The SAT+CAS Paradigm and the Williamson Conjecture

Curtis Bright
University of Waterloo

Ilias Kotsireas
Wilfrid Laurier University

Vijay Ganesh
University of Waterloo

Brute-brute force has no hope. But clever, inspired brute force is the future. –Doron Zeilberger

Motivation

Many mathematical conjectures concern the existence or nonexistence of combinatorial objects that 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.

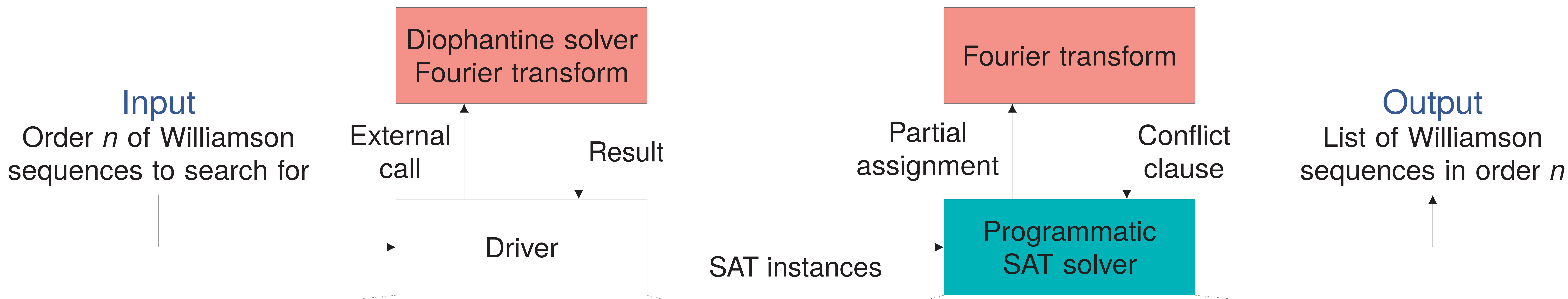
The Williamson Conjecture

Symmetric ±1-sequences A, B, C, D of length n are called *Williamson* if their out-of-phase periodic autocorrelations sum to zero. It had been conjectured that Williamson sequences exist for all orders n but the counterexample 35 was found in 1993.

Results

Williamson sequences were enumerated for odd orders up to 59 in 2007. Our work extends this to orders up to 70 divisible by 2 or 3, finding thousands of new Williamson sequences. We do this by combining satisfiability checking (**SAT** solvers) with symbolic computation (**CAS** functions).

The MathCheck SAT+CAS System



With the help of an external CAS a driver script splits the search into subspaces and generates a SAT instance for each subspace. Some instances can be immediately ruled out because they encode subspaces which violate theorems that Williamson sequences are known to satisfy.

A SAT solver performs an exhaustive search through each subspace. Periodically it will compute the Fourier transform of the potential Williamson sequences to ensure that its values have small enough norm. If the norm is too large, a clause is learned which blocks this sequence.