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

March 9, 2023

Zhengyu Li[1], Curtis Bright[2], Vijay Ganesh[1]

[1] University of Waterloo
[2] University of Windsor

UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS

University of Windsor

Meet the Team

Zhengyu Li

Master Student
University of Waterloo
Faculty of Mathematics

Curtis Bright

Assistant Professor
University of Windsor
School of Computer Science

Vijay Ganesh

Associate professor
University of Waterloo
Department of ECE
School of Computer Science

The Kochen-Specker Theorem

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

- The SPIN axiom
- The principle of non-contextuality

In order to prove their theorem, Kochen and Specker establish the existence of a KS vector system.

The KS vector system is important for understanding the limitations of classical intuition in describing quantum phenomena.

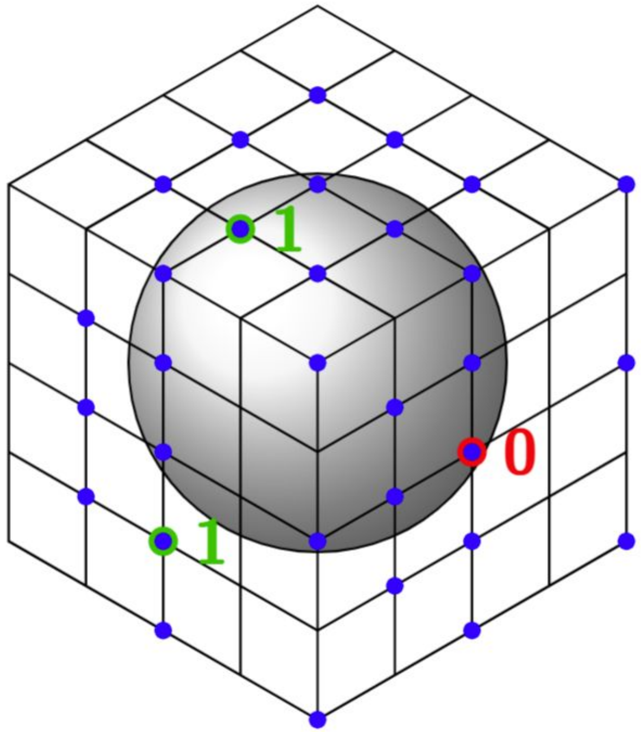
What is a Kochen–Specker System?

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	KS
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

UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS

Our Contributions

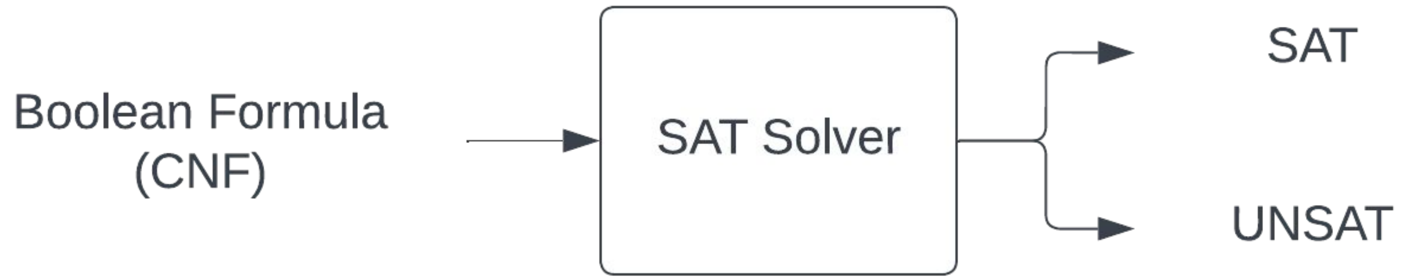
We improved the lower bound on the size of the KS system from 22 to 23, with a significant speed-up (30,000x) over previous computational approaches by incorporating isomorphism removal using a CAS.

