Computational Methods for Combinatorial and Number Theoretic Problems

Curtis Bright

UNIVERSITY OF WATERLOO

March 23, 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.

Three examples, with our new results

1. Williamson matrices
   - Proof that Williamson matrices of order 35 do not exist.
   - Enumeration of all Williamson matrices in orders up to 45, including even orders (open since first defined in 1944).
2. Complex Golay sequences
   - Enumeration of all complex Golay sequences up to order 25.
   - Proof that complex Golay sequences of order 23 do not exist (conjectured in 2002, shown in 2013).
3. Minimal primes
   - Enumeration of all minimal primes in bases up to 16 and several other bases (open since 2000).

Three examples, with our new results

1. Williamson matrices
   - Proof that Williamson matrices of order 35 do not exist.
   - Enumeration of all Williamson matrices in orders up to 45, including even orders (open since first defined in 1944).
2. Complex Golay sequences
   - Enumeration of all complex Golay sequences up to order 25.
   - Proof that complex Golay sequences of order 23 do not exist (conjectured in 2002, shown in 2013).
3. Minimal primes
   - Enumeration of all minimal primes in bases up to 16 and several other bases (open since 2000).

Roadmap

What did we do and what is new?

- Used a reduction to the *Boolean satisfiability problem* (SAT).
- Used a SAT solver coupled with functionality from a *computer algebra system* (CAS) to solve the SAT instances.

The SAT+CAS paradigm

Originated independently in two works in 2015:

1. A paper at the *Conference on Automated Deduction* (CADE) by Edward Zulkoski, Vijay Ganesh, and Krzysztof Czarnecki entitled "MathCheck: A Math Assistant via a Combination of Computer Algebra Systems and SAT Solvers".
2. An invited talk at the *International Symposium on Symbolic and Algebraic Computation* (ISSAC) by Erika Ábrahám entitled "Building Bridges between Symbolic Computation and Satisfiability Checking".

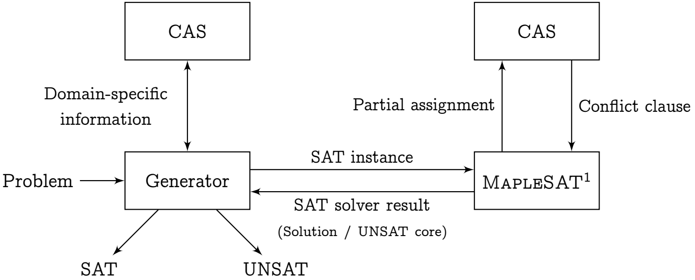
Motivational quote

The research areas of SMT [SAT Modulo Theories] solving and symbolic computation are quite disconnected. On the one hand, SMT solving has its strength in efficient techniques for exploring Boolean structures, learning, combining solving techniques, and developing dedicated heuristics, but its current focus lies on easier theories and it makes use of symbolic computation results only in a rather naive way.

Dr. Erika Ábrahám, RWTH Aachen University, 2015

The MathCheck2 system

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



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

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 and circulant
- $A^2 + B^2 + C^2 + D^2 = 4nI_n$

Symmetric and circulant matrices

Examples ($n = 5$ and 6)

$$\begin{bmatrix} a_0 & a_1 & a_2 & a_2 & a_1 \\ a_1 & a_0 & a_1 & a_2 & a_2 \\ a_2 & a_1 & a_0 & a_1 & a_2 \\ a_2 & a_2 & a_1 & a_0 & a_1 \\ a_1 & a_2 & a_2 & a_1 & a_0 \end{bmatrix}$$

symmetric conditions

$$\begin{bmatrix} a_0 & a_1 & a_2 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_1 & a_2 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_1 & a_2 & a_3 \\ a_3 & a_2 & a_1 & a_0 & a_1 & a_2 \\ a_2 & a_3 & a_2 & a_1 & a_0 & a_1 \\ a_1 & a_2 & a_3 & a_2 & a_1 & a_0 \end{bmatrix}$$

circulant conditions

Symmetric and circulant matrices

Examples ($n = 5$ and 6)

