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

May 1, 2023

Brian 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

CDCL(CAS) paradigm

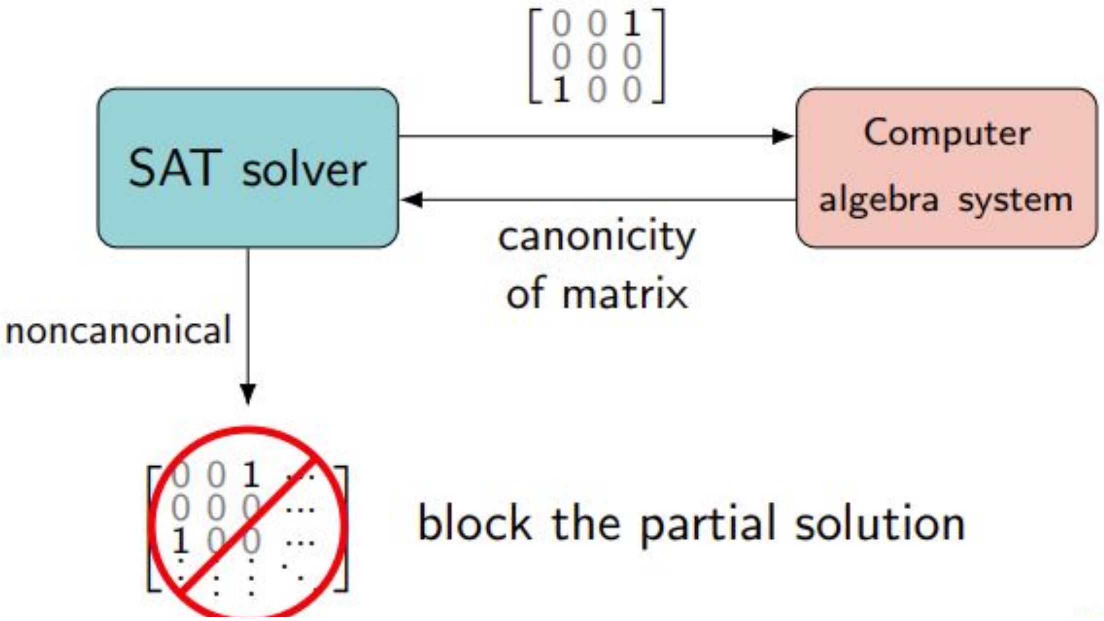
SAT + CAS

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

University of Windsor UNIVERSITY OF WATERLOO FACULTY OF MATHEMATICS

Applications of the SAT + CAS Paradigm

SAT + CAS

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

- Verified Lam's problem and produced the first set of nonexistence certificates
- Found 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)

Satisfiability (SAT) + Computer Algebra Systems (CAS)

Introduction

review articles

DOI:10.1145/3500921

The science of less-than-brute force.

BY CURTIS BRIGHT, ILIAS KOTSIREAS, AND VIJAY GANESH

When Satisfiability Solving Meets Symbolic Computation

MATHEMATICIANS HAVE LONG been fascinated by objects that exhibit exceptionally nice combinatorial properties. However, it is often difficult to determine whether objects satisfying a given combinatorial property exist. Sometimes, the only feasible method of definitively answering the question of existence is simply to perform a systematic search. A famous example of this is the proof of the *four-color theorem*—the notion that four colors suffice to color the regions of a planar map with adjacent regions colored differently.[3] The theorem has been known to be true since 1977, but every known proof relies on computer calculations in an essential way. Mathematical arguments are used to reduce the search for counterexamples to a finite number of cases, and the cases are then exhaustively checked using a custom-written computer program to rule out any counterexamples.

Independently, computer scientists have made significant progress over the last 50 years on developing general-purpose programs that can automatically solve many kinds of mathematical problems. *Satisfiability solving* and *symbolic computation* are two important branches of computer science that each specialize in solving mathematical problems. Both fields have long histories and have produced impressive tools—satisfiability (SAT) solvers in the former and computer algebra systems (CASs) in the latter. Originally, SAT solvers were designed to solve problems in logic, and CASs were tools to manipulate and simplify algebraic expressions. As we will see, these tools have since found an abundance of new applications outside of these original domains.

Despite their common specialization in solving mathematical problems, the SAT and CAS communities have developed independently of each other.[1] Broadly speaking, the SAT community has focused on effective search methods, while the CAS community has focused on effective mathematical algorithms. Recently, these two communities have started to collaborate in crossover initiatives like the SC-square project.[a,2] Since the insights of these communities are largely complementary, bringing them together has resulted in new solutions to problems that were out-of-reach of either community separately and has produced advances in problems involving nonlinear real arithmetic,[13] linear integer arithmetic,[12] and Boolean polynomials,[28] to name a few. In this overview, we focus on our own contribution to this ongoing project—a hybrid SAT and CAS system called MathCheck[b] that we have applied to mathematical problems in graph theory,[45] finite geometry,[5] combinatorics,[9] and number theory.[c,11]

Satisfiability solving. A SAT solver is a program that solves the satisfiability problem from Boolean logic—given a formula in conjunctive normal form, is there an assignment to its variables that makes the expression true? At first glance, SAT solvers seem disconnected from the kinds of problems that most mathematicians and engineers care about. However, stunning progress in applied SAT solving over the last several decades[43] has led to a surprising diversity of applications for SAT solvers—

IMAGE BY ZTARSTOCK

a www.sc-square.org

b www.uwaterloo.ca/mathcheck

c For more applications of the SAT+CAS paradigm see the overview article[17] appearing in a special issue of the *Journal of Symbolic Computation* devoted to SAT and CAS synergies.

