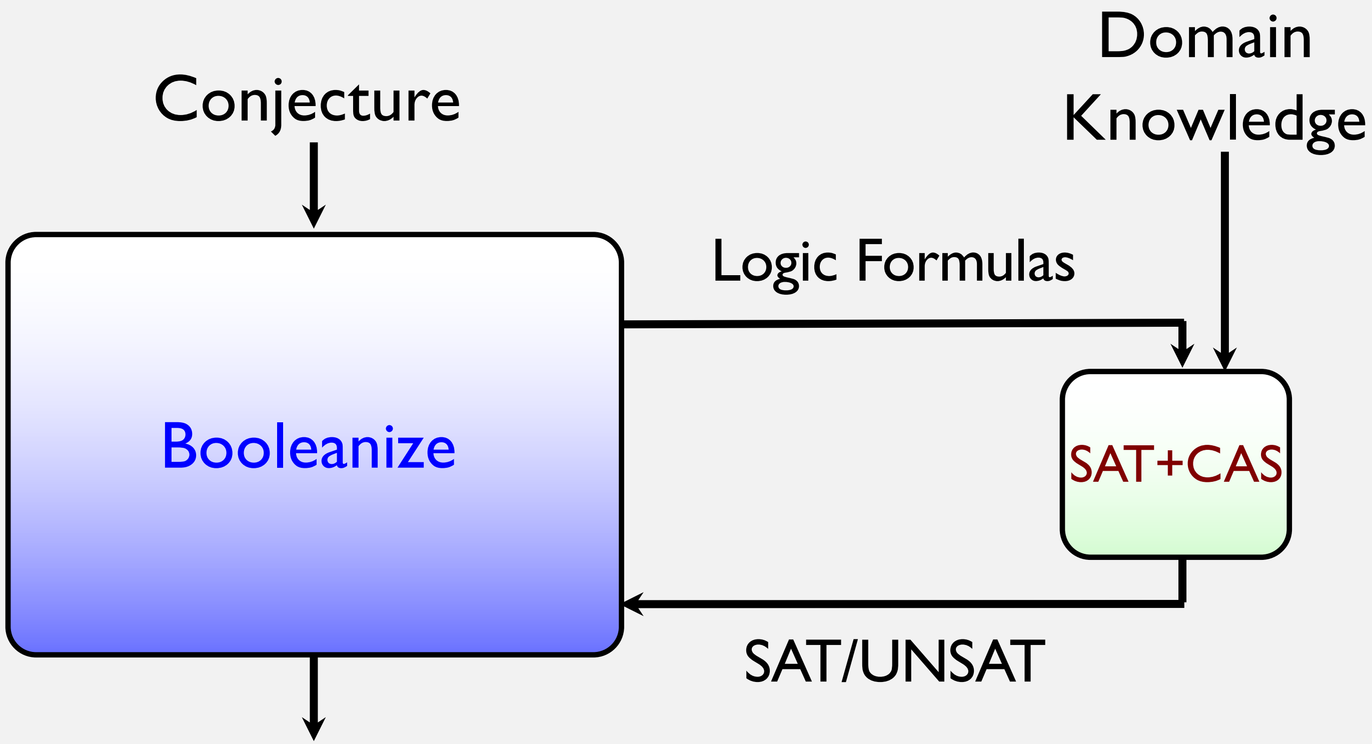
CDCL with Deductive Feedback Loop
Reinforcement Learning



