Enumeration of Complex Golay Pairs via Programmatic SAT

Curtis Bright Ilias Kotsireas
Albert Heinle Vijay Ganesh

Symbolic Computation Group, University of Waterloo
Computer Aided Reasoning Group, University of Waterloo
Computer Algebra Research Group, Wilfrid Laurier University

July 17, 2018

SAT + CAS

SAT + CAS

Brute force

SAT + CAS

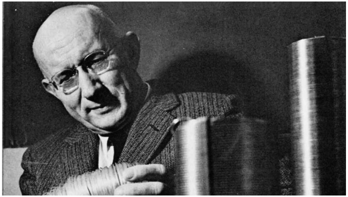
Brute force + Cleverness

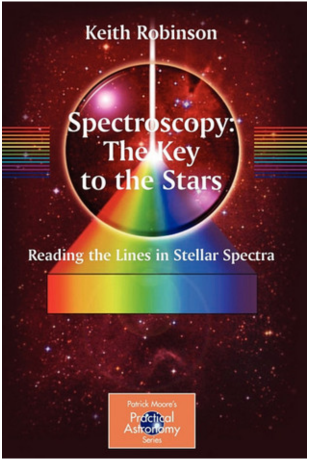
The research areas of SMT [SAT Modulo Theories] solving and symbolic computation are quite disconnected. [. . .] More common projects would allow to join forces and commonly develop improvements on both sides.

Dr. Erika Ábrahám
RWTH Aachen University
ISSAC 2015 Invited talk

Golay pairs

- Golay pairs, termed *complementary series* by Marcel Golay, were introduced in 1949 to solve a problem in multi-slit spectrometry.





Definition

- Let A and B be polynomials with ± 1 coefficients and degree $n-1$. They are a *Golay pair* if

$$|A(z)|^2 + |B(z)|^2 = 2n$$

for all z on the unit circle.

Example

- $A = 1 + z$ and $B = 1 - z$ are a Golay pair since for z on the unit circle we have

$$|1 + z|^2 + |1 - z|^2 = 4.$$

Norm test

- If A, B is a Golay pair then

$$|A(z)|^2 \leq 2n \quad \text{and} \quad |B(z)|^2 \leq 2n$$

for all z on the unit circle.

Sum-of-squares test

- If A, B is a Golay pair then

$$|A(z)|^2 + |B(z)|^2 = 2n$$

  is a decomposition of $2n$ into two *integer* squares when z is ± 1.

Alternate definition

- ± 1-sequences $A = [a_0, \ldots, a_{n-1}]$ and $B = [b_0, \ldots, b_{n-1}]$ are a *Golay pair* if

$$\sum_{k=0}^{n-s-1} a_k a_{k+s} + \sum_{k=0}^{n-s-1} b_k b_{k+s} = 0$$

for $s = 1, \ldots, n-1$.

Alternate definition

- ± 1-sequences $A = [a_0, \ldots, a_{n-1}]$ and $B = [b_0, \ldots, b_{n-1}]$ are a *Golay pair* if

$$\sum_{k=0}^{n-s-1} a_k a_{k+s} + \sum_{k=0}^{n-s-1} b_k b_{k+s} = 0$$

for $s = 1, \ldots, n-1$.

$N_A(s)$: A measure of how much A is correlated with itself with the first s entries removed.

Example

- $A = [1, 1, 1, -1]$ and $B = [1, 1, -1, 1]$ are a Golay pair since

$$\begin{aligned} N_A(1) + N_B(1) &= 1 + (-1) = 0 \\ N_A(2) + N_B(2) &= 0 + 0 = 0 \\ N_A(3) + N_B(3) &= (-1) + 1 = 0. \end{aligned}$$

Problem

- Golay found Golay pairs in lengths 2, 10, and 26.
- Golay pairs of length $2^a 10^b 26^c$ can be constructed using these "primitive" pairs but it is conjectured that Golay pairs exist in no other lengths.
- Borwein and Ferguson have searched lengths up to 100.

Peter Borwein and Ron Ferguson. A complete description of Golay pairs for lengths up to 100. *Mathematics of computation*, 2004.

Generalization

- What if we allow sequences with $\{\pm 1, \pm i\}$ entries?