» key insights

- Satisfiability (SAT) solving and symbolic computation are fields of computer science with distinguished histories that have developed mostly independently.
- Advances in SAT solving and computer algebra systems (CASs) have led to the development of tools that can solve mathematical search problems significantly larger than ever before—and in a faster, more verifiable way.
- Hybrid "SAT+CAS" systems combine the efficient search and learning routines of SAT solvers with the efficient mathematical algorithms and expressiveness of CASs in order to achieve the best of both worlds.

Our Main Result: SAT+CAS for Minimal Kochen-Specker Problem

The first ever successful implementation of the satisfiability solver + computer algebra system approach (SAT + CAS) for problems in quantum foundations, namely, the minimal Kochen-Specker vector system problem.

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.

Quantum Foundations: Goals and Problems

- “Explain” counter-intuitive aspects of Quantum Mechanics (QM) such as non-locality, contextuality, complementarity, entanglement,…
- Answer questions such as the measurement problem
- Attempts include Copenhagen Interpretation, Hidden Variable theories
- Axiomatize QM in logic and study its meta properties, e.g., soundness, relationship to classical logic, proof systems etc.

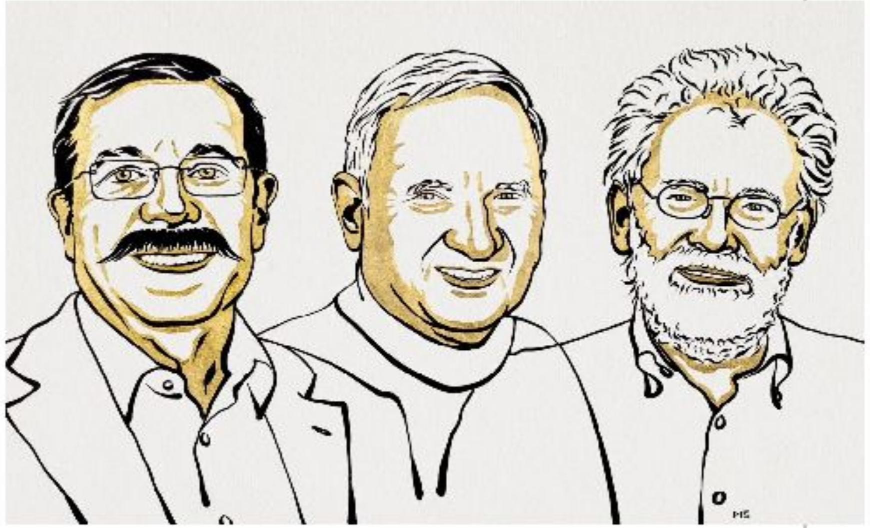
Quantum Foundations

Nobel Prize in Physics

The 2022 physics laureates

The Nobel Prize in Physics 2022 was awarded to Alain Aspect, John F. Clauser and Anton Zeilinger "for experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science".

Their results have cleared the way for new technology based upon quantum information.



Ill. Niklas Elmehed © Nobel Prize Outreach

Did you know?

The Kochen-Specker and Free-Will Theorems

KS Theorem

The Kochen-Specker (KS) Theorem states that there is a contradiction between the SPIN axiom of standard quantum mechanics and the assumption of non-contextuality [3]. (More precisely, there is a contradiction between empirical predictions of QM and the following three properties one assumes all systems must possess: value-definiteness + non-contextuality + one-one Hilbert correspondence.)

The Free Will theorem, proposed by John Conway and Simon Kochen, is a result in quantum mechanics that challenges determinism. The theorem is based on and extends the Kochen-Specker theorem, which shows the limits of our ability to know the properties of a quantum system.