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

University of Windsor UNIVERSITY OF WATERLOO FACULTY OF MATHEMATICS

Satisfiability (SAT) solver

SAT + CAS



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)

Maple™

sage

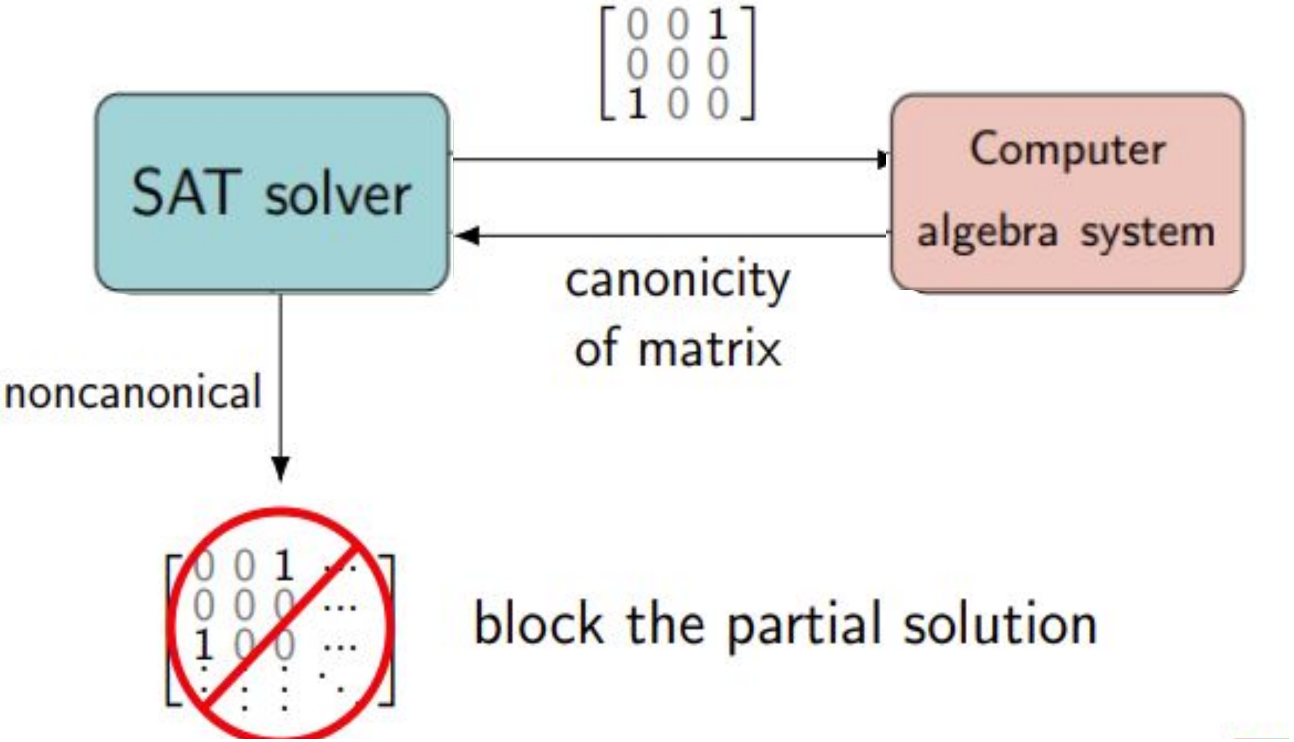
Wolfram Mathematica

nauty and Traces

Brendan McKay and Adolfo Piperno

SAT or CAS independently does not work

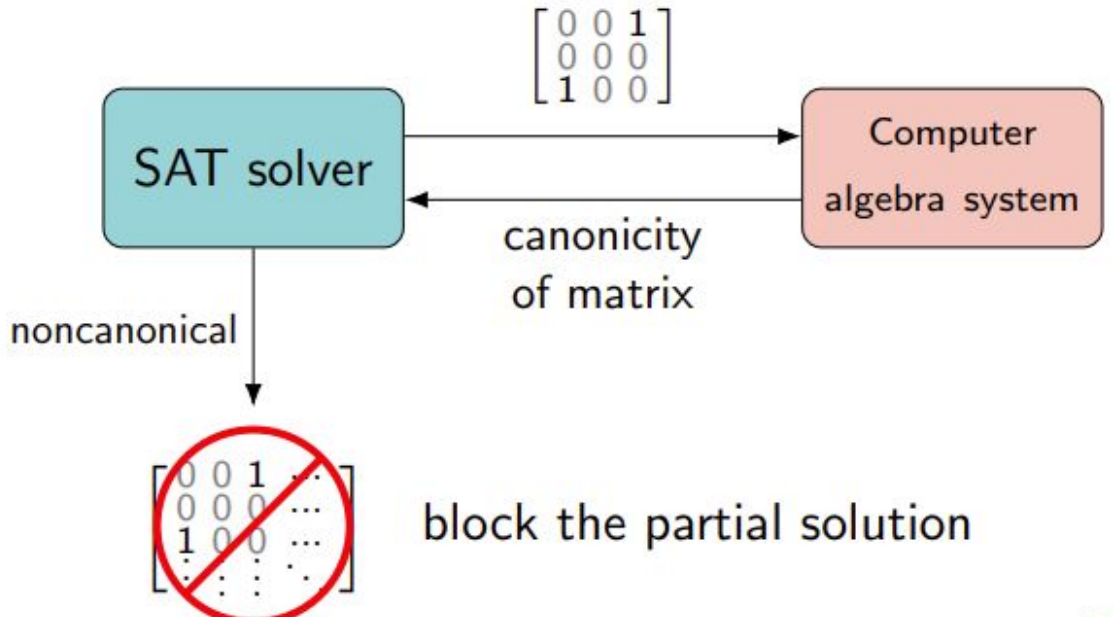
SAT + CAS



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+CAS = excellent search + 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]

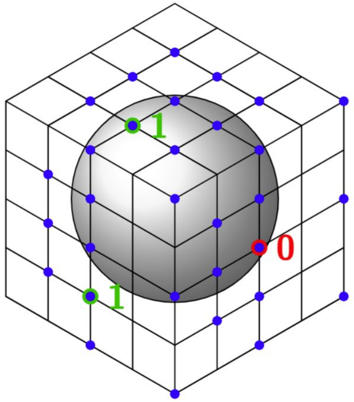
