FourierSAT: A Fourier Expansion-Based Algebraic Framework for Solving Hybrid Boolean Constraints

Anastasios Kyrillidis

Anshumali Shrivastava

Moshe Vardi

Zhiwei Zhang

Computer Science Dept., Rice University

Background: Boolean SATisfiability Problem

RICE UNIVERSITY

- Variables: $x, y, z... \in \{T, F\}$
- Connectives: $\neg(Not), \wedge(and), \vee(or), \oplus(xor)...$
- Formula: $(x \wedge \neg y) \oplus z \ ...$
- Solution: an assignment with T/F of variables s.t. formula yields T

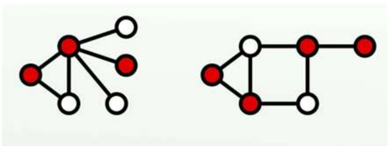
- SAT: Does a formula have a solution or not?

  $x = T, y = F$ is a solution of $x \wedge \neg y$

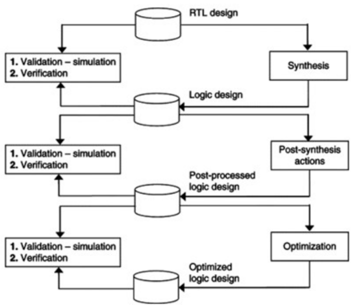
  no solution exists for $x \wedge \neg x$
- NP-completeness of SAT was proven in 1971 by Stephen Cook

Applications of SAT

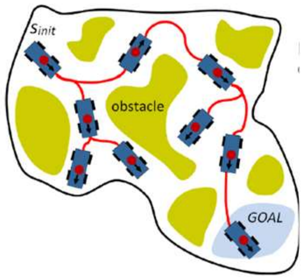
Used by hardware and software designers on a daily basis



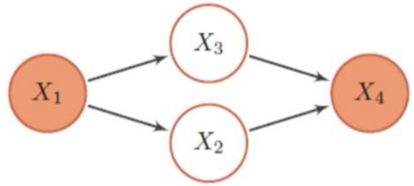
Discrete Optimization
[Ignatiev et al., 2017]



Software Verification
[Velev, 2004]



Motion planning
[Bera, 2017]



Probabilistic inference
[Chavira et al., 2008]

SAT solvers solve industrial SAT instances with millions of variables
[Katebi et al., 2011]

CNF and Hybrid SAT Solving

RICE UNIVERSITY

- Conjunctive Normal Form (CNF)
  - Connectives: $\neg, \wedge, \vee$
  - Clauses: $x_1 \vee x_2 \vee \neg x_3 \ \ldots$
  - Formulas: $(x_1 \vee x_2 \vee \neg x_3) \wedge (x_2 \vee x_4) \ \ldots$
  - 3-CNF is NP-complete [Cook, 1971]

- Non-CNF Clauses/Constraints
  - cryptography: XOR [Bogdanov et al., 2011]
  - graph theory: cardinality constraints [Costa et al., 2009]
    not-all-equal (NAE) [Tomas J, 1978]

$$x \oplus y \oplus z$$

$$x + y + z \geq 2$$

$$NAE(x, y, z) = \neg(x = y = z)$$

Related Work: Hybrid SAT Solving

RICE UNIVERSITY

- CNF-encoding of Non-CNF constraints

  Involves large number of new variables and clauses [Wynn, 2018]

  Encodings make a big difference [Prestwich 2009]

- Extensions of CNF solvers

  Cryptominisat (CNF + XOR) [Soos et al., 2009]
  Minicard (CNF + cardinality constraints) [Liffition et al., 2012]
  MonoSAT (CNF + graph properties) [Bayless et al. 2015]
  Pueblo (CNF + pseudo Boolean constraints) [Sheini et al., 2006]