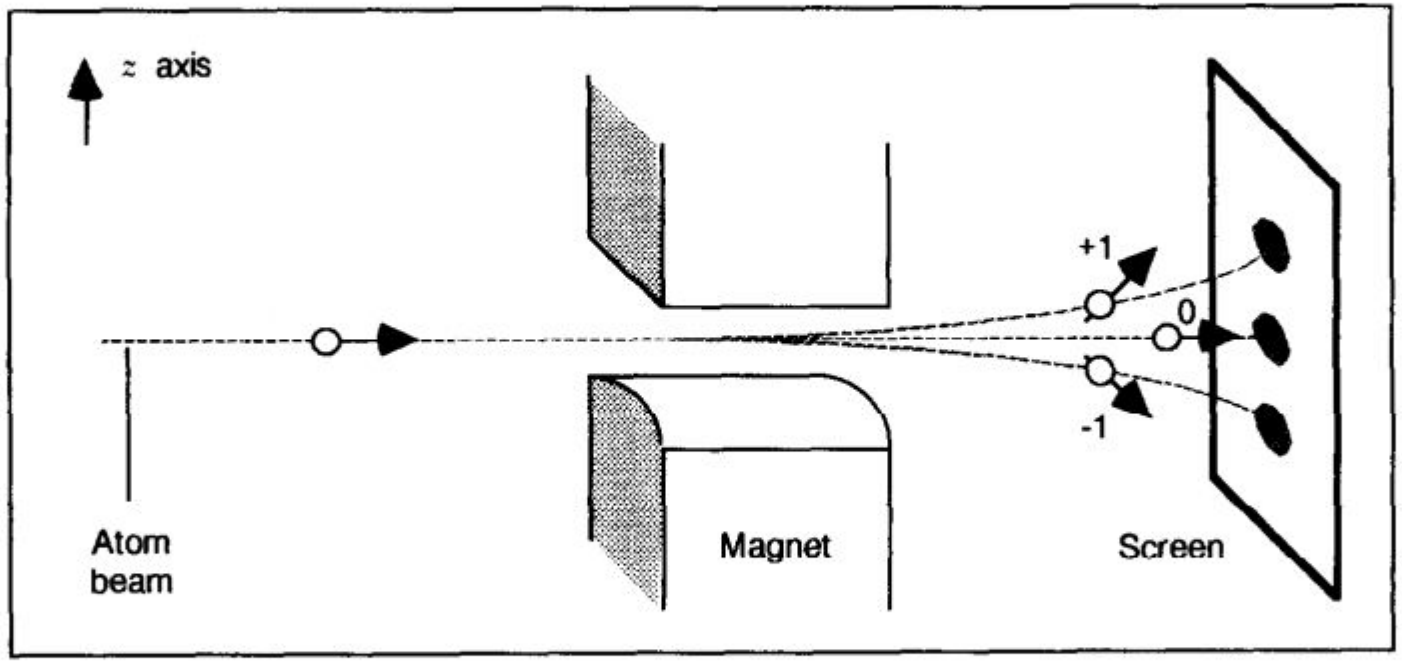
[3] Carsten Held. The Kochen-Specker Theorem. In Edward N. Zalta, editor, The Stanford Encyclopedia of Philosophy. Metaphysics Research Lab, Stanford University, Spring 2018 edition, 2018.

Spin of a Particle

One of the central ideas of quantum mechanics is the notion of spin. Certain subatomic particles have spin. Given a direction, a particle can spin up (positive), down (negative), or not at all.

Observing SPIN - The Stern–Gerlach Experiment (1922)

We can observe the particle spinning by performing such experiment.



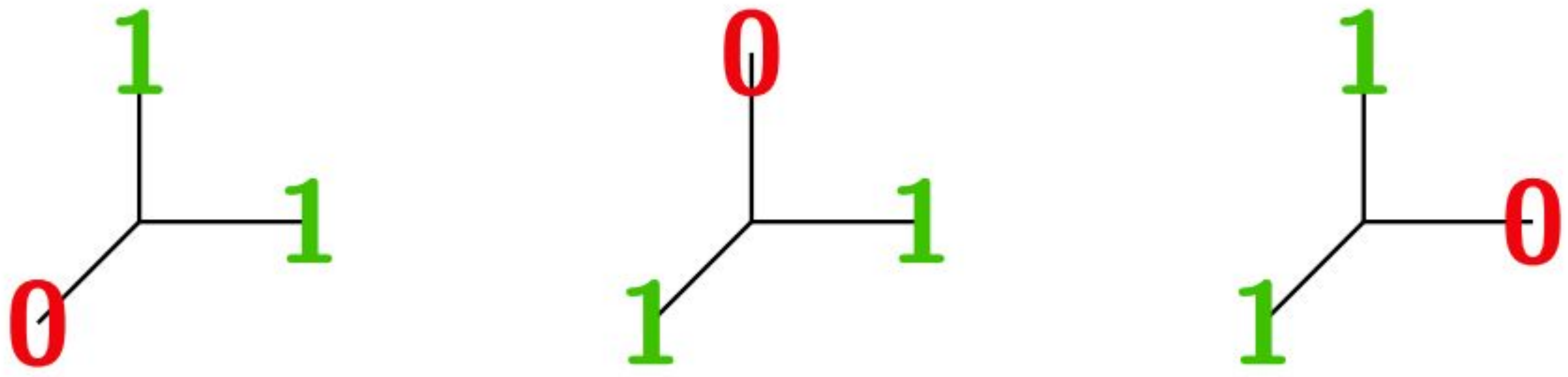
The spin of the atom (in the direction of the field) is +1, −1, or 0.

The Kochen–Specker Experiment

Measure the squared spin of a SPIN-1 particle in three mutually orthogonal directions.

The SPIN Axiom

- The squared spin of spin-1 particles measured along three orthogonal directions is zero in exactly one of these directions.
- Antipodal directions have the same squared spin.



What is Non-Contextuality?

Intuitively, non-contextuality asserts that if a QM system possesses a property (value of an observable), then it does so independently of any measurement context, i.e., independently of *how* that value is eventually measured.

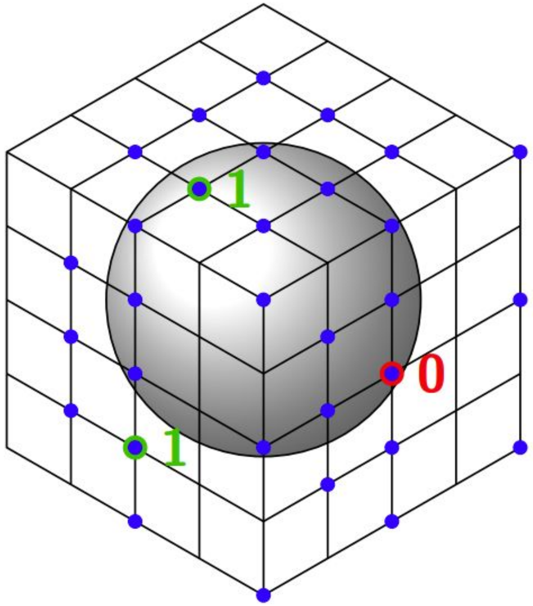
The KS theorem asserts that any non-contextual hidden variable theory cannot reproduce the predictions of QM.