PART III

SAT+CAS

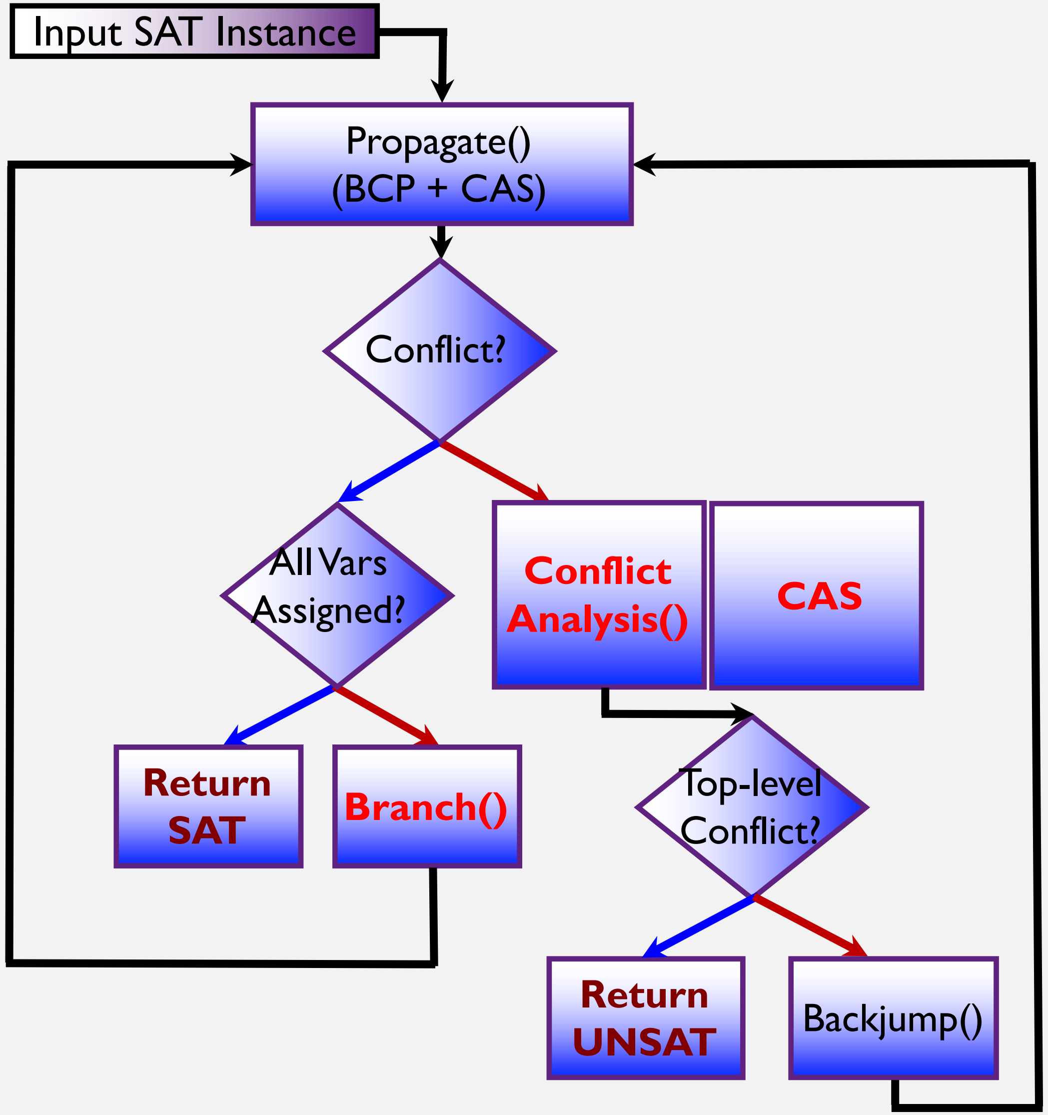
SAT+CAS for Math
Search + Domain Knowledge