  Need to design algorithms for each specific type of constraints

Contribution: A versatile Boolean SAT Solver

RICE UNIVERSITY

$$f = c_1 \wedge c_2 \wedge \cdots \wedge c_m$$

Each c_i can be a CNF, XOR, Not-all-equal constraint or cardinality constraint

Goal: Handle different types of constraints uniformly & naturally

$FourierSAT$

Fourier Expansion of Boolean Function

RICE UNIVERSITY

Boolean formulas → Multilinear Polynomials

$f:\{1,-1\}^n \rightarrow \{1,-1\}$ → $p:\{1,-1\}^n \rightarrow \{1,-1\}$

{F, T}

$x \wedge y$ → $\frac{1}{2}\cdot 1+\frac{1}{2}\cdot x+\frac{1}{2}\cdot y-\frac{1}{2}\cdot xy$

x	y	$x \wedge y$	$\frac{1}{2}+\frac{1}{2}x+\frac{1}{2}y-\frac{1}{2}xy$
1	1	1	1
1	-1	1	1
-1	1	1	1
-1	-1	-1	-1

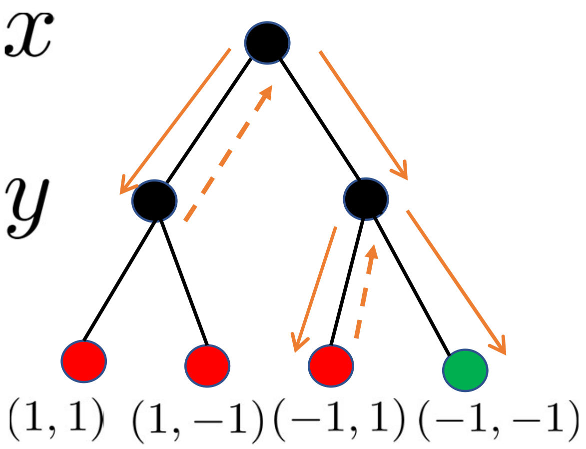
Theorem (Walsh-Fourier Transform)

Every Boolean function has a unique representation in multilinear polynomial.

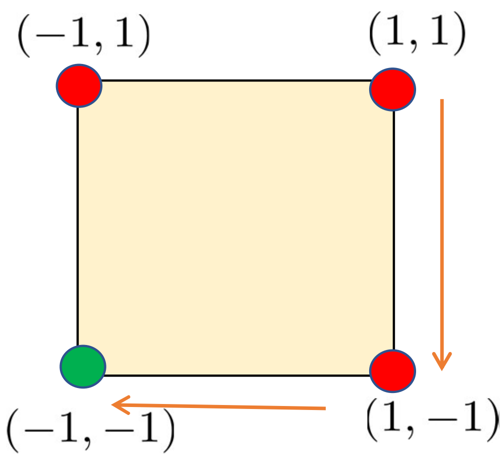
From SAT to continuous optimization

$$x \wedge y$$

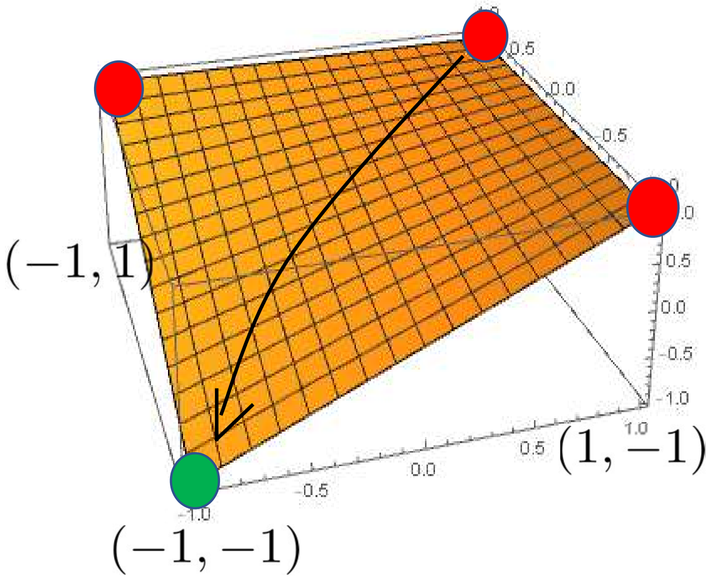
$$\frac{1}{2} + \frac{1}{2}x + \frac{1}{2}y - \frac{1}{2}xy$$