Put differently and informally, the act of measurement creates properties/reality as we understand it. Prior to measurement, QM system don't have any fixed properties, i.e., they are in a superposition of all possible values of an observable.

University of Windsor UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS

Recap: The Kochen–Specker Theorem

There is a contradiction between the SPIN axioms and non-contextuality. It is impossible to assign {0, 1} values to the following 31 vectors in a way that does not violate the SPIN axiom. The particle cannot have a predetermined spin in every direction. [Kochen & Specker 1967]



31 vector KS system of Conway and Kochen, 1990.

University of Windsor
UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS

Intuition behind the KS Theorem

- If the North pole direction does not have spin (0), then the South pole direction also lacks spin. Then all directions along the equator must have spin 1 (a).
- Assign the direction slightly to the right of the North pole as 0 (b) and continue doing so until we reach (d).
- It's impossible to continue this process until every point on the sphere is assigned either 0 or 1.

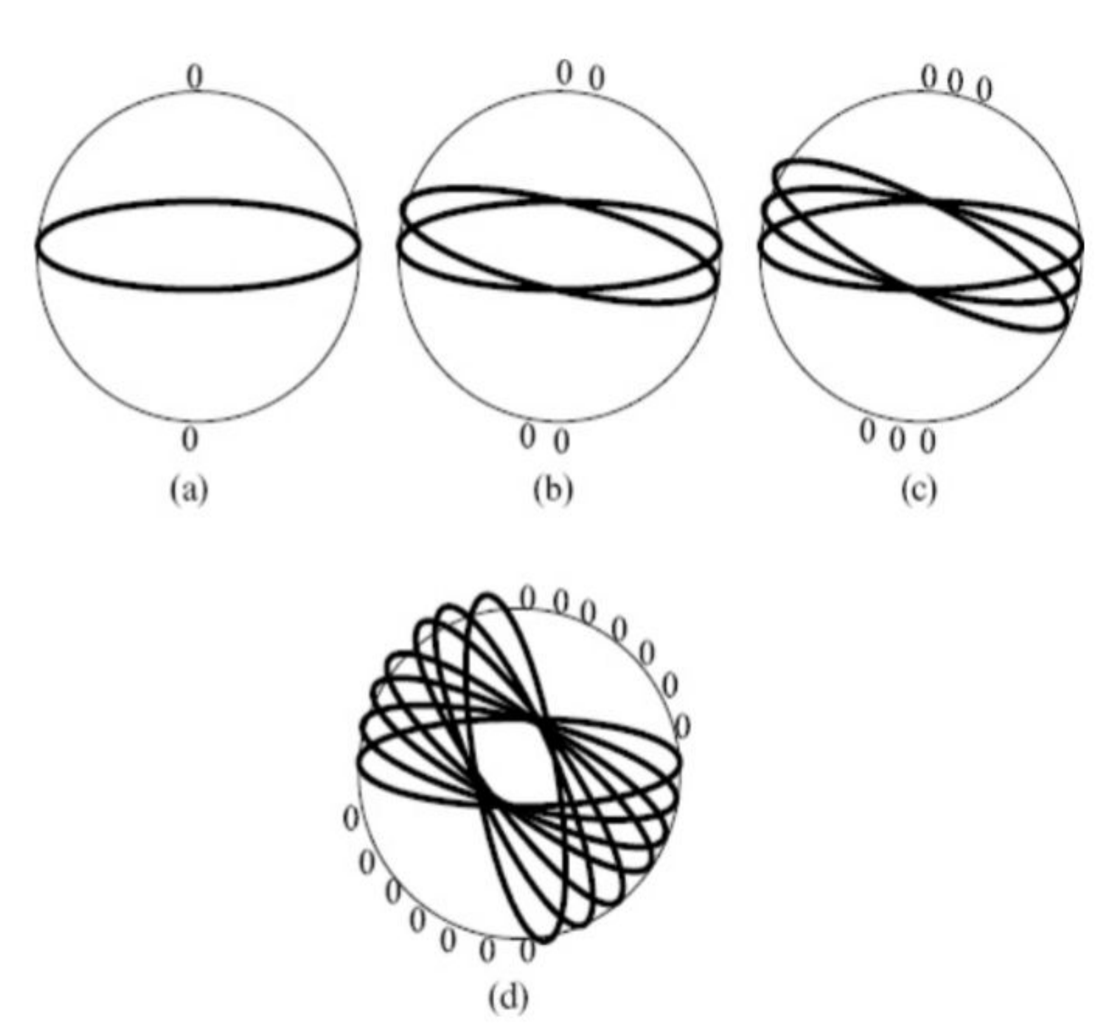


FIgure 7.17 from The Outer Limits of Reason
by Noson S. Yanofsky

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

Table: A history of the bounds on the size of the minimum KS system.

Converting SPIN axiom to SAT via Graph Colorability

Encoding

The squared spin components of a spin-1 particle are 1, 0, 1 in these three directions.

