SAT+CAS:

A Powerful New Combinatorial Search Method

Curtis Bright
University of Waterloo

Ottawa–Carleton Combinatorics & Optimization Seminar
October 5, 2018

SAT:

Boolean satisfiability problem

SAT:

Boolean satisfiability problem

SAT solvers: Glorified brute force

Freakish 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.

Freakish 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.

Examples

- Scheduling
- Dependency resolution
- Microprocessor verification
- Solving puzzles like Sudoku
- Finding combinatorial objects

Limitations of SAT solvers

Even though SAT solvers can solve some complicated problems with millions of variables they fail on some trivial tiny problems.

Limitations of SAT solvers

Even though SAT solvers can solve some complicated problems with millions of variables they fail on some trivial tiny problems.

Example

Have a SAT solver to try to find a way to put 20 pigeons into 19 holes such that no hole contains more than one pigeon...

CAS:

Computer algebra system

CAS:

Computer algebra system

Mathematical expression manipulators

Effectiveness of CAS

Modern computer algebra systems contain a huge number of functions from many domains of mathematics and can derive many mathematical identities.

Effectiveness of CAS

Modern computer algebra systems contain a huge number of functions from many domains of mathematics and can derive many mathematical identities.

Example

Ask MAPLE to evaluate

$$\sum_{n=1}^{\infty} \frac{1}{n^2}$$

and it returns $\pi^2/6$.

Effectiveness of CAS

Modern computer algebra systems contain a huge number of functions from many domains of mathematics and can derive many mathematical identities.

Example

Ask MAPLE to evaluate

$$\sum_{n=1}^{\infty} \frac{1}{n^2}$$

and it returns $\pi^2/6$ (*not* 1.64493406685).

Limitations of CAS

CASes do not typically contain optimized general-purpose search algorithms.

SAT + CAS

Brute force + Knowledge

The research areas of SMT [SAT Modulo Theories] solving and symbolic computation are quite disconnected. [. . .] More common projects would allow to join forces and commonly develop improvements on both sides.

Dr. Erika Ábrahám
RWTH Aachen University
ISSAC 2015 Invited talk

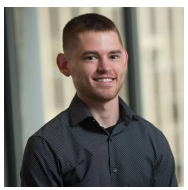
MathCheck I

- In 2015, a SAT+CAS system called MathCheck solved open cases of two conjectures in graph theory.
- It was shown that any matching of a hypercube graph of order $n \leq 5$ can be extended to a Hamiltonian cycle.


E. Zulkoski, V. Ganesh, K. Czarnecki. MathCheck: A math assistant based on a combination of computer algebra systems and SAT solvers. *International Conference on Automated Deduction*, 2015.

MathCheck II

- We have also applied the SAT+CAS method to combinatorial design theory and number theory.
- In particular, we have found many new Hadamard matrices and shown certain types of Hadamard matrices don't exist.






E. Zulkoski, C. Bright, A. Heinle, I. Kotsireas, K. Czarnecki, V. Ganesh. Combining SAT solvers with computer algebra systems to verify combinatorial conjectures. *Journal of Automated Reasoning*, 2017.

Hadamard matrices

- 125 years ago Jacques Hadamard defined what are now known as *Hadamard matrices*.
- Square matrices with ± 1 entries and pairwise orthogonal rows.

Jacques Hadamard. Résolution d'une question relative aux déterminants.
Bulletin des sciences mathématiques, 1893.

The Hadamard conjecture

- The *Hadamard conjecture* says that Hadamard matrices exist in order $4n$ for all $n \geq 1$.
- Strongly expected to hold but still open after 125 years.

The Hadamard conjecture

- The *Hadamard conjecture* says that Hadamard matrices exist in order $4n$ for all $n \geq 1$.
- Strongly expected to hold but still open after 125 years.

The Williamson conjecture

- In 1944, John Williamson discovered a way to construct Hadamard matrices of order $4n$ via four symmetric matrices A, B, C, D of order n with ± 1 entries.
- The *Williamson conjecture* says that such matrices exist in all orders n.

