MathCheck: A SAT+CAS Mathematical Conjecture Verifier

Curtis Bright[1] Ilias Kotsireas[2] Vijay Ganesh[1]

[1]University of Waterloo
[2]Wilfrid Laurier University

July 26, 2018

SAT + CAS

SAT + CAS

Brute force

SAT + CAS

Brute force + Cleverness

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

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.

Williamson matrices

- 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.
- Such matrices are *circulant* (each row a shift of the previous row) and satisfy

$$A^2 + B^2 + C^2 + D^2 = 4nI$$

where I is the identity matrix.

The Williamson conjecture

Only a finite number of Hadamard matrices of Williamson type are known so far; it has been conjectured that one such exists of any order $4t$.

Dr. Richard Turyn
Raytheon Company
1972

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 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.
- 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 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.
- In 1962, Baumert, Golomb, and Hall found one in order 23.
- In 1965, Baumert and Hall found seventeen sets of Williamson matrices in the orders 15, 17, 19, 21, 25, and 27.
- In 1966, Baumert found one in order 29.

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.
- In 1962, Baumert, Golomb, and Hall found one in order 23.
- In 1965, Baumert and Hall found seventeen sets of Williamson matrices in the orders 15, 17, 19, 21, 25, and 27.
- In 1966, Baumert found one in order 29.
- 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 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.
- In 1962, Baumert, Golomb, and Hall found one in order 23.
- In 1965, Baumert and Hall found seventeen sets of Williamson matrices in the orders 15, 17, 19, 21, 25, and 27.
- In 1966, Baumert found one in order 29.
- 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.
- In 1977, Sawade found four in order 25 and four in order 27.
- In 1977, Yamada found one in order 37.
- In 1988, Koukouvinos and Kounias found four in order 33.

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.
- In 1962, Baumert, Golomb, and Hall found one in order 23.
- In 1965, Baumert and Hall found seventeen sets of Williamson matrices in the orders 15, 17, 19, 21, 25, and 27.
- In 1966, Baumert found one in order 29.
- 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.
- In 1977, Sawade found four in order 25 and four in order 27.
- In 1977, Yamada found one in order 37.
- In 1988, Koukouvinos and Kounias found four in order 33.
- In 1992, Đoković found one in order 31.
- In 1993, Đoković found one in order 33 and one in order 39.
- In 1995, Đoković found two in order 25 and one in order 37.

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.
- In 1962, Baumert, Golomb, and Hall found one in order 23.
- In 1965, Baumert and Hall found seventeen sets of Williamson matrices in the orders 15, 17, 19, 21, 25, and 27.
- In 1966, Baumert found one in order 29.
- 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.
- In 1977, Sawade found four in order 25 and four in order 27.
- In 1977, Yamada found one in order 37.
- In 1988, Koukouvinos and Kounias found four in order 33.
- In 1992, Đoković found one in order 31.
- In 1993, Đoković found one in order 33 and one in order 39.
- In 1995, Đoković found two in order 25 and one in order 37.
- In 2001, van Vliet found one in order 51.

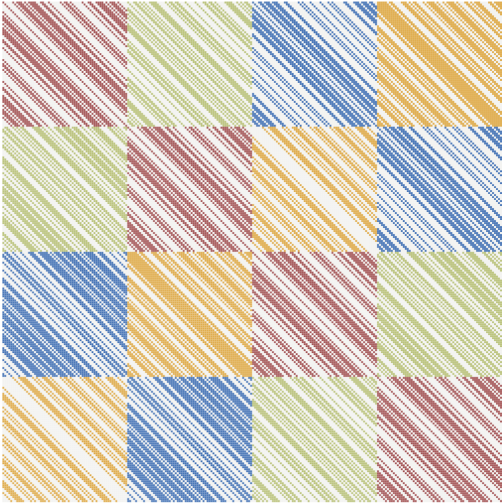
Williamson matrices in odd orders

- 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.
- In 1962, Baumert, Golomb, and Hall found one in order 23.
- In 1965, Baumert and Hall found seventeen sets of Williamson matrices in the orders 15, 17, 19, 21, 25, and 27.
- In 1966, Baumert found one in order 29.
- 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.
- In 1977, Sawade found four in order 25 and four in order 27.
- In 1977, Yamada found one in order 37.
- In 1988, Koukouvinos and Kounias found four in order 33.
- In 1992, Đoković found one in order 31.
- In 1993, Đoković found one in order 33 and one in order 39.
- In 1995, Đoković found two in order 25 and one in order 37.
- In 2001, van Vliet found one in order 51.
- In 2008, Holzmann, Kharaghani, and Tayfeh-Rezaie found one in order 43.

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.
- In 1962, Baumert, Golomb, and Hall found one in order 23.
- In 1965, Baumert and Hall found seventeen sets of Williamson matrices in the orders 15, 17, 19, 21, 25, and 27.
- In 1966, Baumert found one in order 29.
- 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.
- In 1977, Sawade found four in order 25 and four in order 27.
- In 1977, Yamada found one in order 37.
- In 1988, Koukouvinos and Kounias found four in order 33.
- In 1992, Đoković found one in order 31.
- In 1993, Đoković found one in order 33 and one in order 39.
- In 1995, Đoković found two in order 25 and one in order 37.
- In 2001, van Vliet found one in order 51.
- In 2008, Holzmann, Kharaghani, and Tayfeh-Rezaie found one in order 43.
- In 2018, Bright, Kotsireas, and Ganesh found one in order 63.

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



Status of the conjecture

- The Williamson conjecture for odd orders is false, 35 being the smallest counterexample.

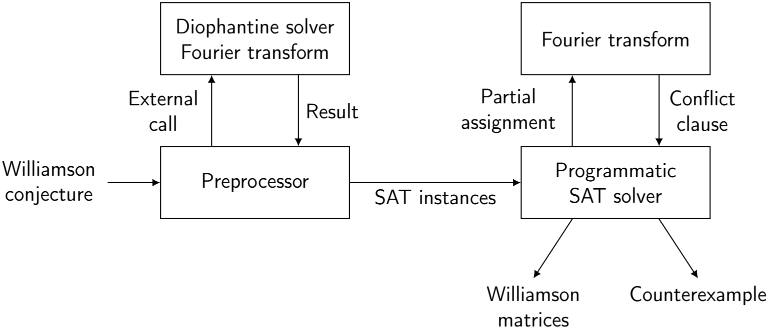
  D. Đoković. Williamson matrices of order $4n$ for $n = 33, 35, 39$. *Discrete mathematics*, 1993.

- The Williamson conjecture for even orders is open.

Williamson matrices in even orders

- In 1944, Williamson found Williamson matrices in the orders 2, 4, 8, 12, 16, 20, and 32.
- In 2006, Kotsireas and Koukouvinos found them in all even orders up to 22.
- In 2016, Bright, Ganesh, Heinle, Kotsireas, Nejati, and Czarnecki found them in all even orders up to 34.
- In 2017, Bright, Kotsireas, and Ganesh found them in all even orders up to 64.
- In 2018, Bright, Kotsireas, and Ganesh found them in all even orders up to 70.

How we performed our enumerations



Preprocessing: Compression

- When the order n is a multiple of 3 we can *compress* a row to obtain a row of length $n/3$:

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

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

Discrete Fourier transform

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

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

Power spectral density

- The *power spectral density* of a sequence $A = [a_0, \ldots, a_{n-1}]$ is a sequence PSD_A whose kth entry is

$$\left| \sum_{j=0}^{n-1} a_j \exp(2\pi i j k / n) \right|^2 .$$

PSD criterion

- If A, B, C, D are the initial rows of Williamson matrices (or any compression of them) then

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

is a constant sequence whose entries are $4n$.

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

Preprocessing

- Suppose n is even, so 2-compressions of rows of Williamson matrices are $\{0, \pm 2\}$-sequences of length $n/2$.
- The space of sequences of length $n/2$ is much smaller than the space of sequences of length n, and for n around 70 we can find all sequences of length $n/2$ which satisfy the PSD criterion.

Uncompression

- We use a SAT solver to *uncompress* the sequences found in the preprocessing stage.
- Let the entries of the first row of A be represented by the Boolean variables $a_0, \dots, a_{n-1}$ with true representing 1 and false representing -1.

SAT instances

- Say the 2-compression of A is $[2, 0]$.
- This tells us that both a_0 and a_2 are true and exactly one of a_1 and a_3 are true, so we use the following clauses:

$$a_0$$

$$a_2$$

$$\neg a_1 \vee \neg a_3$$

$$a_1 \vee a_3$$

SAT instances: Problem

- How can the PSD criterion be encoded into a SAT instance?

SAT instances: Problem

- How can the PSD criterion be encoded into a SAT instance?
- We use a SAT solver custom-tailored to this problem which can *programmatically* learn logical facts.

Programmatic SAT example

- Say the SAT solver, in the process of searching for a solution to the SAT instance, assigns all a_k to true.
- In this case PSD_A will contain an entry larger than $4n$ meaning the PSD criterion cannot hold.
- Regardless of the values of B, C, and D, we know A will never be part of a set of Williamson matrices, so we learn the clause

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

Programmatic results

- For orders around 45 the programmatic approach was found to perform *thousands* of times faster than an approach which only used CNF clauses.
- Performed better as the order increased.

Enumeration results

- Enumerated all Williamson matrices with orders divisible by 2 or 3 up to order 70.
- Found over 100,000 new Williamson matrices in even orders and one new set of Williamson matrices in order 63.
- Available on the MathCheck website:

  `https://sites.google.com/site/uwmathcheck/`

Conclusion

- The SAT+CAS paradigm is very general and can be applied to problems in a large number of domains.
- Especially good for problems that require high-level mathematics as well as some kind of unstructured brute-force search.
- Pro: Make use of the immense amount of engineering effort that has gone into CAS and SAT solvers.
- Con: Can be difficult to split the problem in a way that takes advantage of this.