Thus, the observable corresponding to the question “is the squared spin 1?” measured in three mutually orthogonal directions will always produce no in exactly one direction and yes in the other two orthogonal directions in 3-dimensional Euclidean space.

Satisfying the SPIN axiom is equivalent to being 101-colorable:

- Two adjacent vertices are not both assigned to 0.
- Three mutually adjacent vertices are not all assigned to 1.

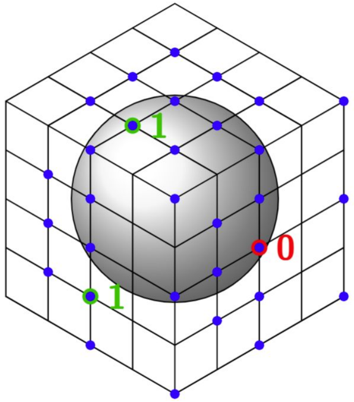
Encoding the KS Problem

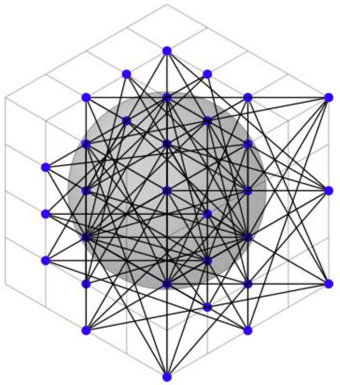
To find a KS system, we want to find graphs G such that

- 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



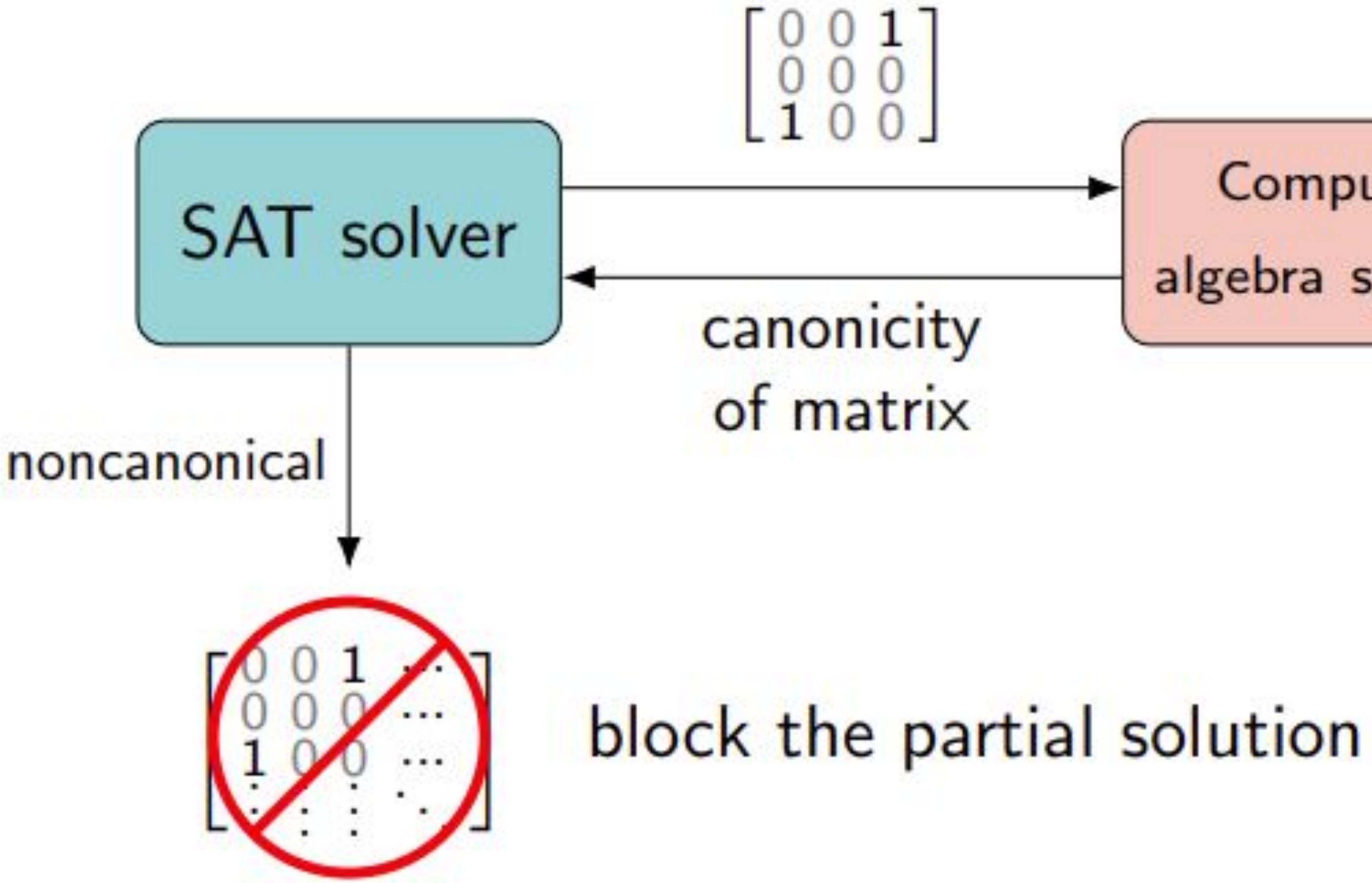


```
p cnf 40 210
-1 -4 -3 -6 0
-2 -4 -3 -5 0
-1 -2 -5 -6 0
-1 -7 -3 -9 0
-2 -7 -3 -8 0
```