Tree Search/Backtracking



Local Search



discrete searching on Boolean domain

optimization on continuous domain

Workflow

RICE UNIVERSITY

$f = (x_1 \vee \neg x_2)$
$\wedge(x_2 \oplus x_3 \oplus x_4)$
$\wedge(x_4 + x_5 + x_6 + x_9 \geq 2)$
… **hybrid Boolean formula**

Fourier transform →

$$F = -0.32 + 0.02x_1 - 0.03x_2 + 0.04x_3 - 0.007x_4 + \cdots + 0.000875x_5x_6x_7x_8x_9 + \cdots$$

multilinear polynomial

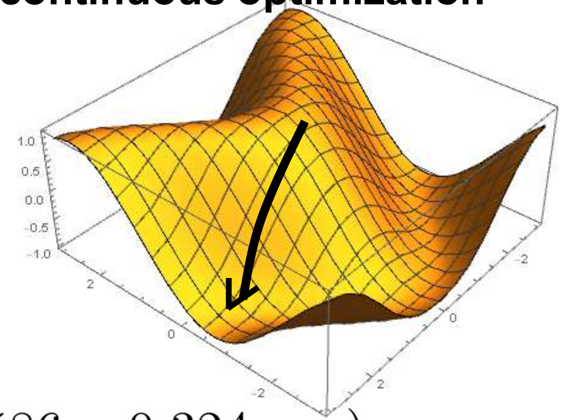
analytical computation →

$$\frac{\partial F}{\partial x_1} = 0.003x_2 + \cdots$$
$$\frac{\partial F}{\partial x_2} = 0.008x_1 + \cdots$$
$\cdots$

gradients

→

continuous optimization



$(0.586, -0.324, \cdots)$

discretize →

$(1, -1, \cdots)$

discrete assignment

↑

Is a solution?

No → continuous optimization

Factored Representation

RICE UNIVERSITY

- Generally, computing the Fourier Expansion of a Boolean function is #P-hard
- How to evaluate a polynomial with exponentially many terms?

$$f = c_1 \wedge c_2 \wedge \cdots \wedge c_m$$

- Many types of constraints has closed form Fourier expansions

Type of Constraint	Example	Fourier Expansion
CNF clauses	$x \wedge y$	$\frac{1}{2} + \frac{1}{2}x + \frac{1}{2}y - \frac{1}{2}xy$
XOR	$x \oplus y \oplus z$	$x \cdot y \cdot z$
Cardinality constraints	$x + y + z \geq 2$	$\frac{1}{2}x + \frac{1}{2}y + \frac{1}{2}z - \frac{1}{2}xyz$
Not-all-equal	$NAE(x, y, z)$	$-\frac{1}{2} + \frac{1}{2}xy + \frac{1}{2}yz + \frac{1}{2}xz$

Define a new objective function by the Fourier Expansion of each clause

Objective Function Construction

RICE UNIVERSITY

$$f = c_1 \wedge c_2 \wedge \cdots \wedge c_m$$

$$F = p_1 + p_2 + \cdots + p_m$$

$$F = \sum_{i=1}^{m} p_i$$

Fourier expansions

$$f = (x \vee \neg y) \bigwedge (x \oplus y)$$

$$F = (-\tfrac{1}{2} + \tfrac{1}{2}x - \tfrac{1}{2}y - \tfrac{1}{2}x \cdot y) + (x \cdot y)$$

$$= -\frac{1}{2} + \frac{1}{2}x - \frac{1}{2}y + \frac{1}{2}x \cdot y$$

Theorem

$$f \text{ is SAT} \Leftrightarrow \underset{x \in [-1,1]^n}{Min}(F) = -m$$

Theoretical Properties of FourierSAT

RICE UNIVERSITY

Randomized Rounding:

$P[R(x)_i = -1] = \frac{1}{2} - \frac{1}{2}x_i$

$P[R(x)_i = 1] = \frac{1}{2} + \frac{1}{2}x_i$

Theorem

$F(x) = -k \Rightarrow \frac{m+k}{2}$ clauses can be satisfied in expectation

Making progress in expectation per iteration

Theorem

Every local minimum x of F can be discretized to x^* with $F(x^*) = F(x)$

$F(x) = -k$

x is a local minimum $\Rightarrow \frac{m+k}{2}$ clauses can be satisfied

(Deterministically)