Williamson matrices

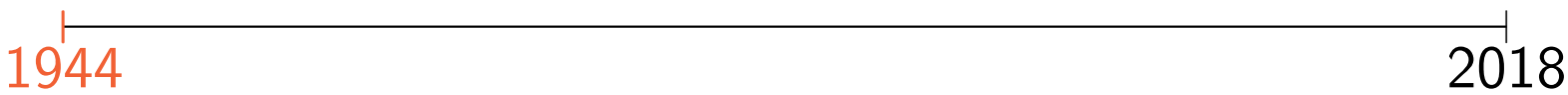
Williamson matrices are *circulant* (each row a shift of the previous row) and

$$A^2 + B^2 + C^2 + D^2$$

is the scalar matrix $4nI$.

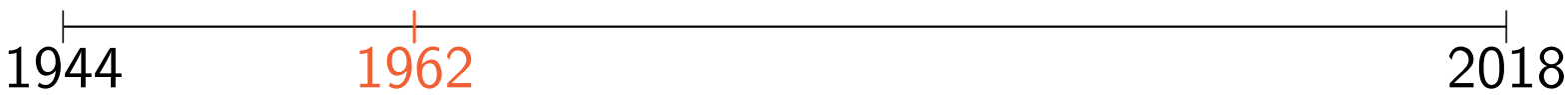
Williamson matrices in odd orders

In 1944, Williamson found twenty-three sets of Williamson matrices in the orders 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 25, 37, and 43.



Williamson matrices in odd orders

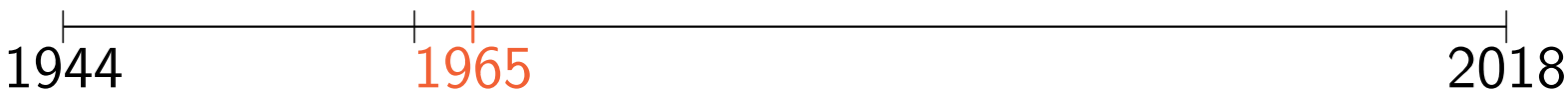
In 1962, Baumert, Golomb, and Hall found one in order 23.



L. Baumert, S. Golomb, M. Hall. Discovery of an Hadamard matrix of order 92. *Bulletin of the American mathematical society*, 1962.

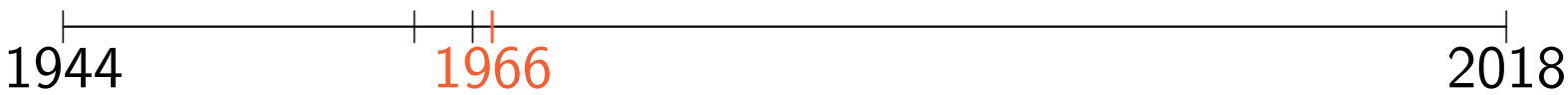
Williamson matrices in odd orders

In 1965, Baumert and Hall found seventeen sets of Williamson matrices in the orders 15, 17, 19, 21, 25, and 27.



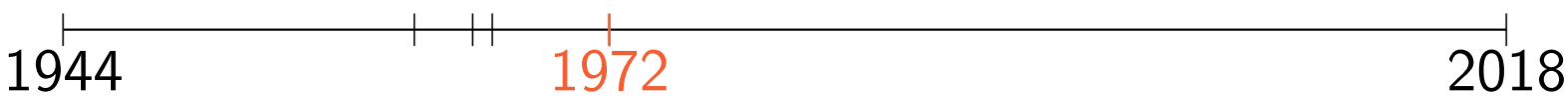
Williamson matrices in odd orders

The next year Baumert found one in order 29.



Williamson matrices in odd orders

In 1972, Turyn found an infinite class of them, including one in each order 27, 31, 37, 41, 45, 49, 51, 55, 57, 61, 63, and 69.

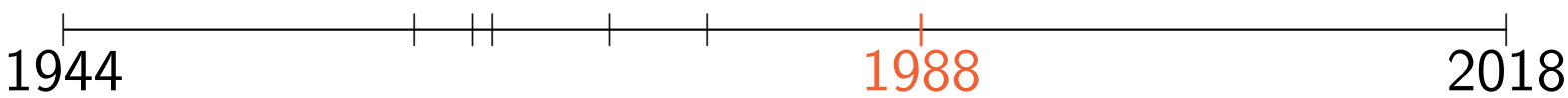


Williamson matrices in odd orders

In 1977, Sawade found four in order 25 and four in order 27 and Yamada found one in order 37.