University of Windsor
UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS

SAT+CAS Solver

Orderly Generation



SAT Symmetry Breaking

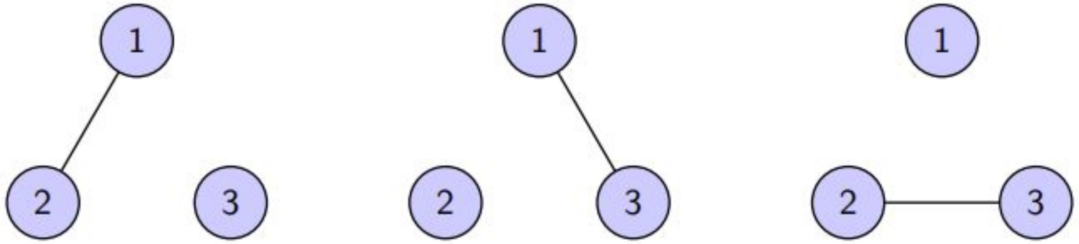
A SAT approach outperformed the previously used graph enumeration approach. However, a SAT solver generates many isomorphic copies of the same graph.

Thus, we combine SAT with isomorph-free exhaustive generation (also previously used to solve Lam's problem) [Bright, Cheung, Stevens, Kotsireas, and G. 2021].

[4] C. Bright, K. Cheung, B. Stevens, I. Kotsireas, V. Ganesh. A SAT-based Resolution of Lam's Problem. AAAI 2021.

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.



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

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.

Canonicity Examples

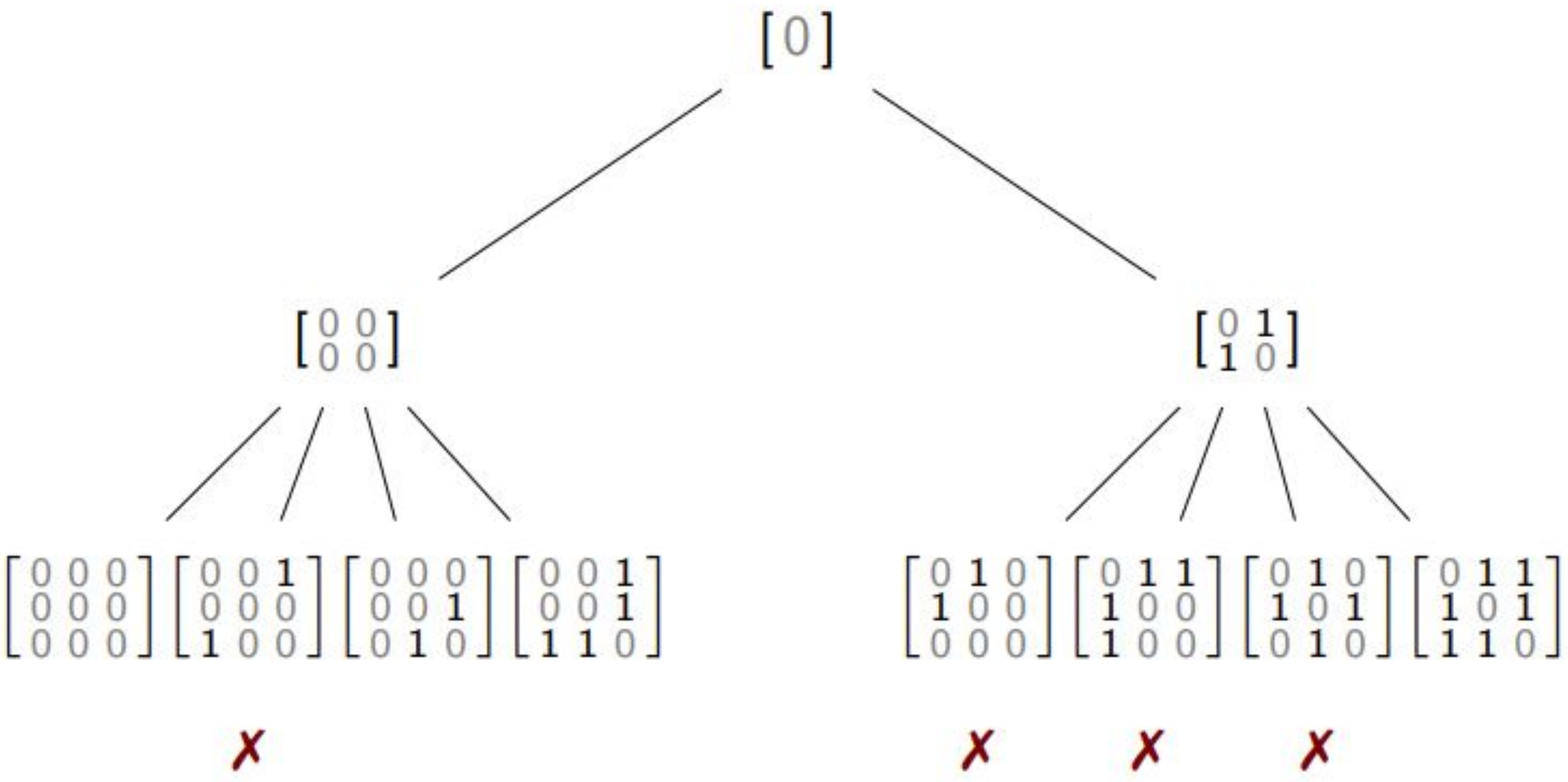
An adjacency matrix is canonical if its “vector representation” is lex-minimal among all matrices in the same isomorphism class.