$$\begin{bmatrix} a_0 & a_1 & a_2 & a_2 & a_1 \\ a_1 & a_0 & a_1 & a_2 & a_2 \\ a_2 & a_1 & a_0 & a_1 & a_2 \\ a_2 & a_2 & a_1 & a_0 & a_1 \\ a_1 & a_2 & a_2 & a_1 & a_0 \end{bmatrix}$$

symmetric conditions

$$\begin{bmatrix} a_0 & a_1 & a_2 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_1 & a_2 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_1 & a_2 & a_3 \\ a_3 & a_2 & a_1 & a_0 & a_1 & a_2 \\ a_2 & a_3 & a_2 & a_1 & a_0 & a_1 \\ a_1 & a_2 & a_3 & a_2 & a_1 & a_0 \end{bmatrix}$$

circulant conditions

Such matrices are defined by their first $\lceil \frac{n+1}{2} \rceil$ entries so we may refer to them as if they were sequences.

Williamson sequences

- sequences A, B, C, D of length n with ± 1 entries
- symmetric
- $\mathrm{PAF}_A(s) + \mathrm{PAF}_B(s) + \mathrm{PAF}_C(s) + \mathrm{PAF}_D(s) = 0$ for $s = 1, \ldots, n-1$.

The PAF (*periodic autocorrelation function*) of sequence $X = [x_0, \ldots, x_{n-1}]$ is defined

$$\mathrm{PAF}_X(s) \coloneqq \sum_{k=0}^{n-1} x_k x_{(k+s) \bmod n}.$$

Power spectral density

The *power spectral density* of a sequence A is

$$\mathrm{PSD}_A(s) \coloneqq |\mathrm{DFT}_A(s)|^2$$

where DFT_A is the *discrete Fourier transform* of A.

PSD test

A theorem of Wiener and Khinchin (and a special case of a theorem of Đoković and Kotsireas) implies that Williamson sequences satisfy

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

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

PSD test

A theorem of Wiener and Khinchin (and a special case of a theorem of Đoković and Kotsireas) implies that Williamson sequences satisfy

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

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

Corollary

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

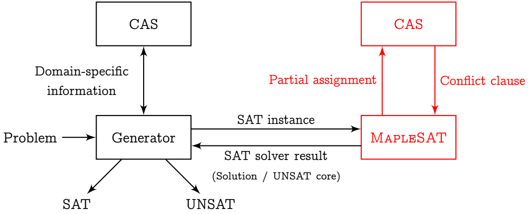
Problem: How to use the PSD test?

- The Williamson PAF condition is straightforward to encode in a SAT instance.
- Encoding the PSD test is not easy.

Roadmap

Solution: Programmatic SAT

- A *programmatic* SAT solver[2] 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.



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

Programmatic PSD test

- 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.

Results

n	Normal MapleSAT	Programmatic MapleSAT	Result
12	0.14	0.13	SAT
13	0.03	0.04	SAT
14	0.12	0.05	SAT
15	0.21	0.07	SAT
16	24.56	0.26	SAT
17	0.30	0.19	SAT
18	1.50	0.06	SAT
19	1.06	1.39	SAT
20	3.09	0.06	SAT
21	390.55	6.60	SAT
22	34.90	0.70	SAT
23	545.71	7.19	SAT
24	3116.93	13.72	SAT
25	591.78	42.62	SAT
26	6238.15	46.98	SAT
27	2485.84	719.32	SAT
28	6234.42	118.14	SAT
29	7053.56	25850.39	SAT
30	29881.94	441.49	SAT
31	20313.47	68538.98	SAT
32	TO	3309.02	SAT
33	TO	8549.17	SAT
34	TO	2986.61	SAT
35	TO	TO	TO
36	TO	639.58	SAT
37	TO	TO	TO
38	TO	TO	TO
39	TO	TO	TO
40	TO	15835.62	SAT

Timings in seconds, with a timeout (TO) of 24 hours

Roadmap

A Diophantine equation

The PSD test 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 test 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 test 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 CAS has functions designed to compute the decompositions.