Williamson matrices in odd orders

In 1988, Koukouvinos and Kounias found four in order 33.

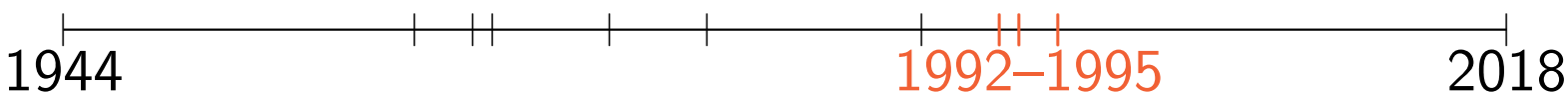


Williamson matrices in odd orders

In 1992, Đoković found one in order 31.

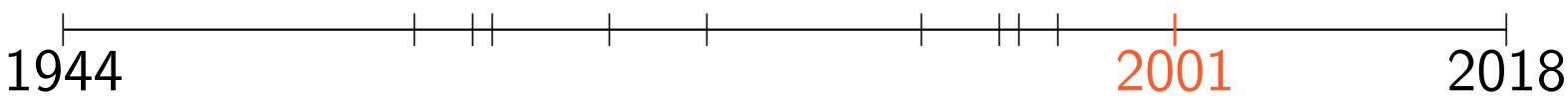
The next year he found one in order 33 and one in order 39.

Two years later he found two in order 25 and one in order 37.



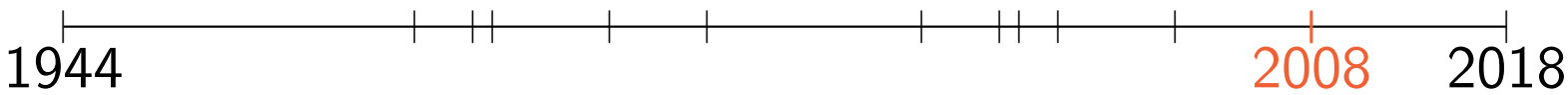
Williamson matrices in odd orders

In 2001, van Vliet found one in order 51.



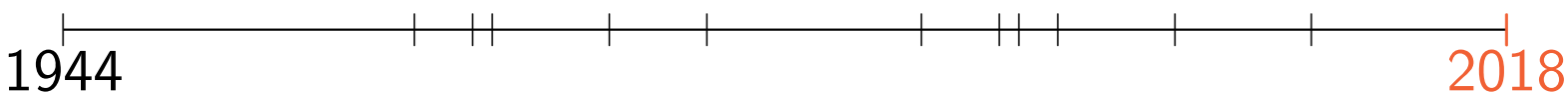
Williamson matrices in odd orders

In 2008, Holzmann, Kharaghani, and Tayfeh-Rezaie found one in order 43.