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 in Practice

Each canonical test is independent, making the method easy to parallelize.

Verifying a matrix is non-canonical is often fast - it requires finding a single permutation of the vertices giving a lex-smaller matrix.

SAT and Isomorph-free Generation

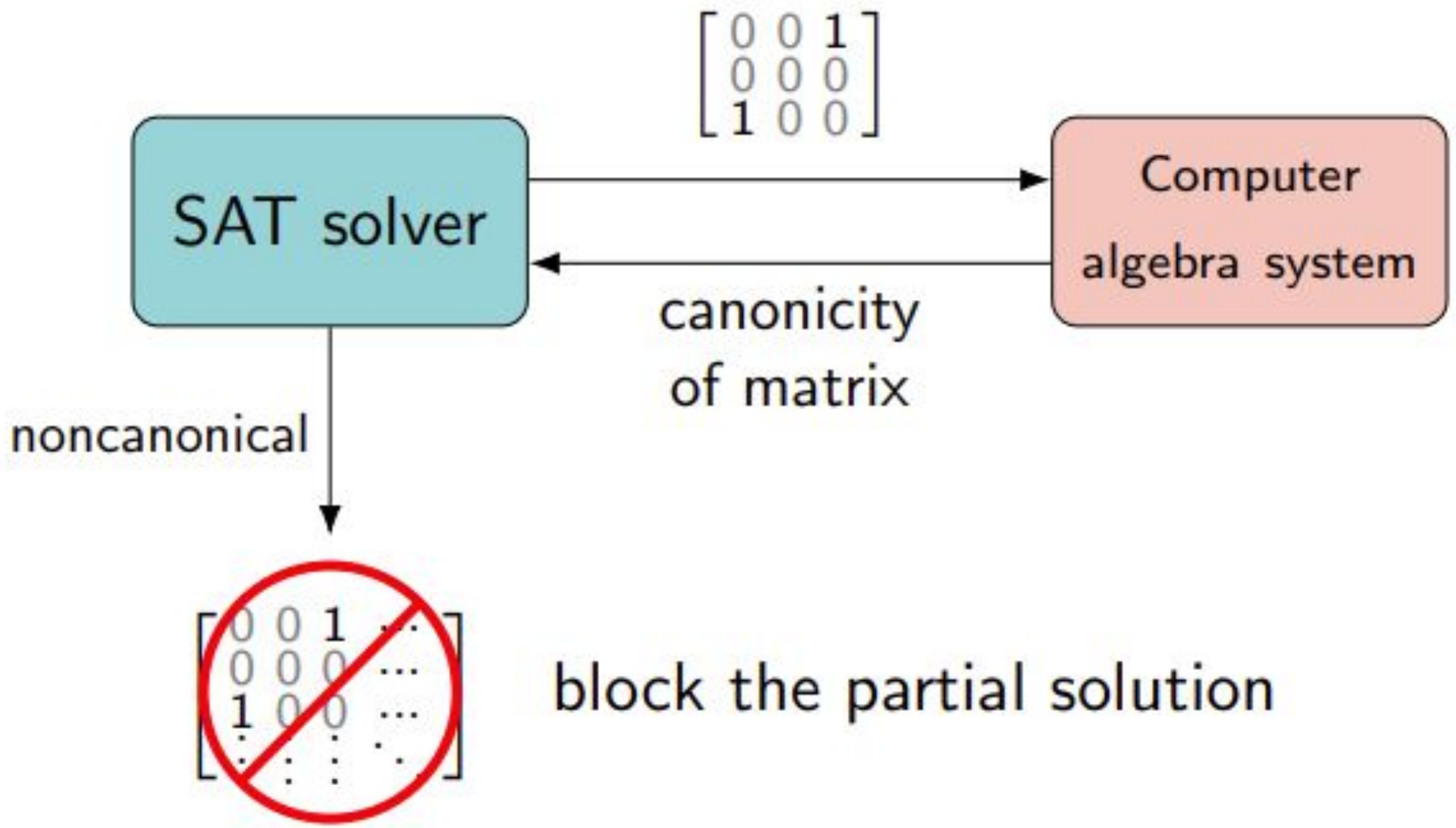
Orderly Generation

Only recently have there been attempts at combining isomorph-free generation and SAT solving. [Junttila, Karpa, Kaski, and Kohonen 2020. Savela, Oikarinen, and Jarvisalo 2020. Kirchweger and Szeider 2021]

This is perhaps a result of the historical separation between the SAT and symbolic computation communities. We will now discuss applying orderly generation and SAT to the minimum Kochen–Specker problem.