Encoding the KS Problem

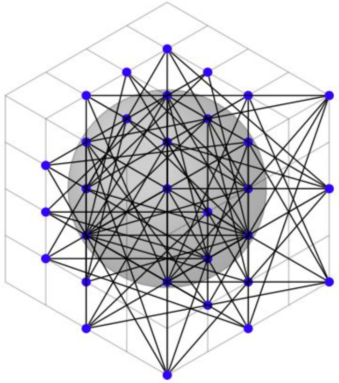
To find a KS system, we want to find graphs G such that

- 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





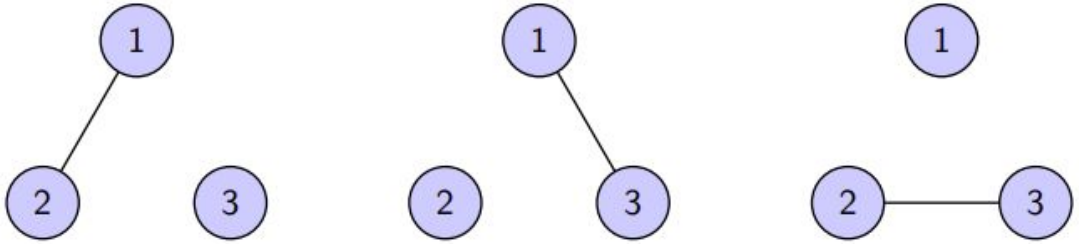
```
p cnf 40 210
-1 -4 -3 -6 0
-2 -4 -3 -5 0
-1 -2 -5 -6 0
-1 -7 -3 -9 0
-2 -7 -3 -8 0
```


University of Windsor
UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS

Key Insight: Symmetry Breaking in SAT+CAS

Orderly Generation

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



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

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.