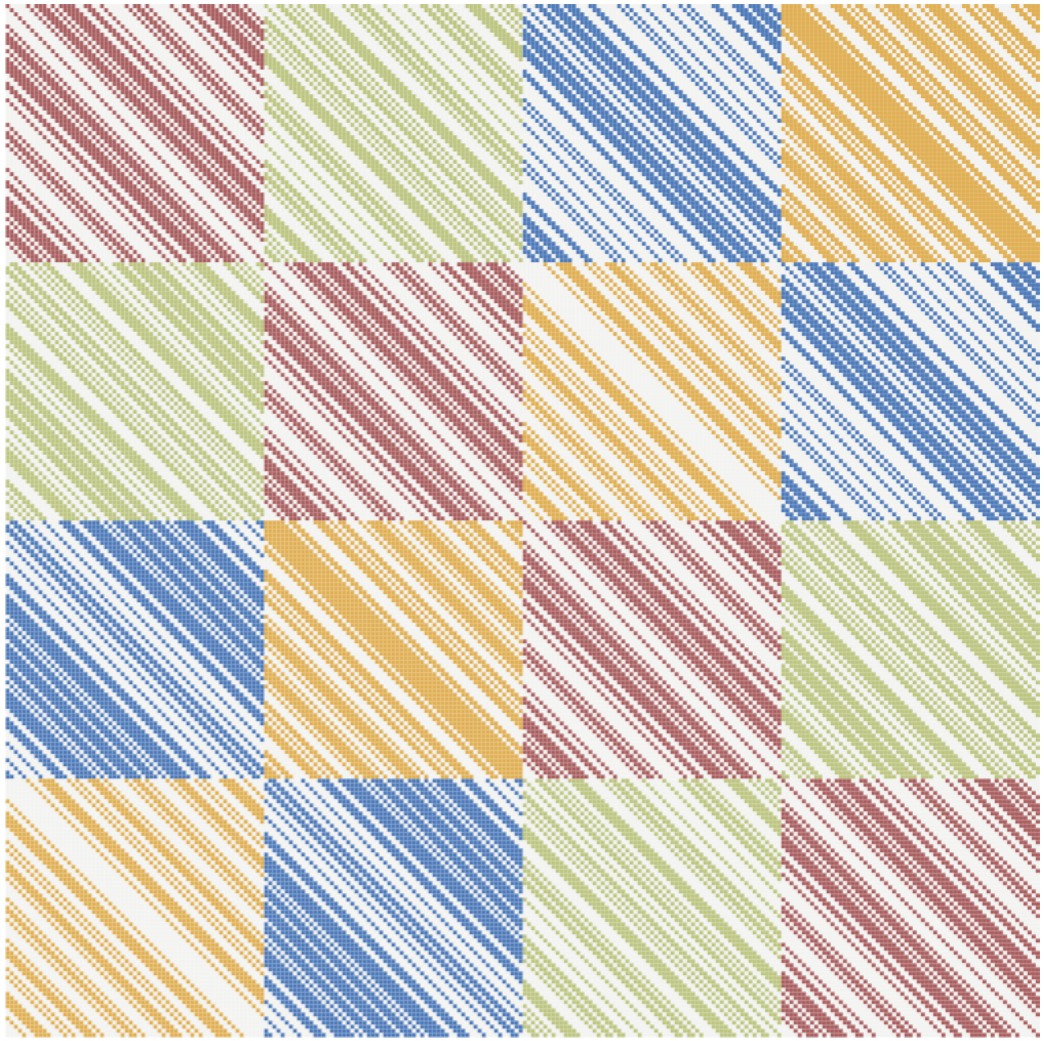


Williamson matrices in odd orders

In 2018, Bright, Kotsireas, and Ganesh found one in order 63.



A Hadamard matrix of order $4 \cdot 63 = 252$



Status of the conjecture I

- The Williamson conjecture for odd orders is false.
  - The counterexample 35 was found in 1993.
    D. Đoković. Williamson matrices of order $4n$ for $n = 33, 35, 39$. *Discrete mathematics*, 1993.
  - The counterexamples 47, 53, and 59 were found in 2008.
    W.H. Holzmann, H. Kharaghani, B. Tayfeh-Rezaie. Williamson matrices up to order 59. *Designs, codes and cryptography*, 2008.

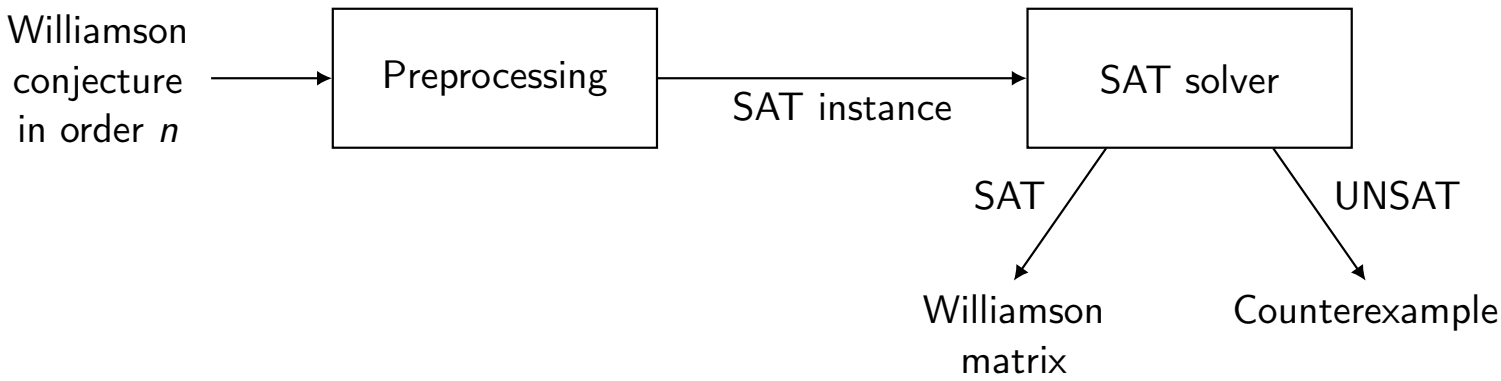
Status of the conjecture II

- The Williamson conjecture for even orders is open.
  - We have constructed over 100,000 Williamson matrices in all even orders $n \leq 70$.

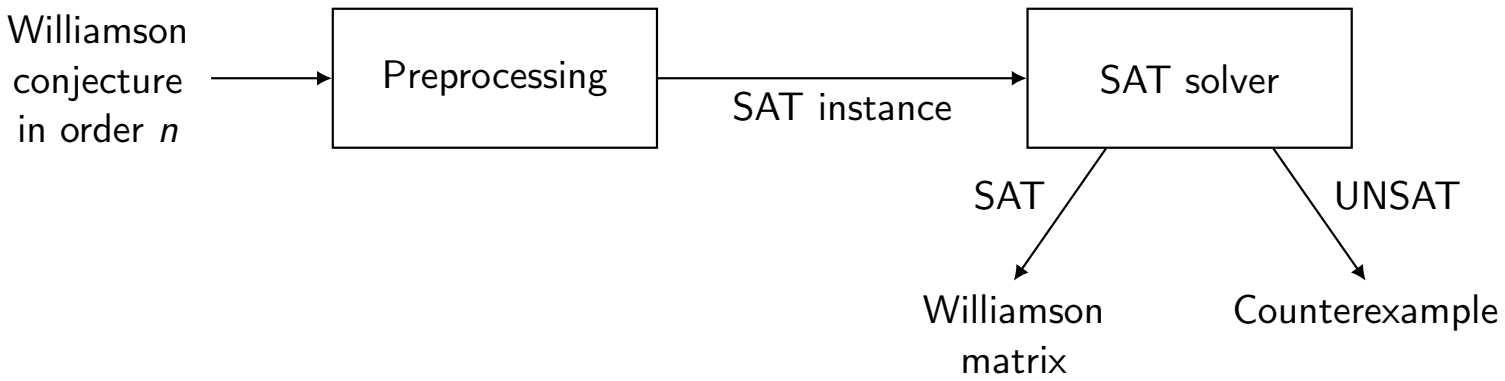
    C. Bright, I. Kotsireas, V. Ganesh. A SAT+CAS method for enumerating Williamson matrices of even order. *AAAI 2018*.

    C. Bright, I. Kotsireas, V. Ganesh. The SAT+CAS paradigm and the Williamson conjecture. *ACM Communications in Computer Algebra*, 2018.

System overview

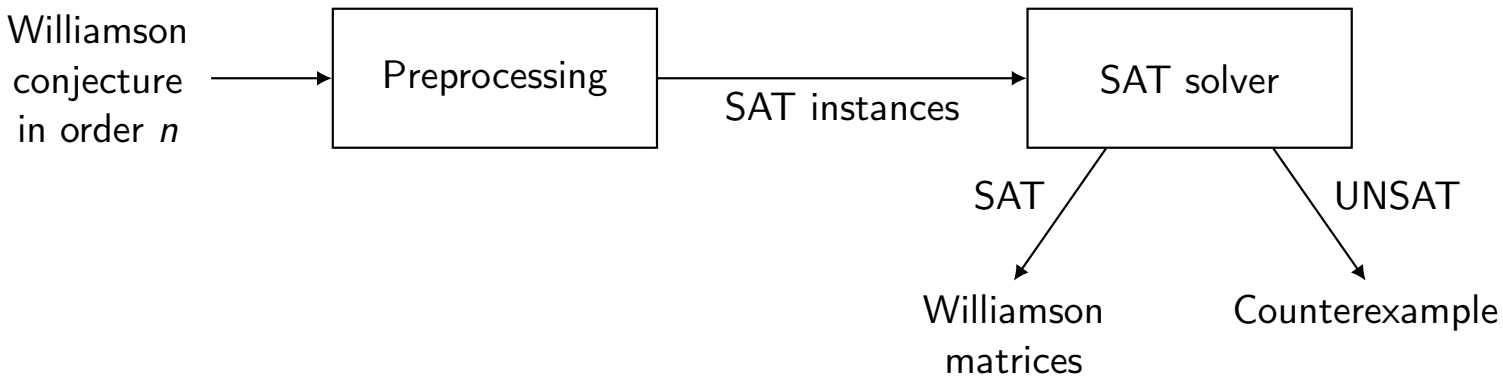


System overview



This setup is simple but only works for small n.

System overview



Split up the search space during preprocessing:

Solvers perform better on smaller search spaces and the subspaces are independent so can be solved in parallel.

Splitting

The simplest thing would be to fix the first entries of A, but this does not perform well.

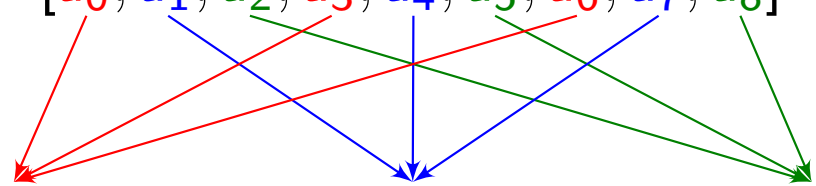
Splitting

The simplest thing would be to fix the first entries of A, but this does not perform well.

Compression

- Instead, we fix the entries of the *compression* of A.
- Compression of a row of order n is defined as follows:

$$A = [a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8]$$



$$A' = \big[a_0 + a_3 + a_6, \quad a_1 + a_4 + a_7, \quad a_2 + a_5 + a_8\big].$$

Uncompression

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

Encoding in SAT

- Say the kth entry in the 2-compression of A is 2, i.e.,

$$a_k + a_{k+n/2} = 2.$$

- As Boolean variables both a_k and $a_{k+n/2}$ must be true.
- We encode this in Boolean logic as

$$a_k \wedge a_{k+n/2}.$$

Encoding in SAT

- Say the kth entry in the 2-compression of A is -2, i.e.,

$$a_k + a_{k+n/2} = -2.$$

- As Boolean variables both a_k and $a_{k+n/2}$ must be false.
- We encode this in Boolean logic as

$$\neg a_k \wedge \neg a_{k+n/2}.$$

Encoding in SAT

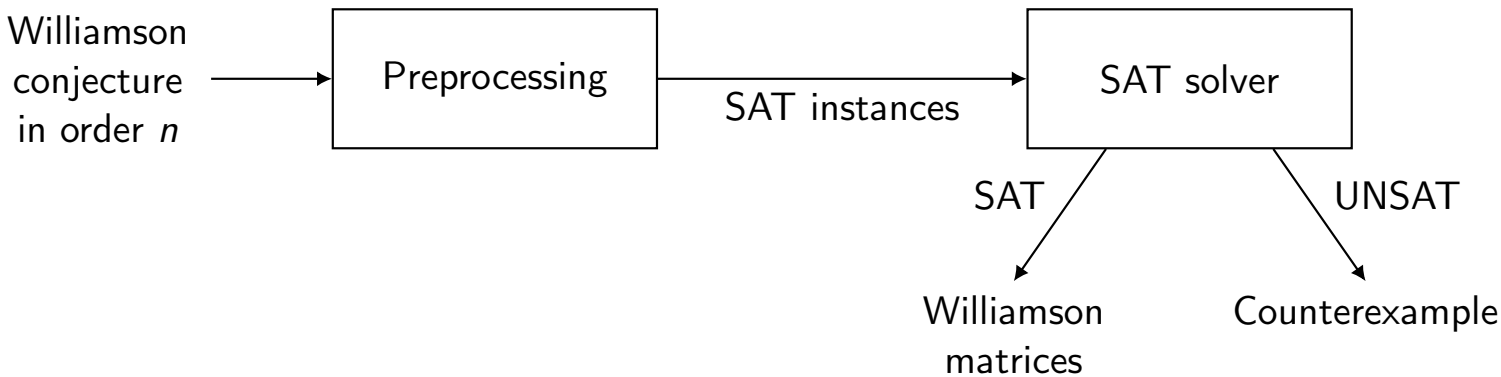
- Say the kth entry in the 2-compression of A is 0, i.e.,

$$a_k + a_{k+n/2} = 0.$$

- As Boolean variables exactly one of a_k and $a_{k+n/2}$ is true.
- We encode this in Boolean logic as

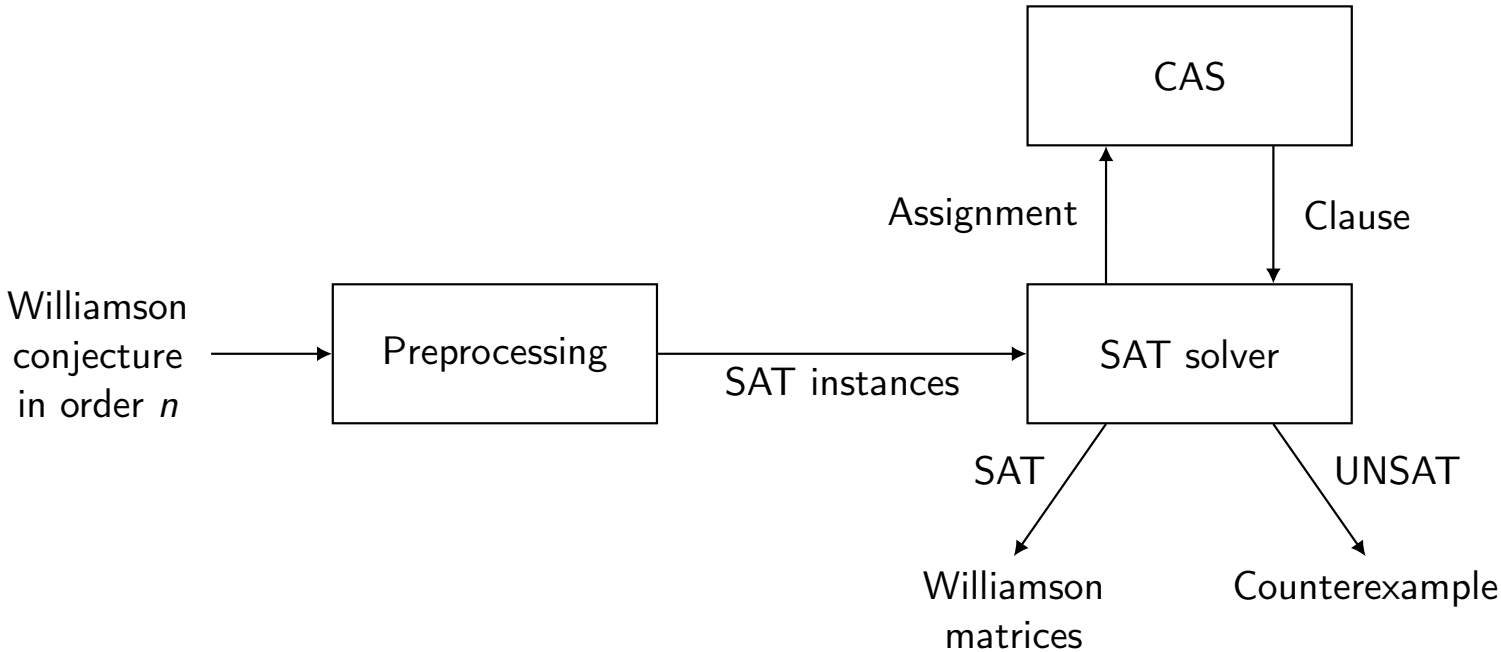
$$(\neg a_k \vee a_{k+n/2}) \wedge (a_k \vee \neg a_{k+n/2}).$$

System overview



This works better but does not exploit theorems about Williamson matrices that cannot easily be encoded in Boolean logic.

System overview



Encode some knowledge *programmatically*:

Allows encoding much more expressive constraints.

Discrete Fourier transform

- The *discrete Fourier transform* DFT_A of $A = [a_0, \ldots, a_{n-1}]$ is the sequence whose kth entry is

$$\sum_{j=0}^{n-1} a_j \exp(2\pi ijk/n).$$

- Can be computed very efficiently by CAS functions.

Discrete Fourier transform

- The *discrete Fourier transform* DFT_A of $A = [a_0, \ldots, a_{n-1}]$ is the sequence whose kth entry is

$$\sum_{j=0}^{n-1} a_j \exp(2\pi ijk/n).$$

- Can be computed very efficiently by CAS functions.

Power spectral density

The *PSD values* PSD_A are the squared absolute values of DFT_A.

PSD theorem

If A, B, C, D are the initial rows of Williamson matrices then each entry of

$$\mathrm{PSD}_A + \mathrm{PSD}_B + \mathrm{PSD}_C + \mathrm{PSD}_D$$

is the constant $4n$. **(!)**

D. Đoković, I. Kotsireas. Compression of periodic complementary sequences and applications. *Designs, codes and cryptography*, 2015.

PSD criterion

Since PSD values are nonnegative it follows that the PSD values of Williamson matrices are at most $4n$.

PSD criterion

Since PSD values are nonnegative it follows that the PSD values of Williamson matrices are at most $4n$.

PSD filtering

If a sequence has a PSD value larger than $4n$ then **it cannot be a row of a Williamson matrix**.

Example

- Say the SAT solver assigns all entries of A to true.
- In this case the first entry of PSD_A will be n^2 which is larger than $4n$ for n larger than 4.

Example

- Say the SAT solver assigns all entries of A to true.
- In this case the first entry of PSD_A will be n^2 which is larger than $4n$ for n larger than 4.

Consequence

A cannot be a row of a Williamson matrix, so learn the clause

$$\neg a_0 \vee \neg a_1 \vee \cdots \vee \neg a_{n-1}.$$

Enumeration results

- Without the programmatic approach we were able to solve orders up to around 35.
- With the programmatic approach we found over 100,000 new Williamson matrices in all even orders up to 70 and one new set of Williamson matrices in order 63.
- Available on the MathCheck website:

`curtisbright.com/mathcheck`

Other results I

- Verified that 35 is the smallest counterexample of the Williamson conjecture.

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

- Enumerated all complex Golay pairs in all orders up to 25 and verified the conjecture that they don't exist in order 23.

  C. Bright, I. Kotsireas, A. Heinle, V. Ganesh. Enumeration of complex Golay pairs via programmatic SAT. *ISSAC 2018*.

Other results II

- Found 8-Williamson matrices in all odd orders up to 35.
  C. Bright, I. Kotsireas, V. Ganesh. Applying computer algebra systems and SAT solvers to the Williamson conjecture. *In submission*, 2018.
- Found new examples of good matrices in the orders 27 and 57 and new counterexamples in the orders 51, 63, and 69.
  C. Bright, D. Đoković, I. Kotsireas, V. Ganesh. A SAT+CAS approach to finding good matrices: New examples and counterexamples. *In submission*, 2018.

Conclusion

- The SAT+CAS paradigm is very general and can be applied to problems in many domains, especially "needle-in-haystack" problems that require rich mathematics.

Conclusion

- The SAT+CAS paradigm is very general and can be applied to problems in many domains, especially "needle-in-haystack" problems that require rich mathematics.
- Make use of the immense amount of engineering effort that has gone into CAS and SAT solvers.

Conclusion

- The SAT+CAS paradigm is very general and can be applied to problems in many domains, especially "needle-in-haystack" problems that require rich mathematics.
- Make use of the immense amount of engineering effort that has gone into CAS and SAT solvers.
- Can be difficult to split up the problem in a way that takes advantage of this.

Conclusion

- The SAT+CAS paradigm is very general and can be applied to problems in many domains, especially "needle-in-haystack" problems that require rich mathematics.
- Make use of the immense amount of engineering effort that has gone into CAS and SAT solvers.
- Can be difficult to split up the problem in a way that takes advantage of this.

I am currently based in Ottawa and welcome collaboration extending this and related work!