University of Windsor
UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS

Orderly Generation with SAT Solver



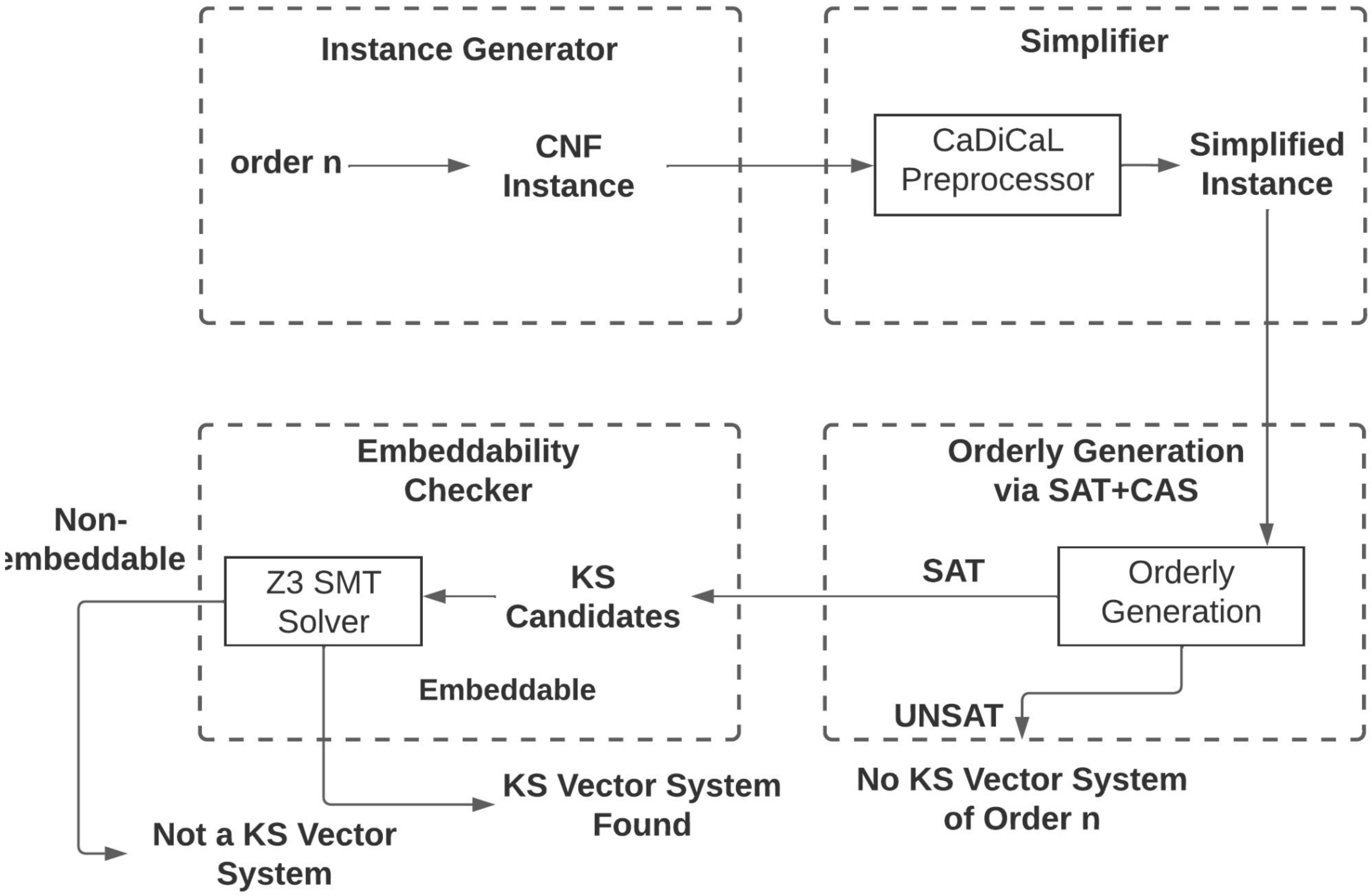
Implementation – Cube-and-Conquer

The cube-and-conquer satisfiability solving paradigm was developed to solve hard combinatorial problems.

- A "cubing solver" splits a SAT instance into a large number of distinct sub-problems specified by cubes-formulas.
- For each cube a "conquering solver" solves the original instance under the assumption that the cube is true.

For large orders, parallelization is applied by dividing the instance into smaller subproblems using the cube-and-conquer approach. During the splitting, cube-and-conquer finds the next variable that splits the search space the most evenly.

Pipeline Overview



University of Windsor
UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS

Verification

Implementation

SAT: We have enabled DRAT proof logging in the SAT solver so that certificates are generated.

CAS: a CAS-derived permutation provides a witness that the blocked matrix is non-canonical.

We used a slightly-modified DRAT-trim (to trust CAS derived clauses) to verify the correctness of the DRAT proof and a permutation-applying Python script to verify its CAS derived clauses.

We have certified the results up to order 21 so far and the original uncompressed proofs are about 200GB in total.

Results

Order	SAT only	CAS only (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	N/A	N/A	109.4 min	N/A	N/A
21	N/A	N/A	1383.6 min	N/A	N/A
22	N/A	N/A	19 days	N/A	N/A

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. **Our method is 30,000x more efficient** on the same hardware than the previous best approach by Uijlen and Westerbaan 2016.

University of Windsor
UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS

Conclusion: SAT+CAS for Problems in Quantum Foundations

- We improve the lower bound over the minimum KS vector system problem and the **search efficiency by 30,000x**.
- We provide a rigorous verification of our result via generation of DRAT proofs.
- We demonstrate the benefits of the SAT + CAS paradigm for a problem in quantum foundations, showing that it is more effective and less error-prone as we uncover inconsistencies with previous result by Uijlen and Westrebaan 2016.
- Future directions: heuristic search, programmatic encoding of non-colorability constraints

University of Windsor

UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS