A SAT Solver + Computer Algebra Attack on the Minimum Kochen–Specker Problem

August 11, 2023

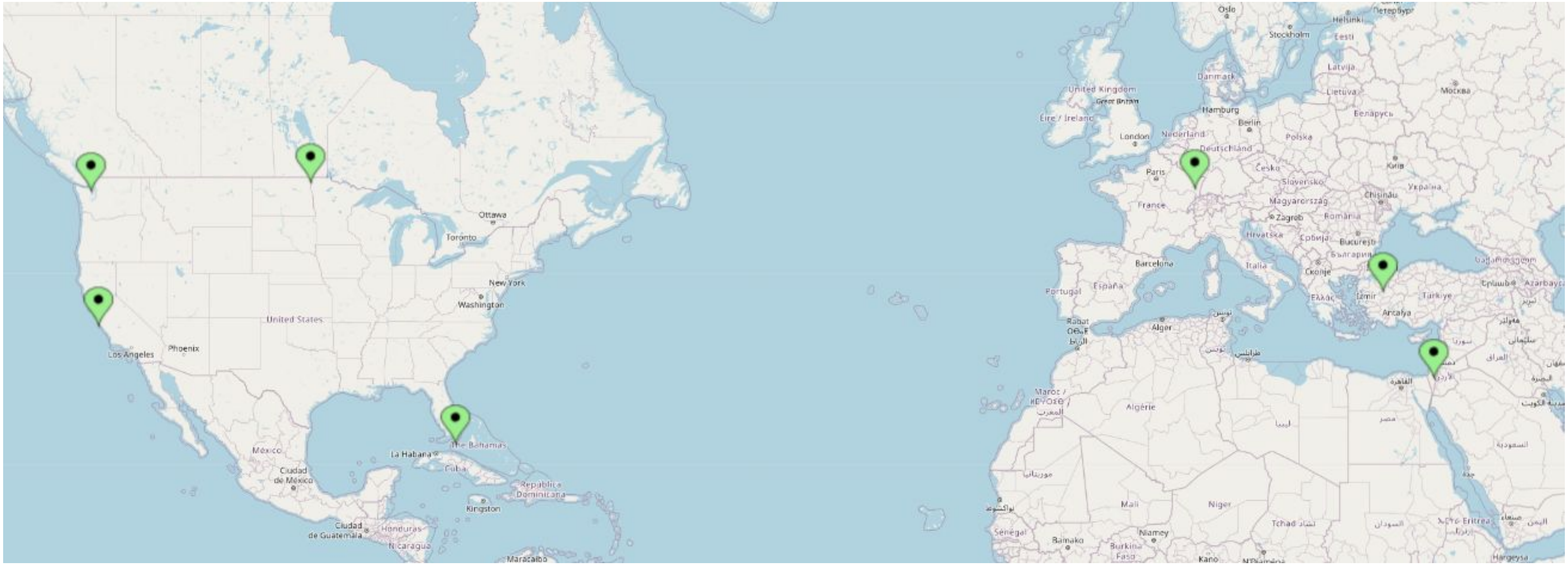
Brian (Zhengyu) Li[1]

[1] University of Waterloo, Faculty of Mathematics

Supervised by Vijay Ganesh, Curtis Bright

UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS

Conference and Seminar Highlights



Conference and Seminar Highlights

- Zhengyu Li
  - Mar. 2023: Southeastern International Conference on Combinatorics, Graph Theory and Computing
  - Aug. 2022: Federated Logic Conference - Workshop on Satisfiability Checking and Symbolic Computation

- Curtis Bright
  - Jun. 2023: CanaDAM - Canadian Discrete and Algorithmic Mathematics
  - Feb. 2022, Apr. 2023, Jun. 2023: Dagstuhl Seminar
  - May 2023: Quantum Computing Academic Assembly
  - Feb 2023: UBC & SFU discrete math seminars
  - Aug. 2022: Application of Computer Algebra
  - Jun. 2022: Satisfiability: Theory, Practice, and Beyond Reunion @ Simons Institute

- Vijay Ganesh
  - May 2023: Extended Reunion: Satisfiability @ Simons Institute
  - Oct. 2022: Dagstuhl Seminar

Research based on My Work

- Kirchweger, Markus, Tomáš Peitl, and Stefan Szeider. "Co-Certificate Learning with SAT Modulo Symmetries." arXiv preprint arXiv:2306.10427 (2023).

- Fazekas, Katalin, Aina Niemetz, Mathias Preiner, Markus Kirchweger, Stefan Szeider, and Armin Biere. "IPASIR-UP: User Propagators for CDCL." In 26th International Conference on Theory and Applications of Satisfiability Testing (SAT 2023). Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2023.

The Kochen-Specker Theorem

In Quantum Foundations, the Kochen-Specker (KS) theorem states that there exists a contradiction between the following:

- The SPIN axiom: measurements must follow a pattern
- The principle of non-contextuality: the outcome of an observation is predetermined

The theorem shows that we cannot assign definite values to certain properties of particles before we measure them, challenging our classical understanding of hidden realities.

To prove the theorem, Kochen and Specker establish the existence of a KS vector system.

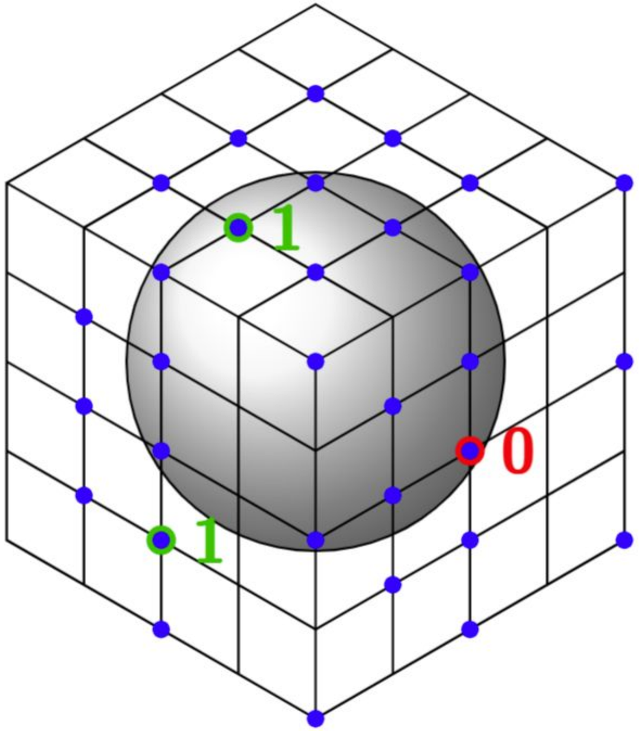
What is a Kochen–Specker System?

A set of vectors is 101-colorable if there exists an {0,1} coloring such that

- Two orthogonal vectors are not both colored 0.
- Three mutually orthogonal vectors are colored 1, 0, 1 in some order.

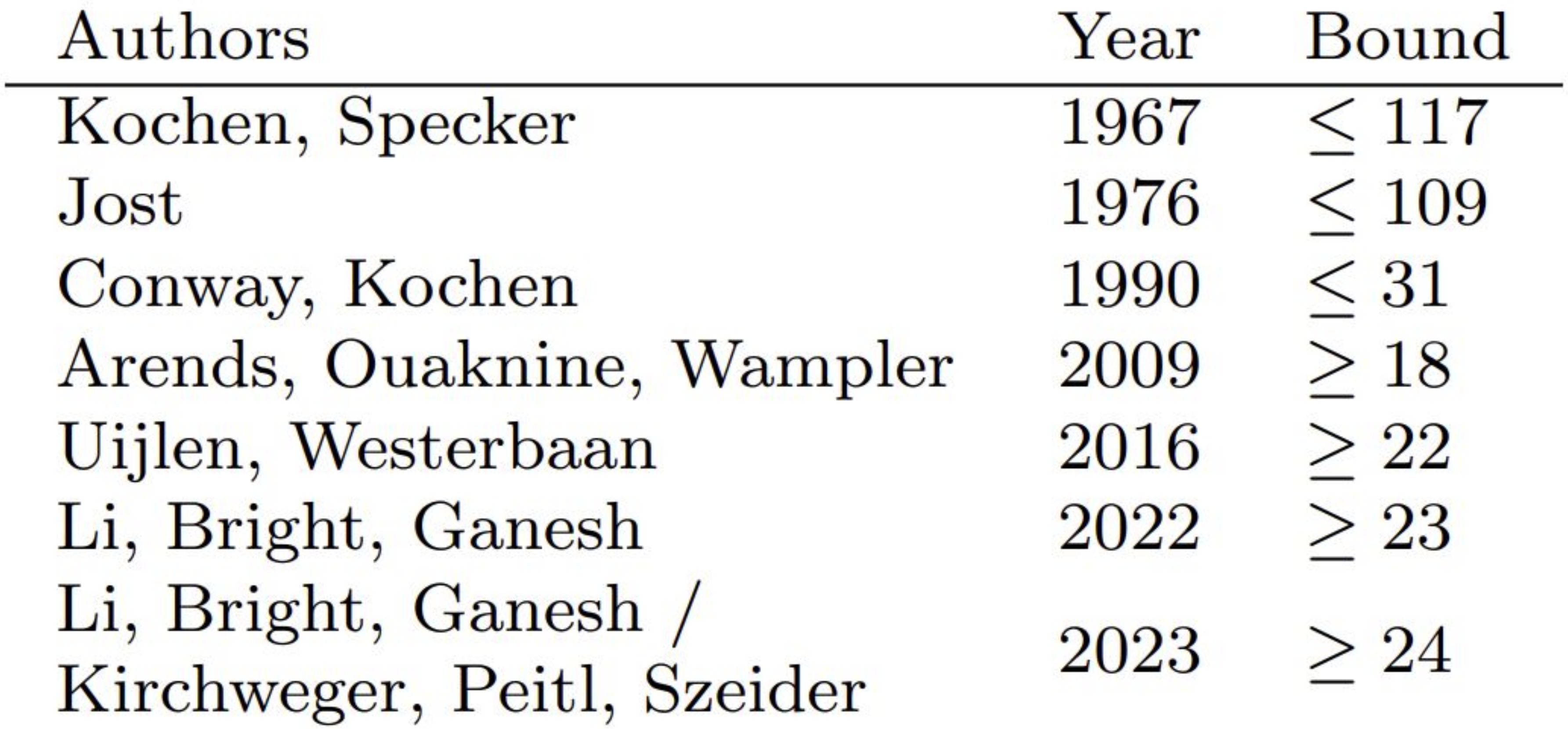
A Kochen-Specker (KS) vector system is a set of 3-dimensional vectors that is not 101-colorable.

The minimum cardinality of such system has been an open problem for over 50 years.



31 vector KS system of Conway and Kochen

Related Work on the KS Problem



Authors	Year	Bound
Kochen, Specker	1967	≤ 117
Jost	1976	≤ 109
Conway, Kochen	1990	≤ 31
Arends, Ouaknine, Wampler	2009	≥ 18
Uijlen, Westerbaan	2016	≥ 22
Li, Bright, Ganesh	2022	≥ 23
Li, Bright, Ganesh / Kirchweger, Peitl, Szeider	2023	≥ 24

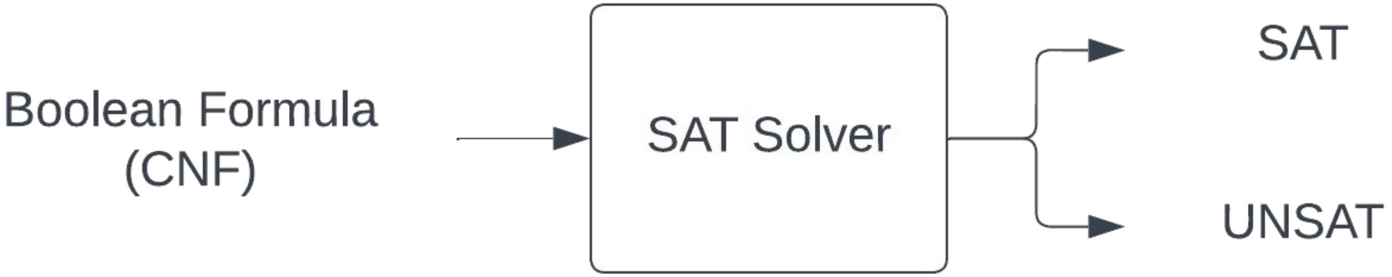
Our Contributions

We improved the lower bound on the size of the KS system from 22 to 24, with a significant speed-up (35,000x) over previous computational approaches by incorporating isomorphism removal using a CAS.

Our approach applies the first ever successful implementation of the satisfiability solver + computer algebra system approach (SAT + CAS) for problems in quantum foundations.

Our work provides the first lower bound in the minimum KS problem with a computer-verifiable proof certificate.

Satisfiability (SAT) solver



A SAT solver is a computer program which aims to solve the Boolean satisfiability problem. It takes Boolean formulas in CNF as input, and returns

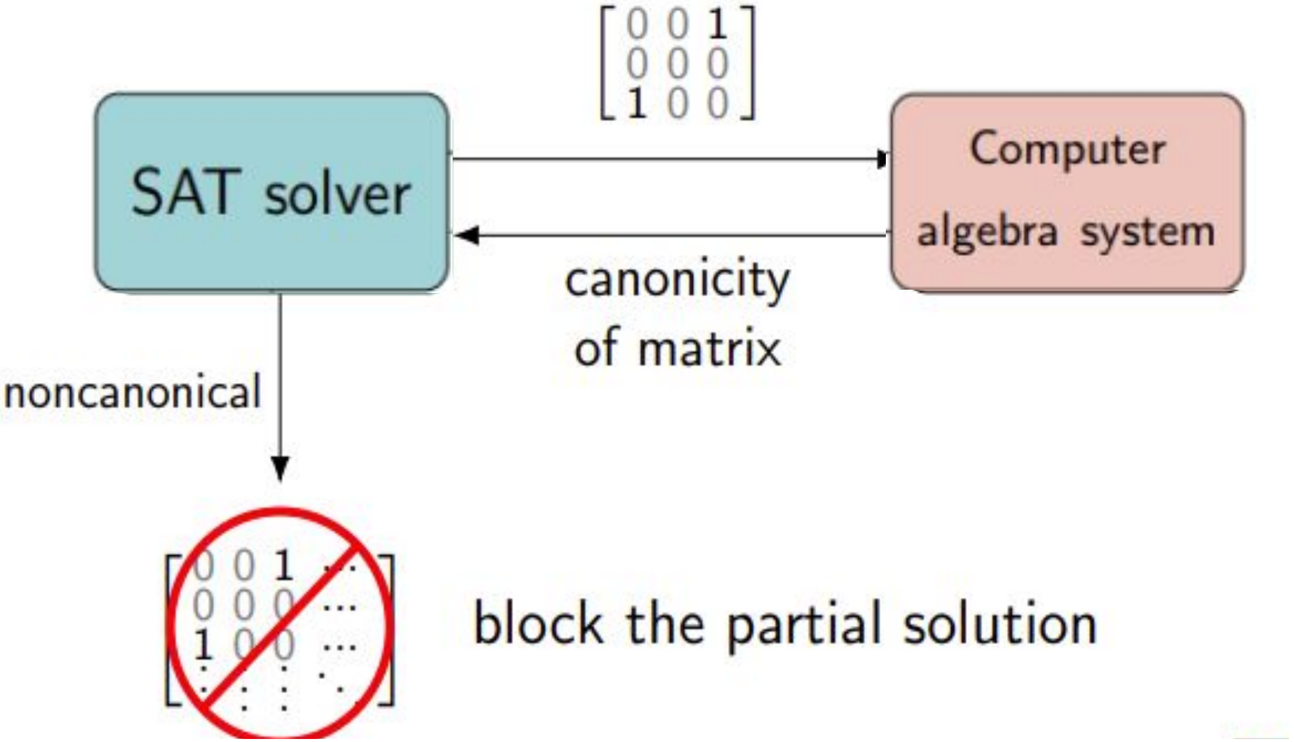
- SAT if it finds a variable assignment that satisfy the input formula
- UNSAT if it can demonstrate that no such assignments exist

Boolean satisfiability is NP-Complete, but SAT solvers are effective for many applications.

Computer Algebra Systems (CASs)

SAT or CAS independently does not work

SAT + CAS



$\begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$
SAT solver
Computer algebra system
canonicity of matrix
noncanonical
$\begin{bmatrix} 0 & 0 & 1 & \cdots \\ 0 & 0 & 0 & \cdots \\ 1 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix}$
block the partial solution

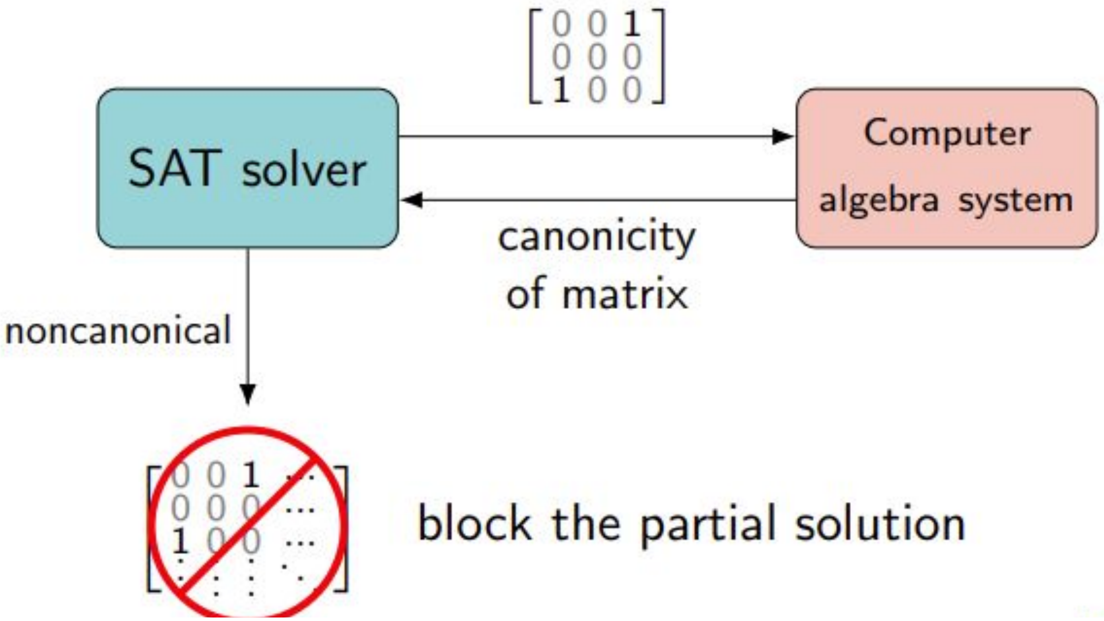
SAT + CAS paradigm

SAT solvers:

- Strength: excellent search capabilities
- Weakness: lack mathematical knowledge

CAS systems:

- Strength: storehouse of mathematical knowledge
- Weakness: lack search capabilities


SAT solver
$\begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$
Computer algebra system
canonicity of matrix
noncanonical
$\begin{bmatrix} 0 & 0 & 1 & \cdots \\ 0 & 0 & 0 & \cdots \\ 1 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix}$
block the partial solution

SAT+CAS = excellent search capabilities + mathematical knowledge

Combinatorial Applications of the SAT + CAS Paradigm

Introduced by Zulkoski, Ganesh et al., and independently by Erika Ábrahám, both in 2015, the SAT + CAS paradigm has made defining contributions in combinatorics and graph theory [1,2,3]:

- Verified Lam's problem and produced the first set of nonexistence certificates
- Verified the smallest counterexample of the Williamson conjecture for the first time
- First independent verification of the Craigen–Holzmann–Kharaghani conjectures about complex Golay pairs up to length 28
- Proved the best known result in the conjecture that every matching of a hypercube extends to a Hamiltonian cycle (Ruskey–Savage conjecture)

[1] Zulkoski, E., Ganesh, V., Czarnecki, K.: MathCheck: a math assistant via a combination of computer algebra systems and SAT solvers. In: Felty, A.P., Middeldorp, A. (eds.) International Conference on Automated Deduction, pp. 607–622. Springer, Cham (2015)
[2] Ábrahám, E.: Building bridges between symbolic computation and satisfiability checking. Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation, pp. 1–6. ACM (2015)
[3]

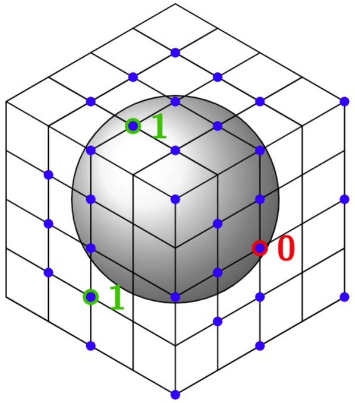
Encoding the KS Problem

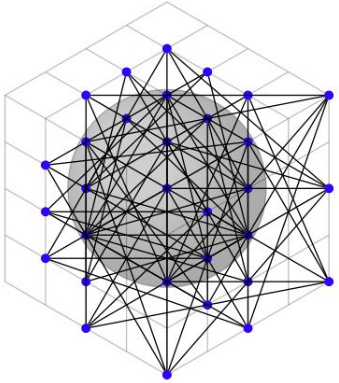
To find a KS system, we want to find graphs *G* such that

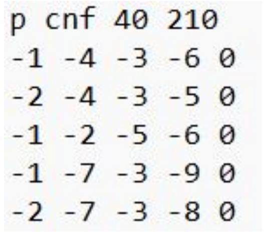
- *G* is non-101-colorable: *G* has no possible 101-coloring
- *G* is embeddable: *G* is an orthogonality graph for a 3-d vector system

In addition, previous research has proven mathematically that *G* satisfies

- Squarefree Constraint: *G* must not contain a square subgraph
- Minimum Degree Constraint: every vertex of *G* must have minimum degree 3
- Triangle Constraint: every vertex is part of at least one triangle subgraph



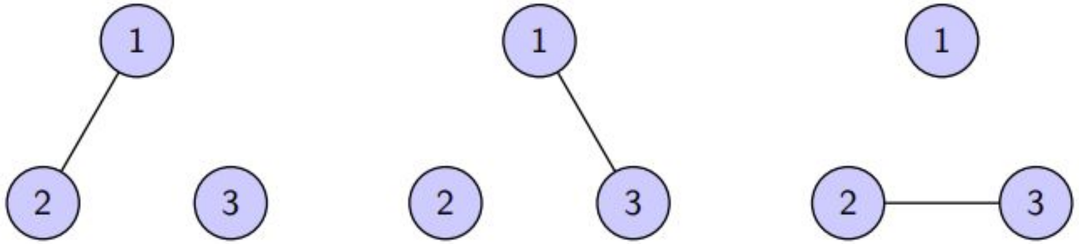




```
p cnf 40 210
-1 -4 -3 -6 0
-2 -4 -3 -5 0
-1 -2 -5 -6 0
-1 -7 -3 -9 0
-2 -7 -3 -8 0
```

Key Insight: Symmetry Breaking in SAT+CAS

The SAT approach outperforms other graph enumeration approach—but the solver generates many isomorphic copies of the same graph.



$$\begin{bmatrix}0 & 1 & 0\\ 1 & 0 & 0\\ 0 & 0 & 0\end{bmatrix} \qquad \begin{bmatrix}0 & 0 & 1\\ 0 & 0 & 0\\ 1 & 0 & 0\end{bmatrix} \qquad \begin{bmatrix}0 & 0 & 0\\ 0 & 0 & 1\\ 0 & 1 & 0\end{bmatrix}$$

Isomorph-free Orderly Generation

When generating combinatorial objects we only care about generating them up to isomorphism.

The notion of canonicity is defined so that:

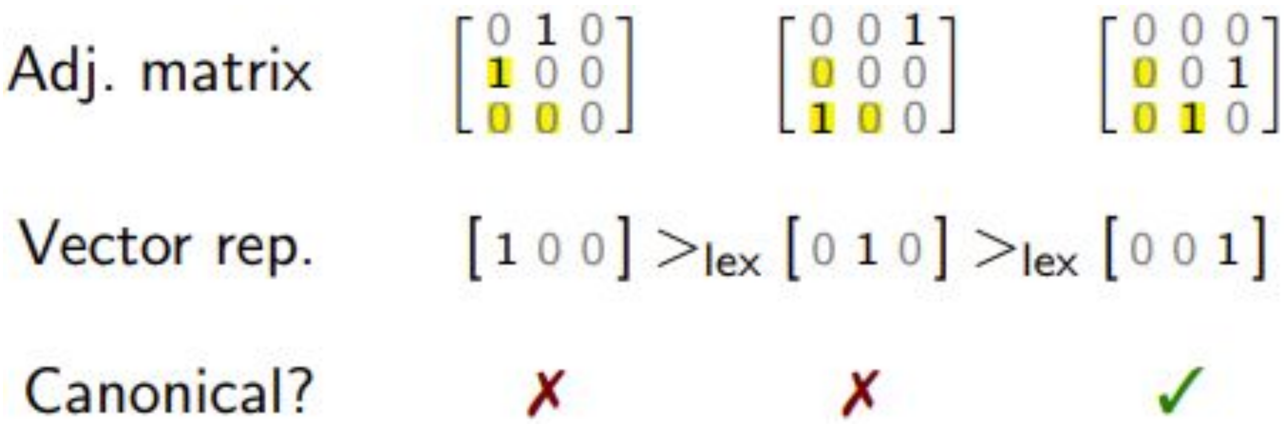
- Every isomorphism class has exactly one canonical representative.
- If an adjacency matrix is canonical then its upper-left submatrix of any size is also canonical.

Developed independently by Faradžev and Read in 1978.

Canonicity Examples

An adjacency matrix is canonical if its “vector representation” is lex-minimal among all matrices in the same isomorphism class.

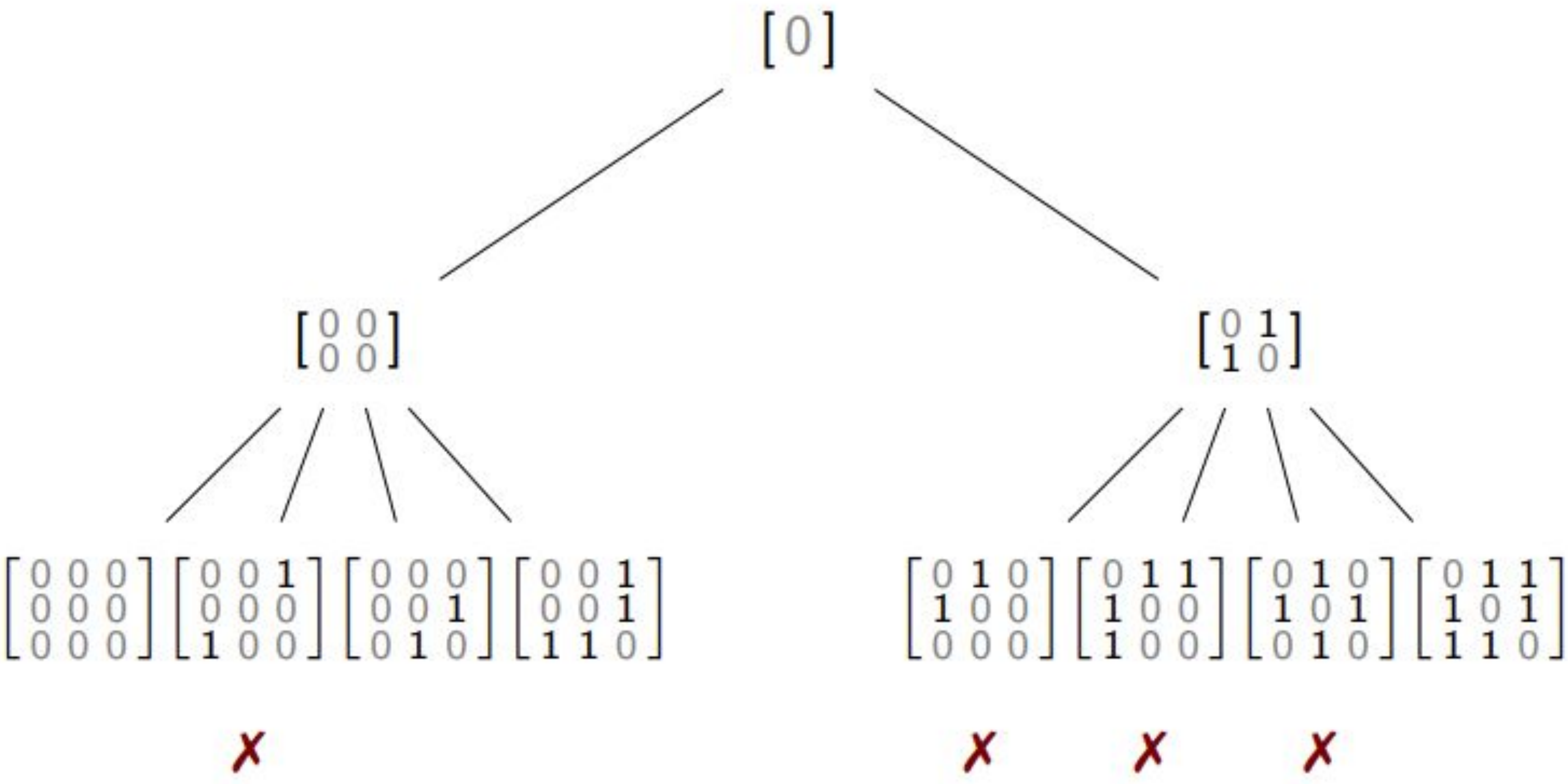
For example,



Adj. matrix	$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$
Vector rep.	$[1\;0\;0] >_{\text{lex}}$	$[0\;1\;0] >_{\text{lex}}$	$[0\;0\;1]$
Canonical?	✗	✗	✓

are isomorphic adjacency matrices but only the last is canonical.

Orderly Generation of Graphs

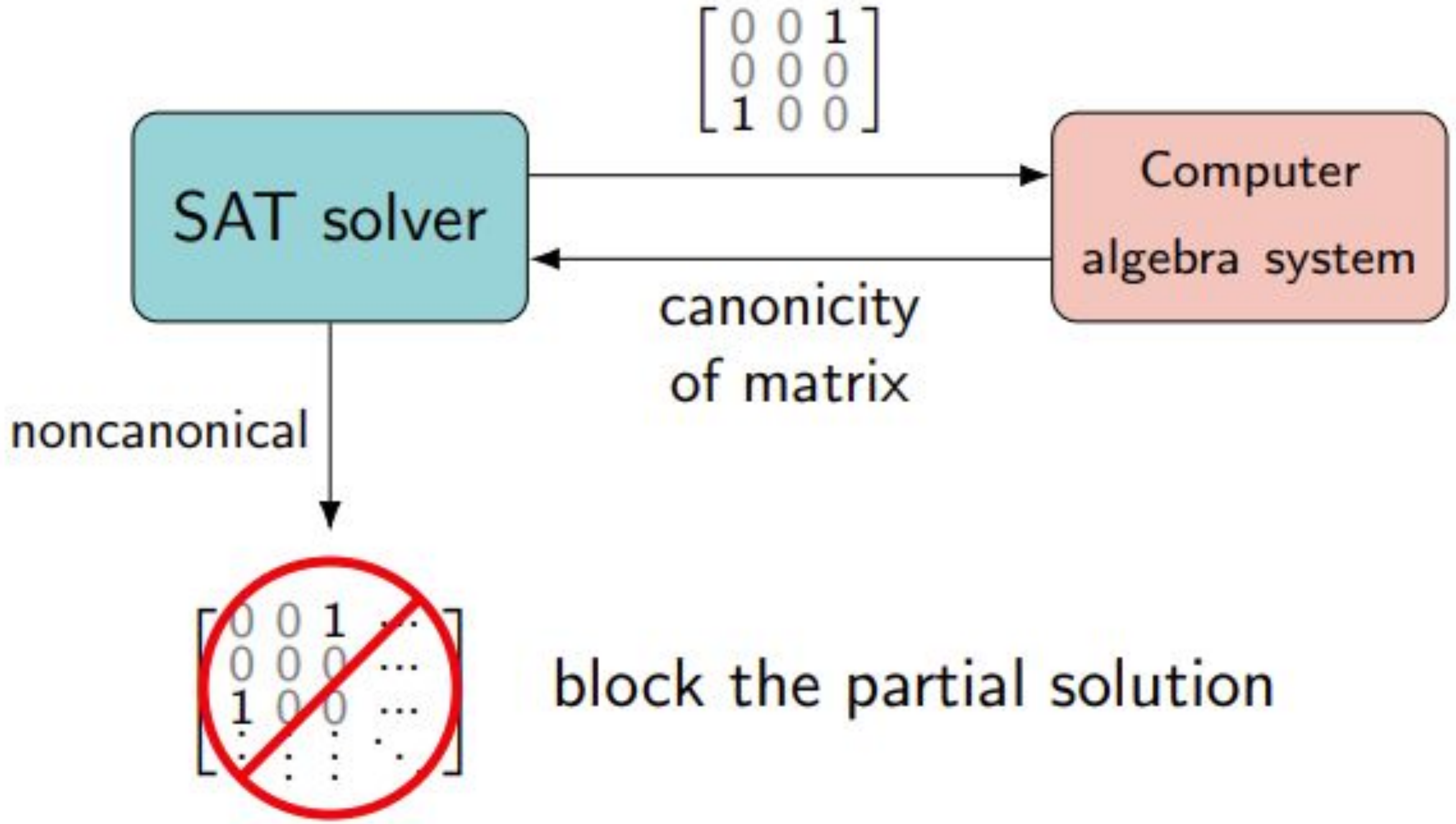


$$\begin{bmatrix} 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

Orderly Generation with SAT Solver



$$\begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

SAT solver

Computer algebra system

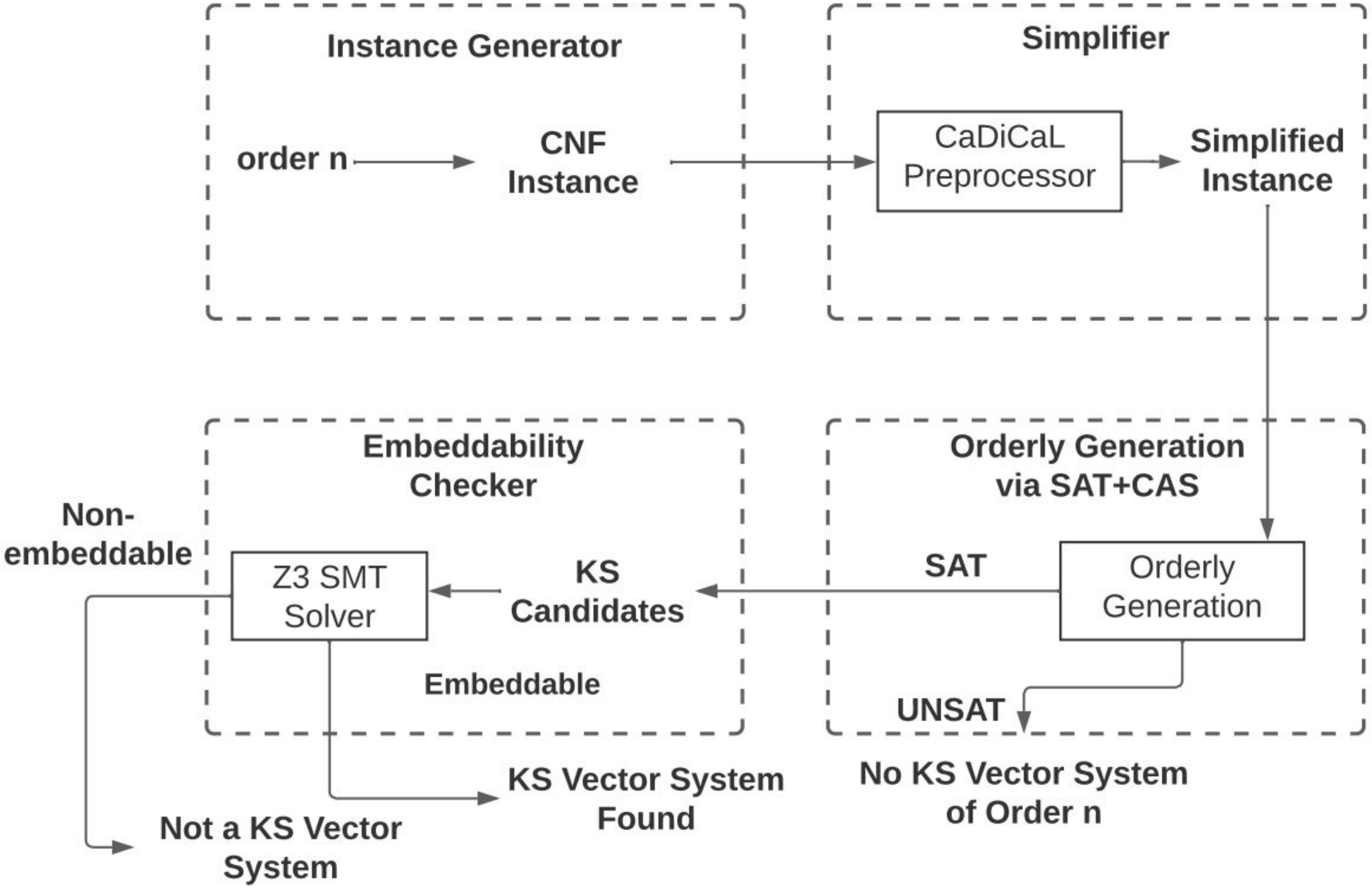
canonicity of matrix

noncanonical

$$\begin{bmatrix} 0 & 0 & 1 & \cdots \\ 0 & 0 & 0 & \cdots \\ 1 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

block the partial solution

A Granular View of the PhysicsCheck Pipeline



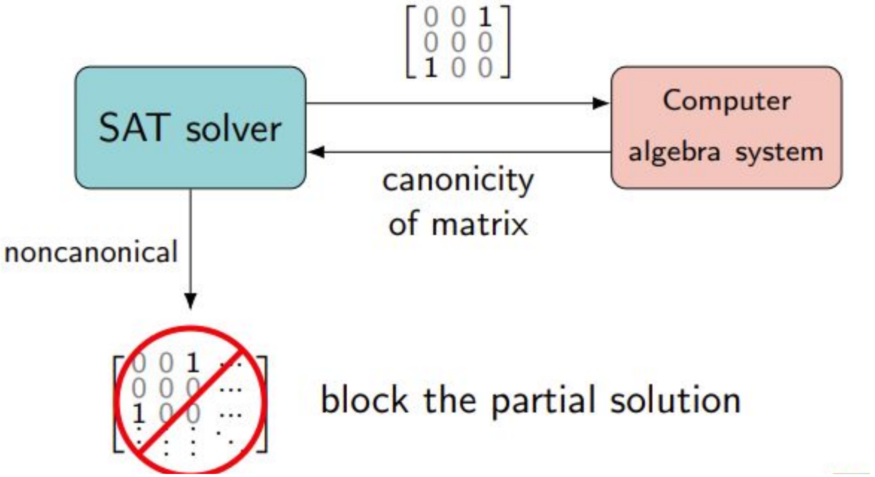
Results

Order	SAT	CAS (nauty)	SAT + CAS	Speedup over SAT	Speedup over CAS
17	10.8 min	25.0 min	0.00 h	8.9x	25.6x
18	53.7 min	395.6 min	0.02 h	161.6x	276.1x
19	6.5 days	6.2 days	0.15 h	834.3x	677.6x
20	timeout	timeout	1.25 h	timeout	timeout
21	timeout	timeout	18.36 h	timeout	timeout
22	timeout	timeout	360.75 h	timeout	timeout
23	timeout	timeout	52619.16 h	timeout	timeout

The order 21 case was resolved in under a day on a single desktop, while the best previous approach used 300 desktops for three months.

Conclusion and a Promising Future

The SAT+CAS paradigm provides exponential speedups over computer algebra or SAT searches. The approach is very general and can be applied to many problems in combinatorics, graph theory, and other areas of mathematics.



Thank you!
brian.li@uwaterloo.ca