Generalization

- What if we allow sequences with $\{\pm 1, \pm i\}$ entries?
- The defining relationship remains exactly the same, only need to modify the autocorrelation function:

$$N_X(s) := \sum_{k=0}^{n-s-1} x_k \overline{x_{k+s}}$$

Generalization

- What if we allow sequences with $\{\pm 1, \pm i\}$ entries?
- The defining relationship remains exactly the same, only need to modify the autocorrelation function:

$$N_X(s) := \sum_{k=0}^{n-s-1} x_k \overline{x_{k+s}}$$

- Sum-of-squares decomposition is now

$$\mathrm{Re}(A(z))^2 + \mathrm{Im}(A(z))^2 + \mathrm{Re}(B(z))^2 + \mathrm{Im}(B(z))^2 = 2n.$$

Example

- $A = [1, 1, -1]$ and $B = [1, i, 1]$ are a complex Golay pair since

$$N_A(1) + N_B(1) = 0 + 0 = 0$$
$$N_A(2) + N_B(2) = (-1) + 1 = 0.$$

Fiedler's theorem

- Let $A = A_{\text{even}} + A_{\text{odd}}$ be a decomposition of A into terms with even degree and terms with odd degree, e.g., $1 + z + z^2 = (1 + z^2) + z$.
- If A, B is a complex Golay pair then

$$|A_{\text{even}}(z)|^2 + |A_{\text{odd}}(z)|^2 + |B_{\text{even}}(z)|^2 + |B_{\text{odd}}(z)|^2 = 2n$$

for all z on the unit circle.

Frank Fiedler. Small Golay sequences. *Advances in mathematics of communications*, 2013.

Preprocessing: Enumerate A_{even} and A_{odd}

- We will find lists of the A_{even} and A_{odd} which pass the norm tests

$$|A_{\text{even}}(z)|^2 \leq 2n \quad \text{and} \quad |A_{\text{odd}}(z)|^2 \leq 2n$$

  for $M = 2^{14}$ equally-spaced points on the unit circle.
- Can compute via brute force for $n \approx 30$.

Stage 1: Enumerate possibilities for A

- For all A_{even} and A_{odd} found in the preprocessing, we form $A = A_{\text{even}} + A_{\text{odd}}$ and filter those which fail either the norm test or the sums-of-squares test. That is, those for which

$$\mathrm{Re}(A(z))^2 + \mathrm{Im}(A(z))^2 + x^2 + y^2 = 2n$$

has no integer solutions x, y for when z is ± 1 or $\pm i$.

Stage 2: Construct B from A

- Given A, generate a SAT instance which encodes the property of (A, B) being a complex Golay pair.
- Let $v_0, \ldots, v_{2n-1}$ be variables which represent the entries of B under the following encoding scheme:

v_{2k}	v_{2k+1}	b_k
F	F	1
F	T	-1
T	F	i
T	T	$-i$

SAT instance

- How to encode the property of A, B being a complex Golay pair into a SAT instance?
- That is, $N_A(s) + N_B(s) = 0$ for $s = 1, \ldots, n-1$.
- We use a SAT solver custom-tailored to this problem which can *programmatically* learn logical facts.

Example

- If $A = [1, 1, -1]$ then $N_A(1) = 0$ and $N_A(2) = -1$.
- Say during the search the SAT solver tries assigning

$$\begin{array}{cccccc} v_0 & v_1 & v_2 & v_3 & v_4 & v_5 \\ \mathrm{F} & \mathrm{F} & ? & ? & \mathrm{T} & \mathrm{T} \end{array}$$

- $B = [1, ?, -i]$ and $N_A(2) + N_B(2) = -1 + i \neq 0$, so we can learn the clause which says at least one of these variables must be assigned differently:

$$v_0 \lor v_1 \lor \neg v_4 \lor \neg v_5.$$

A product theorem

- We proved that if A, B is a complex Golay pair then $a_k a_{n-k-1} b_k b_{n-k-1} = \pm 1$ for $k = 0, \ldots, n-1$.
- From this we deduce if exactly one of $\{b_k, b_{n-k-1}\}$ is real. If so, we learn the following:

$$v_{2k} \vee v_{2(n-k-1)}$$

$$\neg v_{2k} \vee \neg v_{2(n-k-1)}$$

Implementation

- We implemented this algorithm using C and C++ to do the enumerations, MAPLE to form the sum-of-squares decompositions, and FFTW to compute the values of $A(z)$ at equally-spaced points along the unit circle.

Results

- We split the enumeration work across 25 Intel Xeon 2.1 GHz processors and enumerated all complex Golay pairs up to length 25 in 40 realtime hours.
- There are no complex Golay pairs in lengths 23 or 25 but there are 786,432 complex Golay pairs of length 24 (1056 up to an equivalence).
- Available on the MathCheck website:

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

Future optimizations?

- Could the norm test could be done more efficiently by computing the maximum of $|A(z)|^2$ for z on the unit circle?
- Could we make the SAT solver more efficient by encoding other theorems about complex Golay sequences?

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 CAS functions as well as some kind of 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.