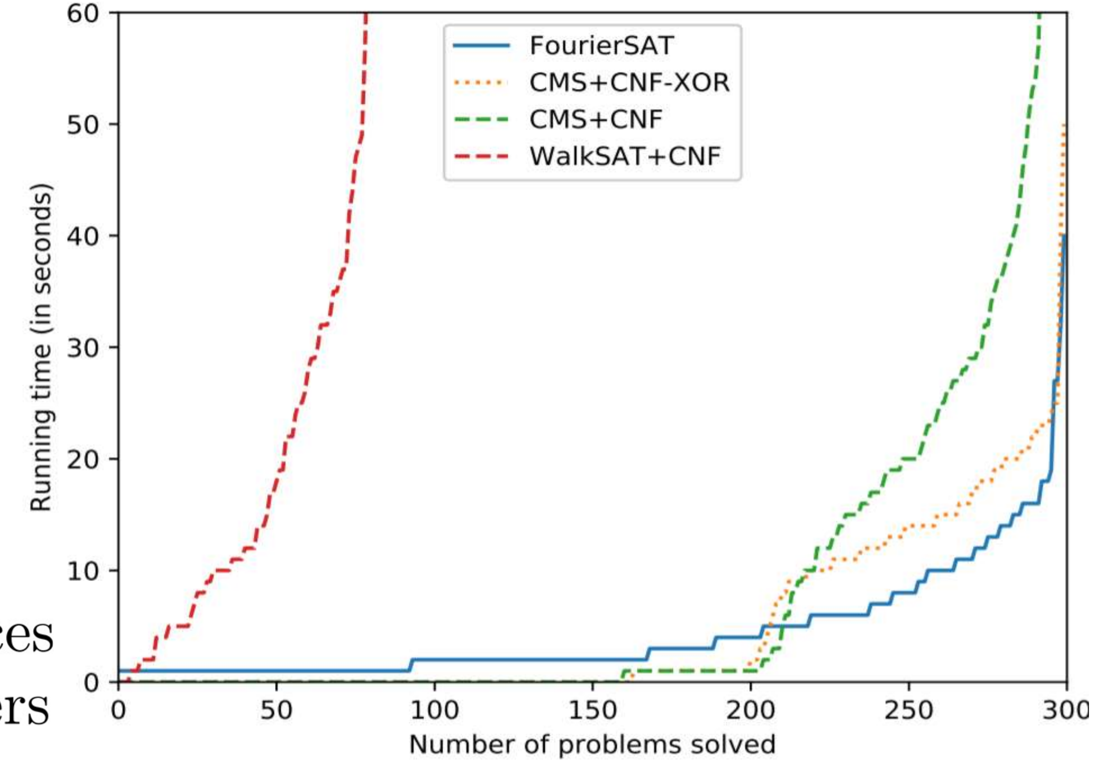
Experimental Results: Parity Learning with Errors

RICE UNIVERSITY

- Solving a random XOR system of m XOR equations and n variables but tolerating up to $e \cdot m$ equations to be violated

$$x_1 \oplus x_2 \oplus x_3 = -1$$
$$x_1 \oplus x_2 = -1$$
$$x_2 \oplus x_3 = -1$$
$$x_1 \oplus x_3 = -1$$

UNSAT for $e = 0$. SAT for $e = 0.25$



- $m = 2n$, $e = \frac{1}{4}$: Known as hard instances for both DPLL and local search SAT solvers

- XORs + 1 Cardinality Constraint

Conclusion

RICE UNIVERSITY

- SAT solving beyond CNF is worth studying
- Our work, FourierSAT is a versatile and robust tool for Boolean SAT
- Applications of Fourier analysis and other algebraic techniques for Boolean logic are promising
  - Bridging discrete and continuous optimization
- Future directions:
  - Proving unsatisfiability algebraically
  - Deploying FourierSAT with methods from machine learning and local search SAT solvers