Program is correct?
or Generate Counterexamples

Modern Conflict-Driven Clause-Learning (CDCL) SAT Solver

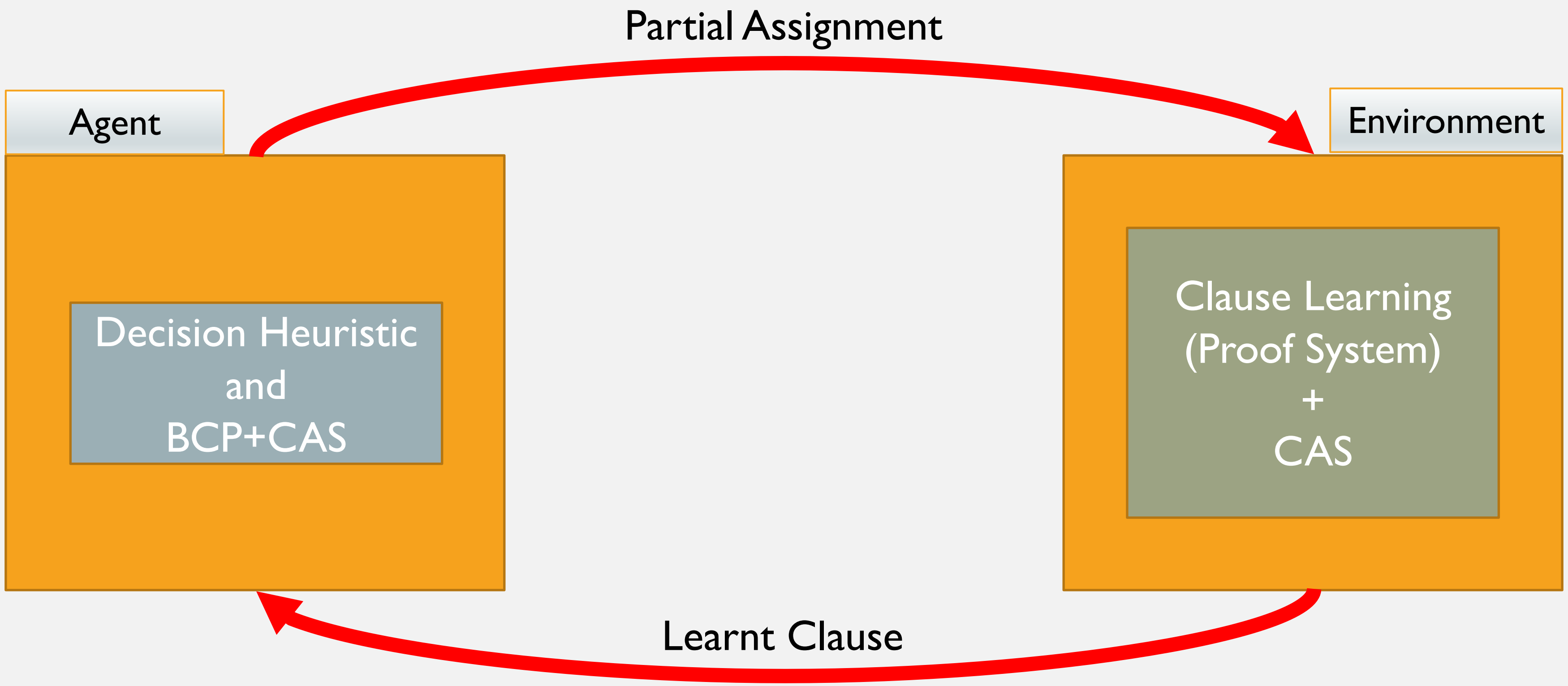
Overview



GRASP Solver: [MS96]
ZChaff Solver: [MMZZM01]

SAT+CAS with Deductive Feedback Loop

Search + Domain Knowledge



[MathCheck: A Math Assistant based on a Combination of Computer Algebra Systems and SAT Solvers]
Zulkoski, Czarnecki, and G.
International Conference on Automated Deduction (**CADE 2015**), Berlin, Germany, August 1-7, 2015

MathCheck: The first SAT+CAS system

We extended MathCheck in 2016 and used it to find (or prove the nonexistence of) Williamson matrices in large orders.[1]

MathCheck has since won several awards including a 2020 best paper award in *Applicable Algebra in Engineering, Communication and Computing* for work on Lam's problem in finite geometry.[2]

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

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

Application I:
The Williamson Conjecture

Hadamard matrices

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

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 \end{bmatrix}$$

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.[3]

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

Williamson's construction

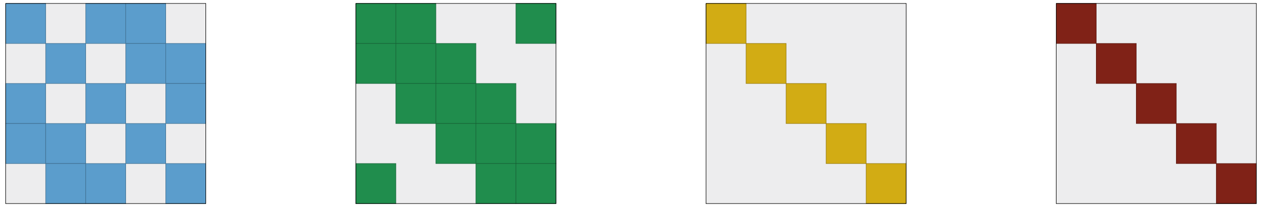
In 1944, John Williamson discovered a method of constructing Hadamard matrices in many orders like this order 8 example:

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

Williamson matrices

Williamson's construction relies on finding a quadruple (A, B, C, D) of $\{\pm1\}$-matrices for which all of the off-diagonal entries of $A^2 + B^2 + C^2 + D^2$ 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.



Williamson matrices of order 5.

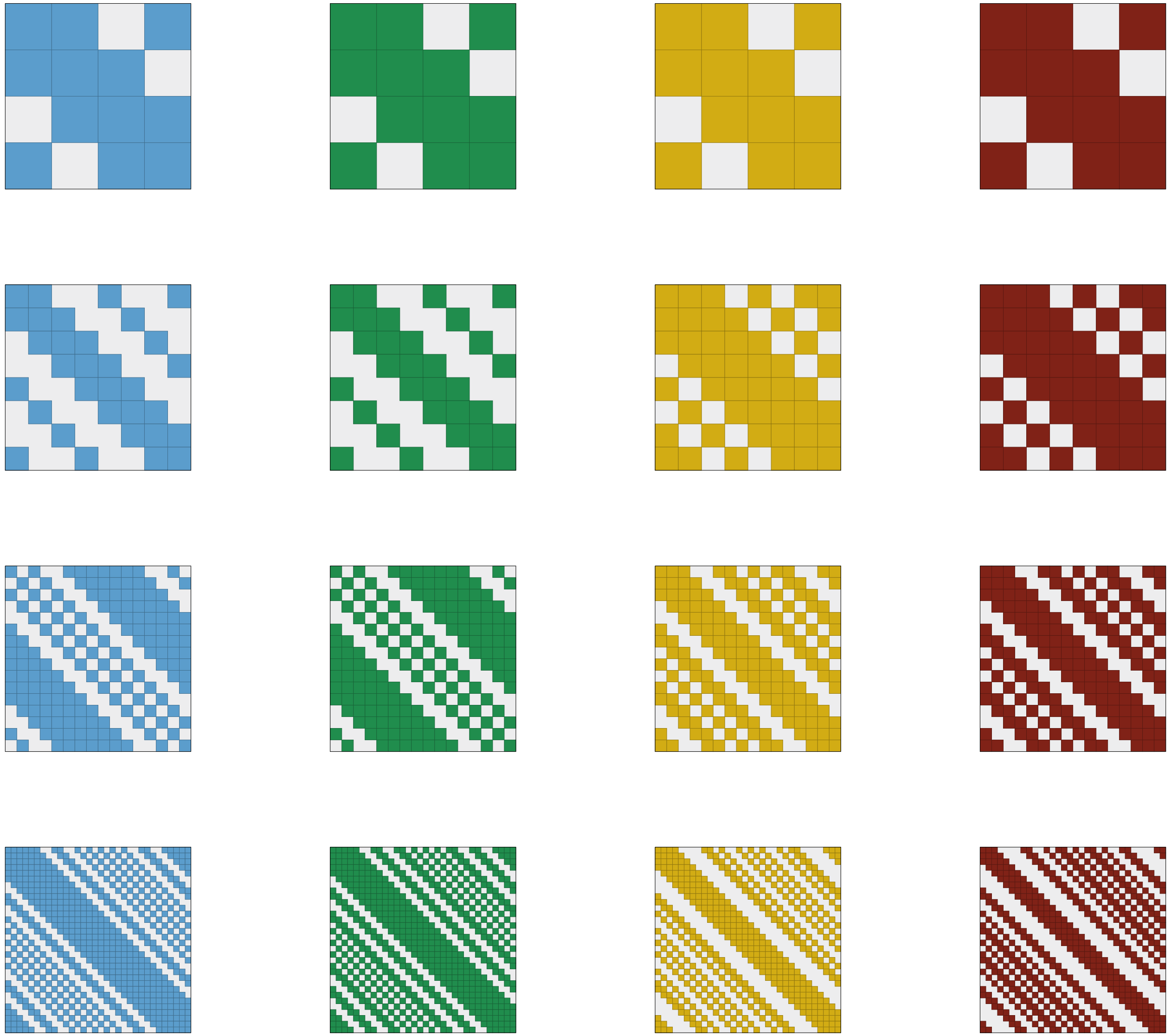
The Williamson conjecture

Many researchers expected Williamson matrices to exist in all orders and this became known as the *Williamson conjecture*.

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

> 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.

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.

In 2019, we ran exhaustive searches for Williamson matrices in all even orders $n \leq 70$ and discovered a large number of Williamson matrices in order 64.[4]

The patterns uncovered by these searches show that Williamson's method works for **all** orders that are powers of two.[5]

---

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

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

Previous searches

In 2006, a computer algebra approach found Williamson matrices in all even orders $n \leq 22$.[6]

In 2016, a satisfiability approach found Williamson matrices in all even orders $n \leq 30$.[7]