Sum-of-squares results I

n	Decomposition	Normal MapleSAT	Programmatic MapleSAT	Result
21	$1^2 + 1^2 + 1^2 + 9^2$	95.13	0.22	SAT
21	$1^2 + 3^2 + 5^2 + 7^2$	73.27	1.46	SAT
21	$3^2 + 5^2 + 5^2 + 5^2$	15.69	0.83	SAT
22	$0^2 + 4^2 + 6^2 + 6^2$	162.70	1.02	SAT
22	$2^2 + 2^2 + 4^2 + 8^2$	44.39	0.22	SAT
23	$1^2 + 1^2 + 3^2 + 9^2$	12595.27	102.03	UNSAT
23	$3^2 + 3^2 + 5^2 + 7^2$	481.19	30.41	SAT
24	$0^2 + 4^2 + 4^2 + 8^2$	1690.09	6.36	SAT
25	$1^2 + 1^2 + 7^2 + 7^2$	57.29	13.29	SAT
25	$1^2 + 3^2 + 3^2 + 9^2$	8051.75	42.68	SAT
25	$1^2 + 5^2 + 5^2 + 7^2$	421.95	17.04	SAT
25	$5^2 + 5^2 + 5^2 + 5^2$	68.14	28.39	SAT
26	$0^2 + 0^2 + 2^2 + 10^2$	1685.26	19.12	SAT
26	$0^2 + 2^2 + 6^2 + 8^2$	2078.38	6.74	SAT
26	$4^2 + 4^2 + 6^2 + 6^2$	60284.93	8.86	SAT
27	$1^2 + 1^2 + 5^2 + 9^2$	12997.81	44.92	SAT
27	$1^2 + 3^2 + 7^2 + 7^2$	32998.14	201.38	SAT
27	$3^2 + 3^2 + 3^2 + 9^2$	TO	2103.05	UNSAT
27	$3^2 + 5^2 + 5^2 + 7^2$	4543.09	147.52	SAT
28	$2^2 + 2^2 + 2^2 + 10^2$	35768.54	48.03	SAT
28	$2^2 + 6^2 + 6^2 + 6^2$	1030.11	12.38	SAT
28	$4^2 + 4^2 + 4^2 + 8^2$	TO	TO	TO
29	$1^2 + 3^2 + 5^2 + 9^2$	TO	1189.22	SAT
29	$3^2 + 3^2 + 7^2 + 7^2$	TO	12144.50	UNSAT
30	$0^2 + 2^2 + 4^2 + 10^2$	85258.48	127.09	SAT
30	$2^2 + 4^2 + 6^2 + 8^2$	10269.38	73.21	SAT

Timings in seconds, with a timeout (TO) of 24 hours

Sum-of-squares results II

n	Decomposition	Normal MapleSAT	Programmatic MapleSAT	Result
31	$1^2+5^2+7^2+7^2$	TO	10491.08	SAT
31	$5^2+5^2+5^2+7^2$	TO	1971.16	SAT
32	$0^2+0^2+8^2+8^2$	TO	100.66	SAT
33	$1^2+1^2+3^2+11^2$	TO	21332.12	SAT
33	$1^2+5^2+5^2+9^2$	TO	7474.67	SAT
33	$3^2+5^2+7^2+7^2$	TO	47245.16	SAT
34	$0^2+0^2+6^2+10^2$	TO	550.86	SAT
34	$0^2+6^2+6^2+8^2$	TO	373.74	SAT
34	$2^2+2^2+8^2+8^2$	TO	402.70	SAT
34	$2^2+4^2+4^2+10^2$	TO	3345.30	SAT
36	$2^2+2^2+6^2+10^2$	TO	687.05	SAT
36	$6^2+6^2+6^2+6^2$	TO	555.97	SAT
38	$0^2+2^2+2^2+12^2$	TO	30178.19	SAT
38	$0^2+4^2+6^2+10^2$	TO	12810.39	SAT
38	$4^2+6^2+6^2+8^2$	TO	23925.97	SAT
40	$0^2+0^2+4^2+12^2$	TO	22969.16	SAT
40	$4^2+4^2+8^2+8^2$	TO	1864.23	SAT
42	$0^2+2^2+8^2+10^2$	TO	11233.80	SAT

Timings in seconds, with a timeout (TO) of 24 hours
Cases with no results are not shown

Compression

5-compression

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

$$A^{(2)} = \left[a_0 + a_2 + a_4 + a_6 + a_8, \quad a_1 + a_3 + a_5 + a_7 + a_9\right].$$

2-compression

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

$$A^{(5)} = \left[a_0 + a_5, \quad a_1 + a_6, \quad a_2 + a_7, \quad a_3 + a_8, \quad a_4 + a_9\right].$$

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 composite order n there are a lot fewer possible *compressions* of Williamson sequences than there are possible Williamson sequences.
- We can use a CAS to generate all possible compressions and generate a SAT instance for each possible compression.

Compression results I

n	Decomposition	Normal MapleSAT	Programmatic MapleSAT	Result
25	$1^2+1^2+7^2+7^2$	0.37	0.10	SAT
25	$1^2+3^2+3^2+9^2$	2.69	0.04	SAT
25	$1^2+5^2+5^2+7^2$	0.61	0.12	SAT
25	$5^2+5^2+5^2+5^2$	3.34	0.04	SAT
26	$0^2+0^2+2^2+10^2$	0.02	0.02	SAT
26	$0^2+2^2+6^2+8^2$	0.02	0.02	SAT
26	$4^2+4^2+6^2+6^2$	0.03	0.03	SAT
27	$1^2+1^2+5^2+9^2$	0.03	0.05	SAT
27	$1^2+3^2+7^2+7^2$	0.19	0.03	SAT
27	$3^2+3^2+3^2+9^2$	7.29	0.35	UNSAT
27	$3^2+5^2+5^2+7^2$	0.12	0.03	SAT
28	$2^2+2^2+2^2+10^2$	0.10	0.07	SAT
28	$2^2+6^2+6^2+6^2$	0.11	0.05	SAT
28	$4^2+4^2+4^2+8^2$	0.22	0.22	UNSAT
30	$0^2+2^2+4^2+10^2$	0.07	0.02	SAT
30	$2^2+4^2+6^2+8^2$	0.03	0.02	SAT
32	$0^2+0^2+8^2+8^2$	4.31	4.18	SAT
33	$1^2+1^2+3^2+11^2$	1.17	0.38	SAT
33	$1^2+1^2+7^2+9^2$	0.59	0.26	SAT
33	$1^2+5^2+5^2+9^2$	1.23	0.43	SAT
33	$3^2+5^2+7^2+7^2$	0.48	0.22	SAT
34	$0^2+0^2+6^2+10^2$	1.25	0.31	SAT
34	$0^2+6^2+6^2+8^2$	0.05	0.03	SAT
34	$2^2+2^2+8^2+8^2$	0.04	0.02	SAT
34	$2^2+4^2+4^2+10^2$	0.13	0.09	SAT

Timings in seconds, using 50 processors in parallel

Compression results II

n	Decomposition	Normal MapleSAT	Programmatic MapleSAT	Result
35	$1^2+3^2+3^2+11^2$	410.79	11.07	UNSAT
35	$1^2+3^2+7^2+9^2$	671.05	20.44	UNSAT
35	$3^2+5^2+5^2+9^2$	311.26	9.15	UNSAT
36	$0^2+0^2+0^2+12^2$	6.00	6.42	UNSAT
36	$0^2+4^2+8^2+8^2$	3.45	3.89	UNSAT
36	$2^2+2^2+6^2+10^2$	0.48	0.14	SAT
36	$6^2+6^2+6^2+6^2$	0.45	0.06	SAT
38	$0^2+2^2+2^2+12^2$	0.36	0.08	SAT
38	$0^2+4^2+6^2+10^2$	0.19	0.03	SAT
38	$4^2+6^2+6^2+8^2$	0.36	0.07	SAT
39	$1^2+3^2+5^2+11^2$	301.85	17.48	UNSAT
39	$1^2+5^2+7^2+9^2$	259.43	16.72	UNSAT
39	$3^2+7^2+7^2+7^2$	126.16	4.86	UNSAT
39	$5^2+5^2+5^2+9^2$	30.11	1.89	SAT
40	$0^2+0^2+4^2+12^2$	5.15	5.14	SAT
40	$4^2+4^2+8^2+8^2$	6.11	4.46	SAT
42	$0^2+2^2+8^2+10^2$	4.21	0.16	SAT
42	$2^2+2^2+4^2+12^2$	3.04	0.16	SAT
42	$2^2+6^2+8^2+8^2$	9.79	0.20	SAT
42	$4^2+4^2+6^2+10^2$	11.16	0.15	SAT
44	$0^2+4^2+4^2+12^2$	3.83	3.42	UNSAT
44	$2^2+6^2+6^2+10^2$	2.95	0.20	SAT
45	$1^2+1^2+3^2+13^2$	TO	1544.99	UNSAT
45	$1^2+3^2+7^2+11^2$	TO	1996.79	UNSAT
45	$1^2+7^2+7^2+9^2$	TO	1448.48	UNSAT
45	$3^2+3^2+9^2+9^2$	TO	1554.98	UNSAT
45	$3^2+5^2+5^2+11^2$	TO	1379.05	UNSAT
45	$5^2+5^2+7^2+9^2$	TO	1093.79	SAT

