A SAT+CAS Method for Enumerating Williamson Matrices of Even Order

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

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

July 29, 2017

***Brute**-brute force has no hope. But clever, inspired brute force is the future.*

Dr. Doron Zeilberger, Rutgers University, 2015

Roadmap

Motivation

- Many conjectures in combinatorics concern the existence or nonexistence of combinatorial objects which are only feasibly constructed through a search.
- To find large instances of these objects, it is necessary to use a computer with a clever search procedure.

Example

- Williamson matrices, first defined in 1944, were enumerated up to order 59 in 2007 but only for *odd* orders[1]. They had never been enumerated in even orders until this work.
- We exhaustively enumerated Williamson matrices up to order ~~44~~ 64 and found that they are much more abundant in even orders than odd orders.

[1] W. H. Holzmann, H. Kharaghani, B. Tayfeh-Rezaie, Williamson matrices up to order 59, Designs, Codes and Cryptography.

Roadmap

Motivational quote

> *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, 2015[2]

---

[2] Building bridges between symbolic computation and satisfiability checking. Invited talk, *ISSAC 2015*.

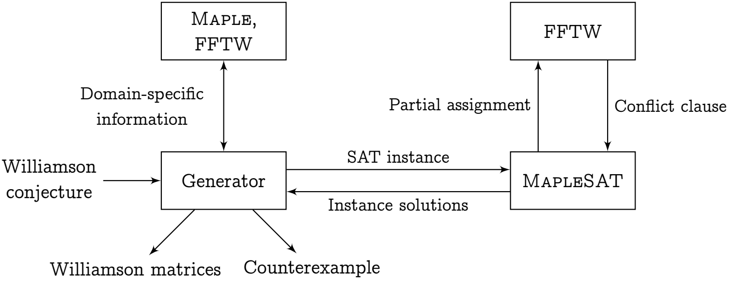
How we performed the enumeration

- Used a reduction to the *Boolean satisfiability problem* (SAT).
- Used a SAT solver coupled with functionality from numerical libraries and a *computer algebra system* (CAS) to perform the search.
- Used the programmatic SAT solver MapleSAT[3] which could programmatically learn conflict clauses, through a piece of code specifically tailored to the domain.

[3] J. Liang et al., Exponential Recency Weighted Average Branching Heuristic for SAT Solvers, AAAI 2016

The MathCheck2 system

Uses the SAT+CAS paradigm to finitely verify or counterexample conjectures in mathematics, in particular the Williamson conjecture.



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

Roadmap

The Williamson conjecture

It has been conjectured that an Hadamard matrix of this [Williamson] type might exist of every order $4t$*, at least for* t *odd.*

Dr. Richard Turyn, Raytheon Company, 1972

Disproof of the Williamson conjecture

- Dragomir Đoković showed in 1993 that $t = 35$ was a counterexample to the Williamson conjecture, i.e., Williamson matrices of order 35 do not exist.
- His algorithm assumed the Williamson order was odd.

Williamson matrices

- $n \times n$ matrices A, B, C, D with ± 1 entries
- symmetric
- circulant (each row is a shift of the previous row)
- $A^2 + B^2 + C^2 + D^2 = 4nI_n$

Williamson sequences

Williamson matrices can equivalently be defined using sequences:

- sequences A, B, C, D of length n with ± 1 entries
- symmetric
- $\mathrm{PSD}_A(s) + \mathrm{PSD}_B(s) + \mathrm{PSD}_C(s) + \mathrm{PSD}_D(s) = 4n$ for all $s \in \mathbb{Z}$.

The values of the PSD (*power spectral density*) of X are the squared absolute values of the discrete Fourier transform of X.

PSD criterion

Since PSD values are non-negative and

$$\mathrm{PSD}_A(s) + \mathrm{PSD}_B(s) + \mathrm{PSD}_C(s) + \mathrm{PSD}_D(s) = 4n,$$

if $\mathrm{PSD}_X(s) > 4n$ for some s then X is not a member of a Williamson sequence.

PSD criterion

Since PSD values are non-negative and

$$\mathrm{PSD}_A(s) + \mathrm{PSD}_B(s) + \mathrm{PSD}_C(s) + \mathrm{PSD}_D(s) = 4n,$$

if $\mathrm{PSD}_X(s) > 4n$ for some s then X is not a member of a Williamson sequence.

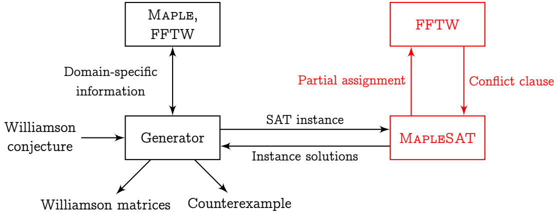
Problem

How can the PSD criterion be encoded in a SAT instance?

Roadmap

Solution: Programmatic SAT

- A *programmatic* SAT solver[4] contains a special *callback* function which periodically examines the current partial assignment while the SAT solver is running.
- If it can determine that the partial assignment cannot be extended into a satisfying assignment then a conflict clause is generated encoding that fact.



[4] V. Ganesh et al., LYNX: A programmatic SAT solver for the RNA-folding problem, SAT 2012

Programmatic PSD criterion

- Given a partial assignment, we compute $\mathrm{PSD}_X(s)$ for $X \in \{A, B, C, D\}$ whose entries are all currently set.
- If any PSD value is larger than $4n$ then we generate a clause which forbids the variables in X from being set the way they currently are.

Programmatic results

- The programmatic approach was found to perform much better than an approach which encoded the Williamson sequence definition using CNF clauses:

order n	programmatic speedup
20	4.33
22	7.00
24	7.12
26	27.00
28	52.56
30	52.21
32	58.16
34	138.37
36	317.61
38	377.84
40	428.71
42	1195.99
44	2276.09

Roadmap

A Diophantine equation

The PSD criterion for $s = 0$ becomes

$$\text{rowsum}(A)^2 + \text{rowsum}(B)^2 + \text{rowsum}(C)^2 + \text{rowsum}(D)^2 = 4n.$$

In other words, every Williamson sequence provides a decomposition of $4n$ into a sum of four squares.

A Diophantine equation

The PSD criterion for $s = 0$ becomes

$$\text{rowsum}(A)^2 + \text{rowsum}(B)^2 + \text{rowsum}(C)^2 + \text{rowsum}(D)^2 = 4n.$$

In other words, every Williamson sequence provides a decomposition of $4n$ into a sum of four squares.

- There are usually only a few such decompositions.

A Diophantine equation

The PSD criterion for $s = 0$ becomes

$$\mathrm{rowsum}(A)^2 + \mathrm{rowsum}(B)^2 + \mathrm{rowsum}(C)^2 + \mathrm{rowsum}(D)^2 = 4n.$$

In other words, every Williamson sequence provides a decomposition of $4n$ into a sum of four squares.

- There are usually only a few such decompositions.
- A CAS (e.g., MAPLE) has functions designed to compute the decompositions.

Compression

When n is even we can *compress* a sequence of length n to obtain a sequence of length $n/2$:

$$A = [a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9]$$

$$A' = \left[a_0 + a_5, \quad a_1 + a_6, \quad a_2 + a_7, \quad a_3 + a_8, \quad a_4 + a_9\right].$$

Đoković–Kotsireas theorem

Any compression A', B', C', D' of a Williamson sequence satisfies

$$\mathrm{PSD}_{A'}(s) + \mathrm{PSD}_{B'}(s) + \mathrm{PSD}_{C'}(s) + \mathrm{PSD}_{D'}(s) = 4n$$

for all $s \in \mathbb{Z}$.

Using compressions

- For a given even order n, searching for compressed Williamson sequences is easier than searching for uncompressed Williamson sequences.
- With the help of a CAS we can generate all possible compressions.
- For each possible compression, we generate a SAT instance which encodes the problem of 'uncompressing' that sequence.

Example SAT instance

If $A' = [2, -2, 0]$ was a possible compression, this implies that

$$a_0 + a_3 = 2$$
$$a_1 + a_4 = -2$$
$$a_2 + a_5 = 0$$

From which we generate the SAT clauses (with 'true' representing 1 and 'false' representing -1)

$$a_0 \wedge a_3$$
$$\neg a_1 \wedge \neg a_4$$
$$(a_2 \vee a_5) \wedge (\neg a_2 \vee \neg a_5)$$

Results

n	Gen. time (m)	Solve time (m)	# instances	# W_n
2	0.00	0.00	1	1
4	0.00	0.00	1	1
6	0.00	0.00	1	1
8	0.00	0.00	1	1
10	0.00	0.00	2	2
12	0.00	0.00	3	3
14	0.00	0.00	3	7
16	0.00	0.00	5	6
18	0.00	0.01	22	40
20	0.00	0.01	21	27
22	0.00	0.01	22	27
24	0.00	0.06	176	80
26	0.01	0.01	24	38
28	0.01	0.03	78	99
30	0.14	0.11	281	268
32	0.06	0.38	1064	200
34	4.17	0.09	214	160
36	6.21	1.10	1705	691
38	67.55	0.18	360	87
40	152.03	28.78	40924	1898
42	1416.95	2.47	2945	561
44	1091.55	2.25	1523	378

The amount of time used to generate and solve the SAT instances, the number of instances generated, and the number of Williamson sequences found (# W_n).

Roadmap

In summary

- We have demonstrated the power of the SAT+CAS paradigm and the programmatic SAT paradigm by applying them to the combinatorial Williamson conjecture.
- Provided an enumeration for the first time of Williamson sequences for even orders up to ~~44~~ 64.
- Shown that Williamson matrices are much more numerous in even orders. (No odd order is known for which $\#W_n > 10$, yet $\#W_{64} = 95{,}504$.)