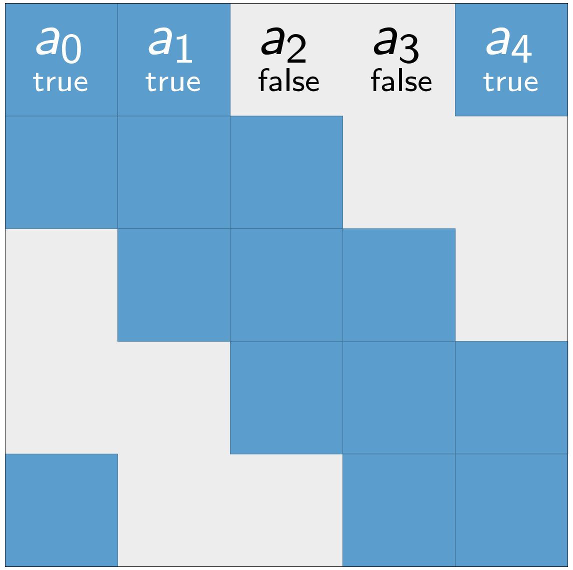
The search space for order $n = 70$ is **twenty-five orders of magnitude** larger than the search space for order $n = 30$—yet it is possible to search exhaustively with a hybrid approach.

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

[7] 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 conjunctive normal form).

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 matrix with first row $[a_0, \ldots, a_{n-1}]$ then

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

where $\mathrm{PSD}_{\boldsymbol{A}}$ is the maximum squared magnitude of the Fourier transform of $[a_0, \ldots, a_{n-1}]$.

Precisely, $\left|\sum_{j=0}^{n-1} a_j \omega^j\right|^2 \leq 4n$ where ω is any nth root of unity.

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

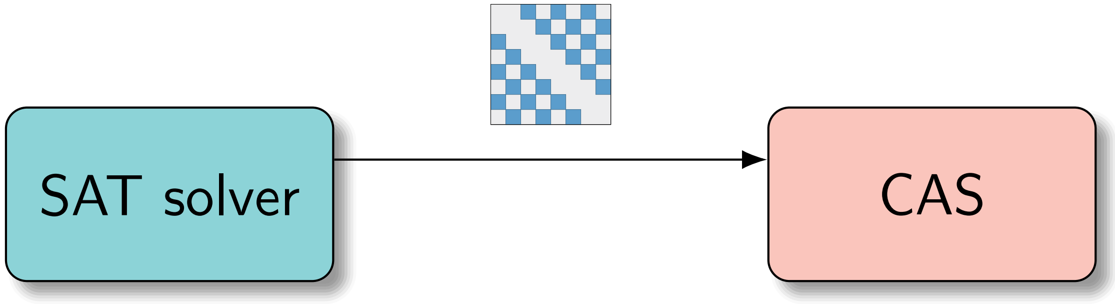
(1) an efficient method of computing the PSD values; and

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

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

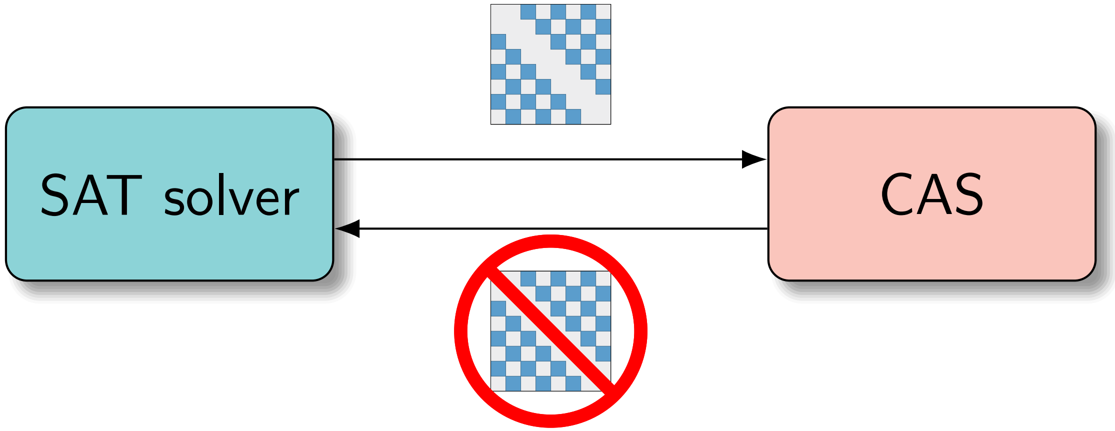
SAT+CAS learning for Williamson matrices

The CAS computes the PSD of a matrix provided by the SAT solver. . .



SAT+CAS learning for Williamson matrices

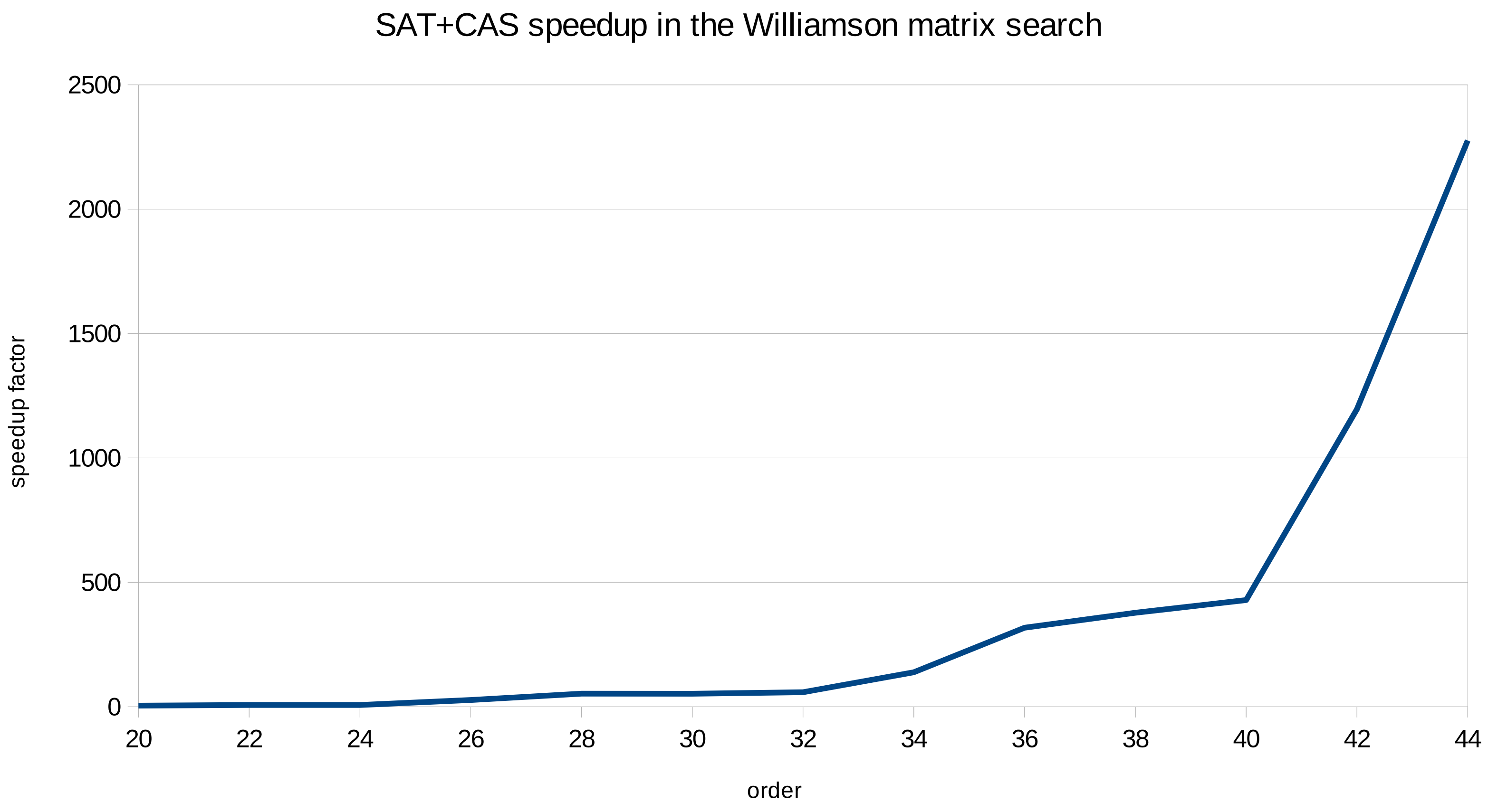
The CAS computes the PSD of a matrix provided by the SAT solver. . .



. . . if it is too large, the matrix is blocked from the search.

Encoding comparison

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



Results

With our SAT+CAS system MathCheck we found over 100,000 new sets of Williamson matrices—even though fewer than 200 had previously been found by computers.

MathCheck also showed that $n = 35$ is the smallest counterexample of the Williamson conjecture (though the nonexistence of solutions in order 35 was previously known.[8])

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

[8] D. Đoković. Williamson matrices of order $4n$ for $n = 33, 35, 39$. *Discrete Mathematics*, 1993.