University of Windsor UNIVERSITY OF WATERLOO FACULTY OF MATHEMATICS

Canonicity Examples

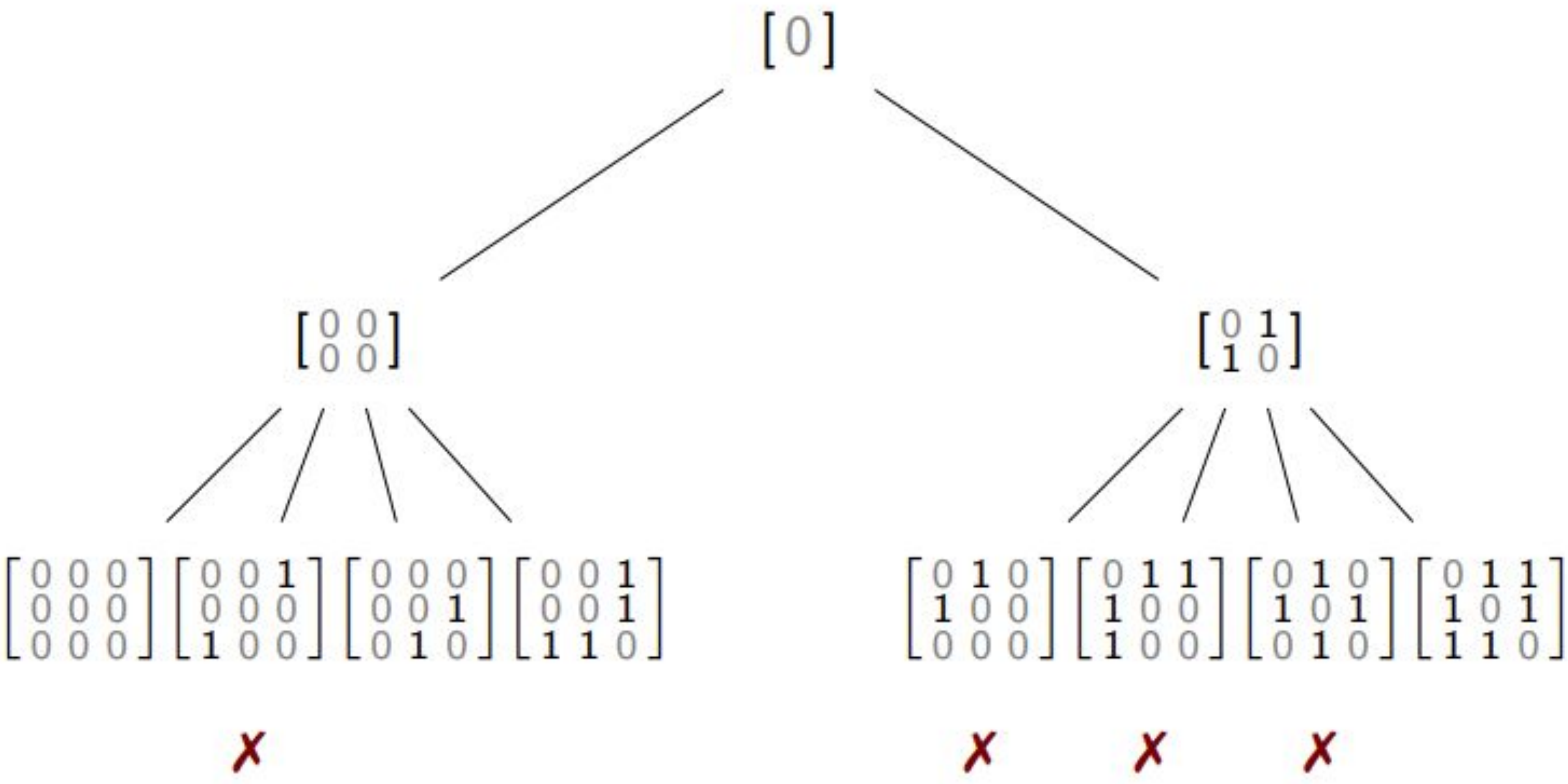
An adjacency matrix is canonical if its “vector representation” is lex-minimal among all matrices in the same isomorphism class.