Timings in seconds, using 50 processors in parallel, with a timeout (TO) of 1 hour

Roadmap

In summary

- We have demonstrated the power of the SAT+CAS paradigm by using the Williamson conjecture as a case study.
- The tool MathCheck2 we have developed can successfully:
  - Show that Williamson matrices of order 35 do not exist in under a minute.
  - Show that Williamson matrices of every even order $\leqslant 45$ exist in around 30 minutes.
- The approach is applicable to other combinatorial conjectures (Kotsireas lists 11 autocorrelation-type problems alone[3]).

[3] Algorithms and Metaheuristics for Combinatorial Matrices. *Handbook of Combinatorial Optimization*, 2013

References

1. C. Bright, V. Ganesh, A. Heinle, I. Kotsireas, S. Nejati, K. Czarnecki.
   MathCheck2: A SAT+CAS Verifier for Combinatorial Conjectures,
   Computer Algebra in Scientific Computing, 2016.

2. 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.

3. C. Bright, V. Ganesh, A. Heinle, I. Kotsireas.
   New Results on Complex Golay Pairs, in submission.

4. C. Bright, R. Devillers, J. Shallit.
   Minimal Elements for the Prime Numbers, Experimental Mathematics, 2016.

Enumeration of complex Golay sequences

Order	Total Pairs	Inequivalent Pairs
1	16	1
2	64	1
3	128	1
4	512	2
5	512	1
6	2048	3
7	0	0
8	6656	17
9	0	0
10	12,288	20
11	512	1
12	36,864	52
13	512	1
14	0	0
15	0	0
16	106,496	204
17	0	0
18	24,576	24
19	0	0
20	215,040	340
21	0	0
22	8192	12
23	0	0
24	786,432	1056
25	0	0

Minimal primes in base 15

2, 3, 5, 7, B, D, 14, 18, 1E, 41, 94, 9E, A1, C1, E1, 111, 681, 698, 801, 988, 991, 9C8, A98, C98, 1091, 1691, 4498, 4898, 49A8, 6061, 6191, 6601, 6911, 8098, 8191, 8881, 8908, 8968, 8E98, 9011, 9611, 96A8, 9811, 9A08, 9AA8, E898, E9A8, EE98, 19001, 19601, 40968, 49668, 49998, 86661, 88898, 89998, 900A8, 91061, 96068, E0098, E0968, E9608, 190661, 490068, 490608, 666661, 9099A8, 90A668, 910001, 9909A8, 999068, E90008, 9000668, 9006008, 9090968, 9660008, 9900968, 9996008, 9999908, 9A66668, E999998, 90000008, 90099668, 90666668, 90909998, 90990998, 90996668, 99099098, 99900998, 99966608, 99966668, 99999668, 99999998, E9066668, 900666608, 909990098, 966666008, 9000099998, E966666666666668, 966 · · · [100 missing 6s] · · · 6608

Thank you!

1. Williamson matrices
    - Proof that Williamson matrices of order 35 do not exist.
    - Enumeration of all Williamson matrices in orders up to 45, including even orders (open since first defined in 1944).
2. Complex Golay sequences
    - Enumeration of all complex Golay sequences up to order 25.
    - Proof that complex Golay sequences of order 23 do not exist (conjectured in 2002, shown in 2013).
3. Minimal primes
    - Enumeration of all minimal primes in bases up to 16 and several other bases (open since 2000).

Questions?