Application II:
Lam's Problem

History

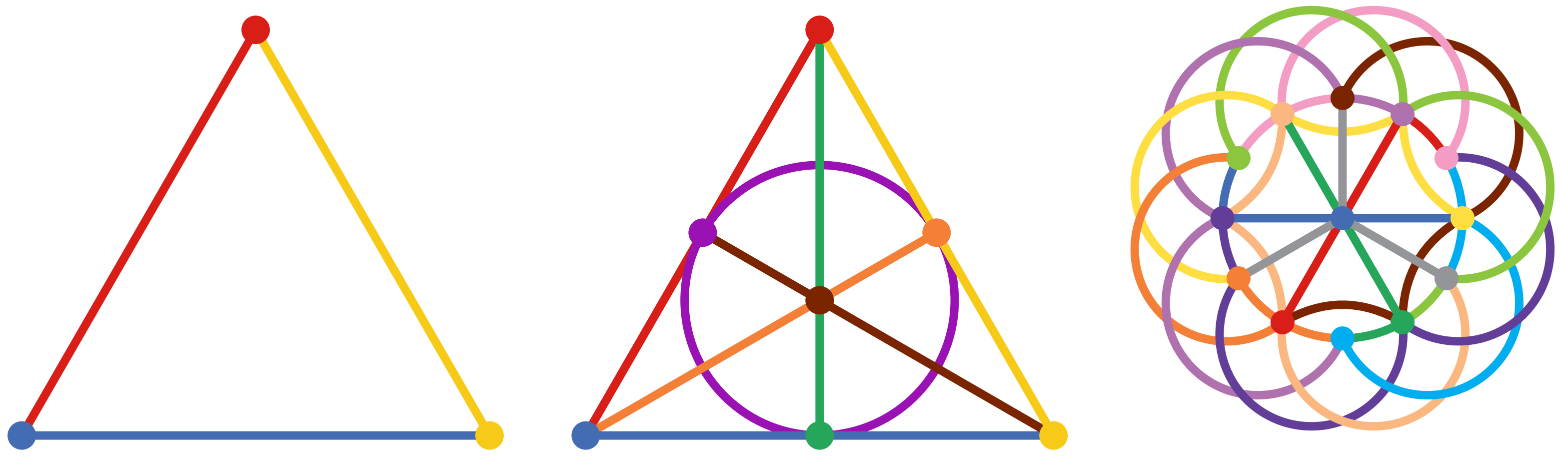
Since 300 BC, mathematicians tried to derive Euclid's "parallel postulate" from his other axioms for geometry.

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

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

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.[9] 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.

Using MathCheck, we generated the first certifiable resolution of Lam's problem.[10]

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

[10] 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

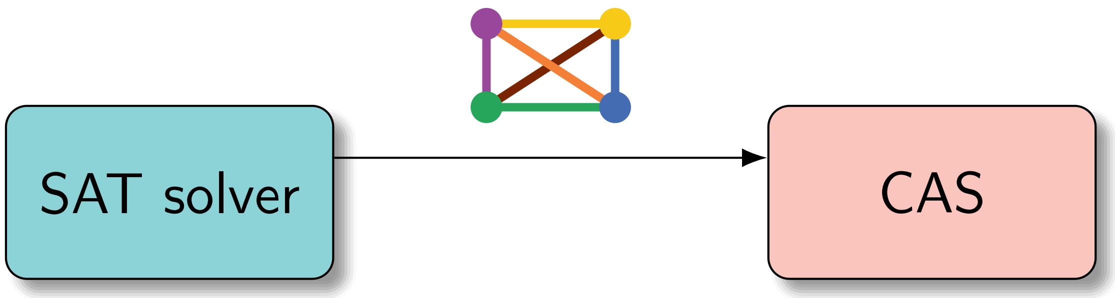
1	0	0	0	1	0	0	0	1	1	0	0	0
0	0	1	1	0	0	0	1	0	1	0	0	0
0	1	0	0	0	1	1	0	0	1	0	0	0
1	0	0	0	0	1	0	1	0	0	1	0	0
0	1	0	1	0	0	0	0	1	0	1	0	0
0	0	1	0	1	0	1	0	0	0	1	0	0
1	0	0	1	0	0	1	0	0	0	0	1	0
0	1	0	0	1	0	0	1	0	0	0	1	0
0	0	1	0	0	1	0	0	1	0	0	1	0
0	0	0	1	1	1	0	0	0	0	0	0	1
0	0	0	0	0	0	1	1	1	0	0	0	1
1	1	1	0	0	0	0	0	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.

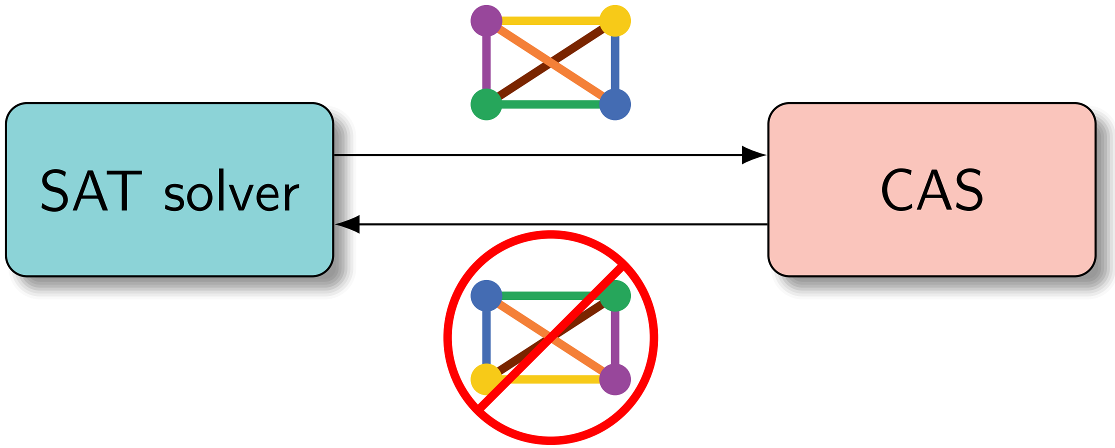
SAT+CAS learning for Lam's problem

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



SAT+CAS learning for Lam's problem

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



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

Results

The search for a projective plane of order 10 can be split into three main cases. The search times compared with previous searches:

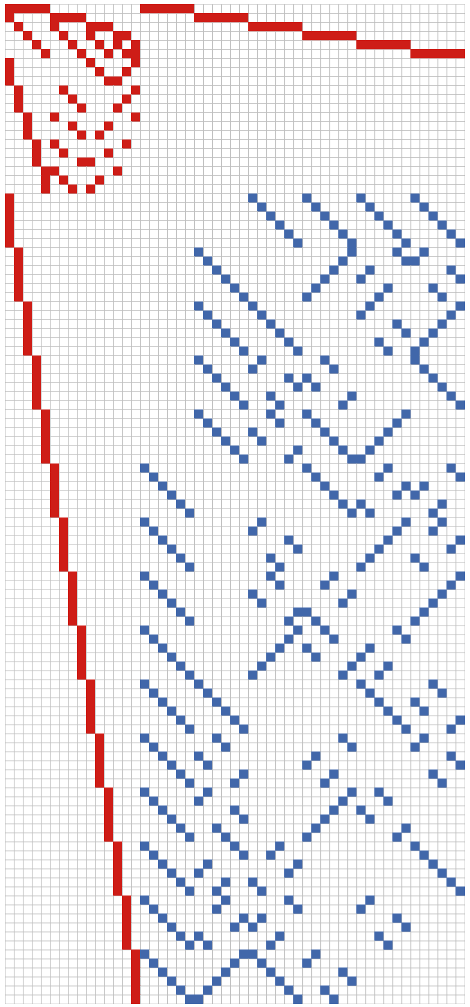
Case	**SAT-based**	**CAS-based**	**SAT+CAS**
1	5 minutes	3–78 minutes	0.1 minutes
2	–	16,000 hours	30 hours
3	–	20,000 hours	16,000 hours

The SAT+CAS approach was much faster in the first two cases and decently faster in the third case (a case where most of the search space was not very symmetric).

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-column partial projective plane of order ten said to not exist in 2011—but we found with MathCheck.



Other results

We have successfully used MathCheck in many other problems:

Problem	**Main 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

`uwaterloo.ca/mathcheck`

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.

Adding CAS functionality to a SAT solver significantly increases its expressiveness and facilitates applying SAT to more problems.

Future work

SAT+CAS methods are poised to forever change what is considered feasible in mathematical search—and there are many promising areas where they have yet to be used.

For example, SAT+CAS methods have been used to find small circuits for matrix multiplication[11] and we are using SAT+CAS methods to look for small Kochen–Specker systems.[12]

`curtisbright.com`

`ece.uwaterloo.ca/~vganesh`

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

[12] J. Conway, S. Kochen. The Free Will Theorem. *Foundations of Physics*, 2006.