For example,

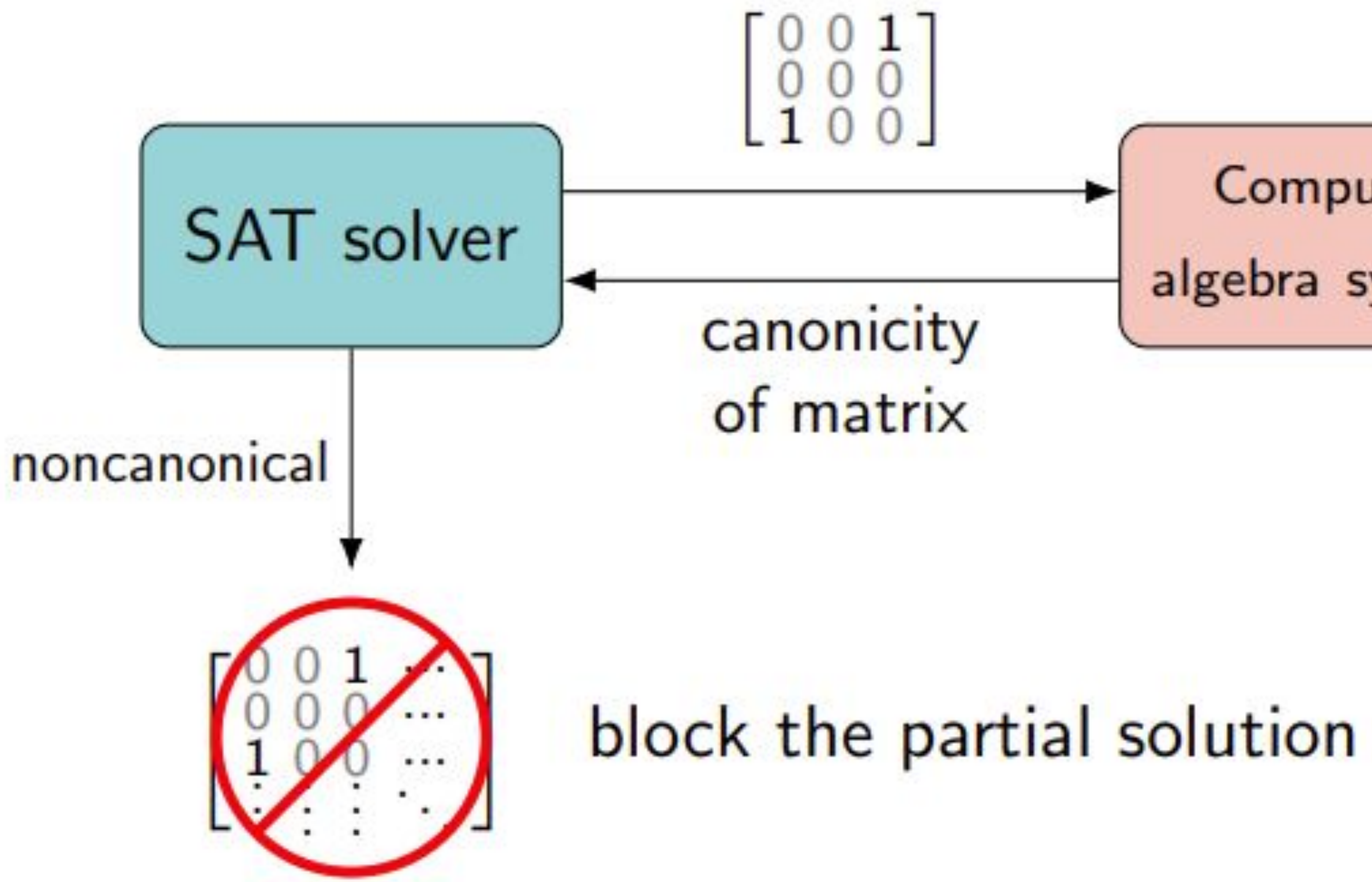
Adj. matrix	$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$
Vector rep.	$[1\ 0\ 0] >_{\text{lex}}$	$[0\ 1\ 0] >_{\text{lex}}$	$[0\ 0\ 1]$
Canonical?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

are isomorphic adjacency matrices but only the last is canonical.

Orderly Generation of Graphs



Orderly Generation with SAT Solver



Results

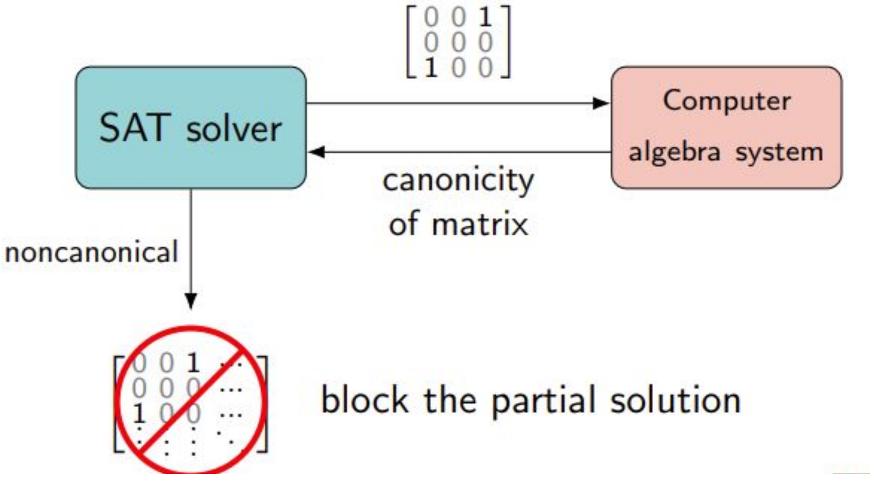
Order	SAT	CAS (nauty)	SAT + CAS	Speedup over SAT	Speedup over CAS
17	10.8 min	25.0 min	0.3 min	36.1x	83.2x
18	53.7 min	395.6 min	1.7 min	31.6x	232.7x
19	6.5 days	6.2 days	13.8 min	675.9x	639.7x
20	timeout	timeout	109.4 min	timeout	timeout
21	timeout	timeout	1383.6 min	timeout	timeout
22	timeout	timeout	19 days	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.

University of Windsor
UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS

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

University of Windsor
UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS