Solving Hybrid Boolean Constraints by Fourier Expansions and Continuous Optimization

Zhiwei Zhang's M.S. thesis defense – Computer Science Department

M.S. committee:

Moshe Y. Vardi (chair)

Anastasios Kyrillidis

Anshumali Shrivastava

Background: SATisfiability Problem

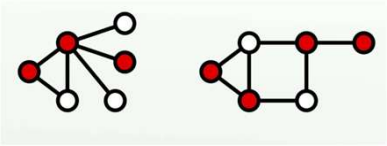
- Variables: $x, y, z... \in \{1, -1\}$ {F, T}
- Connectives: $\neg(Not), \wedge(and), \vee(or), \oplus(xor)...$
- Literals: $\neg x, y, \neg z...$
- Formula: $(x \wedge \neg y) \oplus z$ ...
- Solution: an assignment with -1/1s of variables s.t. formula yields -1
- SAT: Does a formula have a solution or not?

  $x = -1(T), y = 1(F)$ is a solution of $x \wedge \neg y$ (SAT)

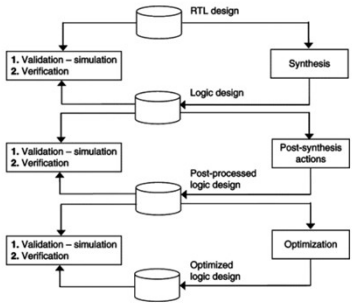
  no solution exists for $x \wedge \neg x$ (UNSAT)
- NP-completeness of SAT was proven in 1971 by Stephen Cook

Applications of SAT

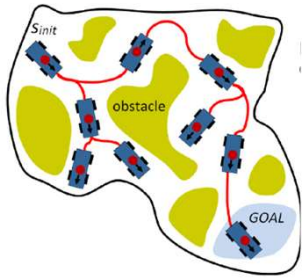
Used by hardware and software designers on a daily basis



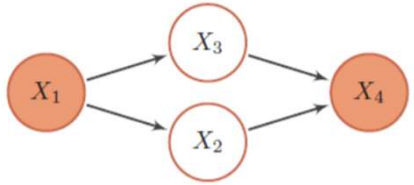
Discrete Optimization
[Ignatiev et al., 2017]



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

- 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

- CNF-encoding of Non-CNF constraints

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

  Encodings differ from size, arc-consistency and density of solutions [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

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

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

FourierSAT: A SAT solver based on gradient method to handle different types of constraints uniformly

Fourier Expansion of Boolean Function

Boolean formulas → Multilinear Polynomials

$f : \{1, -1\}^n \to \{1, -1\}$

{F, T}

$p : \{1, -1\}^n \to \{1, -1\}$

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

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

Fourier Expansion of Boolean Function

Boolean formulas → Multilinear Polynomials

Theorem

Given a Boolean function $f : \{-1,1\}^n \to \mathbb{R}$, there is a unique way of expressing f as a multilinear polynomial:

$$f(x) = \sum_{S \subseteq [n]} \left(\widehat{f}(S) \cdot \prod_{i \in S} x_i \right)$$

[O'Donnell, 2014]

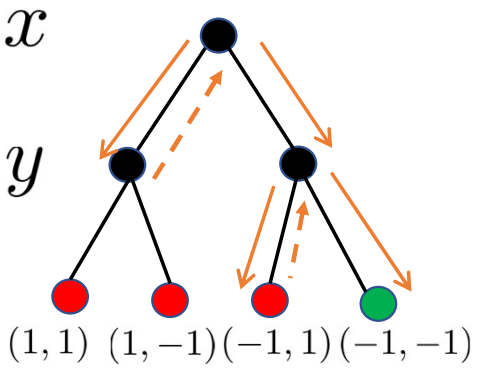
Fourier coefficients on S

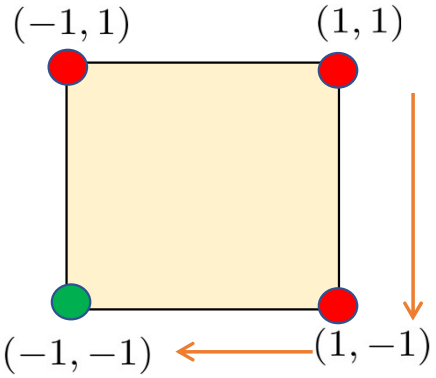
multilinear monomials

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

From SAT to continuous optimization

$$x \wedge y$$





Tree Search/Backtracking
(DPLL/CDCL)

propagation
conflict analysis …

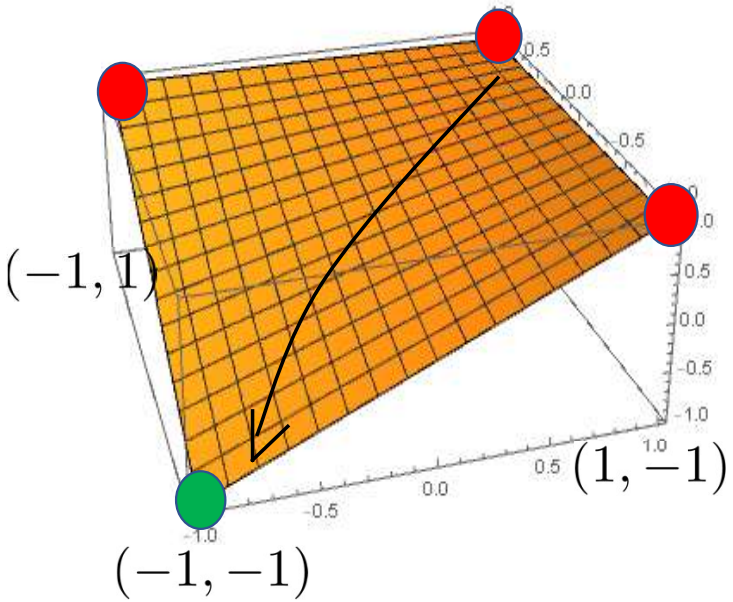
Local Search

“sideway” walk
random walk …

variable selection heuristics

discrete searching on Boolean domain

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

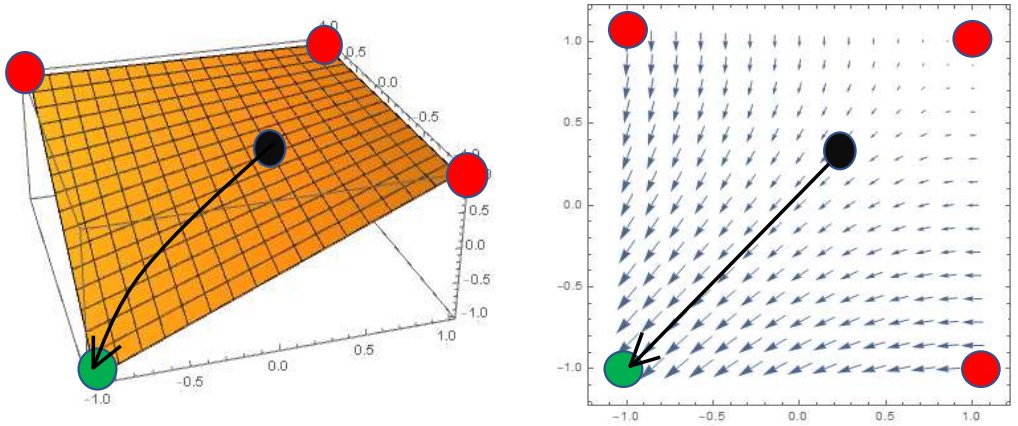


formulas can be evaluate on reals

optimization on continuous domain

Approach: From SAT to Continuous Optimization

Discrete searching on Boolean formulas → Continuous optimization on multilinear polynomials



Let multilinear polynomial G be the Fourier transform of formula f

Theorem

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

Every local minimum of G in $[-1,1]^n$ is global.

Workflow

Problems:

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

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

... **hybrid Boolean formula**

Fourier transform

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

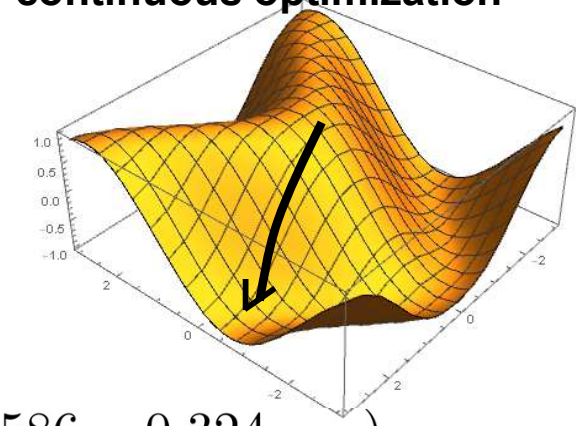
multilinear polynomial

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

Factored Representation

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

- Many symmetric constraints have closed form Fourier expansion

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

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

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

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

Fourier expansions

Objective Function Construction

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

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

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

Fourier expansions

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

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

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

- Efficient Objective Function Evaluation

  F can be evaluated in $O(k^2 \cdot m)$ time

  k --- maximum width of all clauses m--- number of clauses

Theorem

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

Workflow

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

Fourier transform

$F_1 = -0.32 + 0.02x_1 - 0.03x_2$
$F_2 = 0.04x_3 - 0.007x_4$
$F_3 = 0.000875x_5x_6x_7x_8x_9$
multilinear polynomials

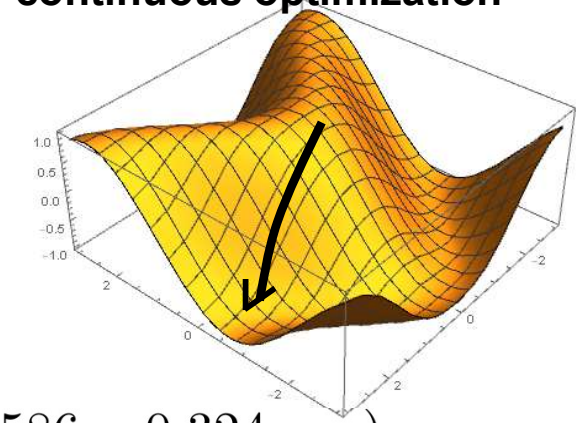
Fourier transform

$F = F_1 + F_2 + F_3$
$= -0.32 + 0.02x_1 - 0.03x_2$
$+ 0.04x_3 - 0.007x_4 + \cdots$
$+ 0.000875x_5x_6x_7x_8x_9 + \cdots$
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

Incomplete SAT solver: cannot prove unsatisfiability

Multilinear Polynomials: Well-behaved

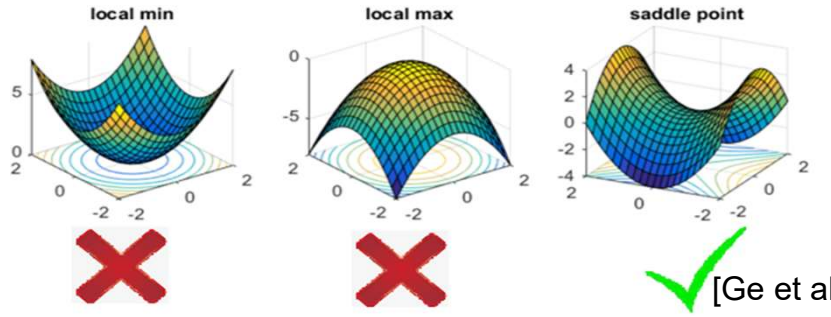
$$F = \sum_{i=1}^{m} p_i$$

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

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

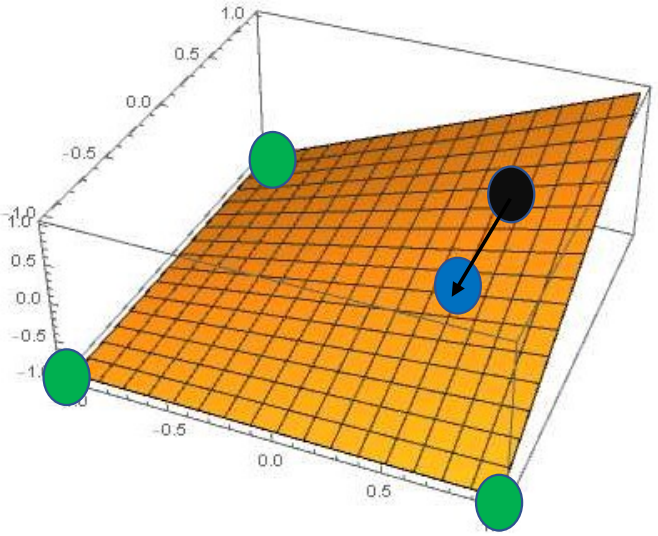
Bounded: $p_i \in [-1, 1]$ and $F \in [-m, m]$ for every $x \in [-1, 1]^n$

Theorem (Saddle Landscape)
At every $x \in \mathbb{R}^n$, $\exists$ a decreasing direction v and $\epsilon > 0$, $F(x + \epsilon v) < F(x)$



[Ge et al., 2016]

What does the Objective Function Value Indicate?



Theorem

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

Making "small" progress in expectation per iteration

Randomized Rounding:

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

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

MAXCUT Relaxitions

- LP relaxation: $\frac{3}{4}$-approximate—25% loss
- SDP relaxation: 0.878-approximate—13.2% loss
- "Fourier relaxation": no loss

Why Not Just Do Discrete Local Search?

Greedy Local Search Solver (GSAT) [Selman et al., 1992]: per iteration, flip a bit to maximize the number of satisfied clauses

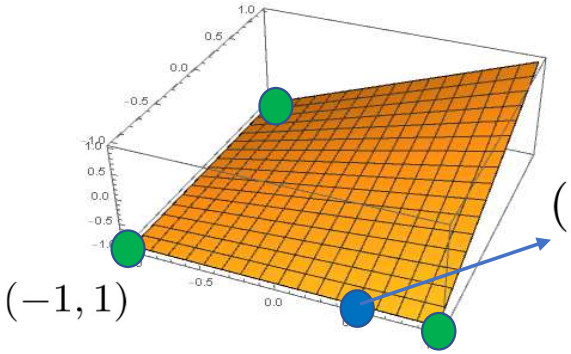
$$x_1 + x_2 + \cdots + x_{100} \geq 70, x_i \in \{0, 1\}$$

$$\text{start from } |x| = 50 \longrightarrow \text{Need to flip at least 20 bits}$$

GSAT will not make progress for a long time!

Local Minimum is “almost integer”

$F = -\frac{1}{2} + \frac{1}{2}x + \frac{1}{2}y + \frac{1}{2}xy \qquad (x \vee y)$



$\Rightarrow$ F(-1,0.5)=F(-1,1)=F(-1,-1)

Local minimum

Theorem

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

$F(x) = -k$

$\Rightarrow \frac{m+k}{2}$ clauses can be satisfied (Deterministically)

x is a local minimum

Projected Gradient Descent Converges Fast

Multilinear polynomials are smooth:

For $F \in [-\alpha, \alpha]$ and $x, y \in [-1, 1]^n$

Lipschitz continuous:

$$|F(x) - F(y)| \leq \alpha\sqrt{n} \cdot \|x - y\|_2$$

Lipschitz gradient:

$$\|\nabla F(x) - \nabla F(y)\|_2 \leq \alpha n \cdot \|x - y\|_2$$

if f is k-SAT $\quad \alpha\sqrt{k}$ $\qquad\qquad$ αk

Theorem

For a formula with n variables and m clauses, Projected Gradient Descent converges to a ϵ-projected-critical point in $O(\frac{nm^2}{\epsilon^2})$

$O(\frac{km^2}{\epsilon^2})$

Implementation Techniques

- Weighted version:

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

- Analytical Gradient Computation

  Feeding gradient to optimizer significantly accelerated the algorithm

- Random Restart and Parallelization

  Different trials are independent so that parallelization is easy

- Fast computation of gradient and function value

$$F\{x_1 \vee x_2 \vee x_3\}(-1, 0.345, -0.474) = -1$$

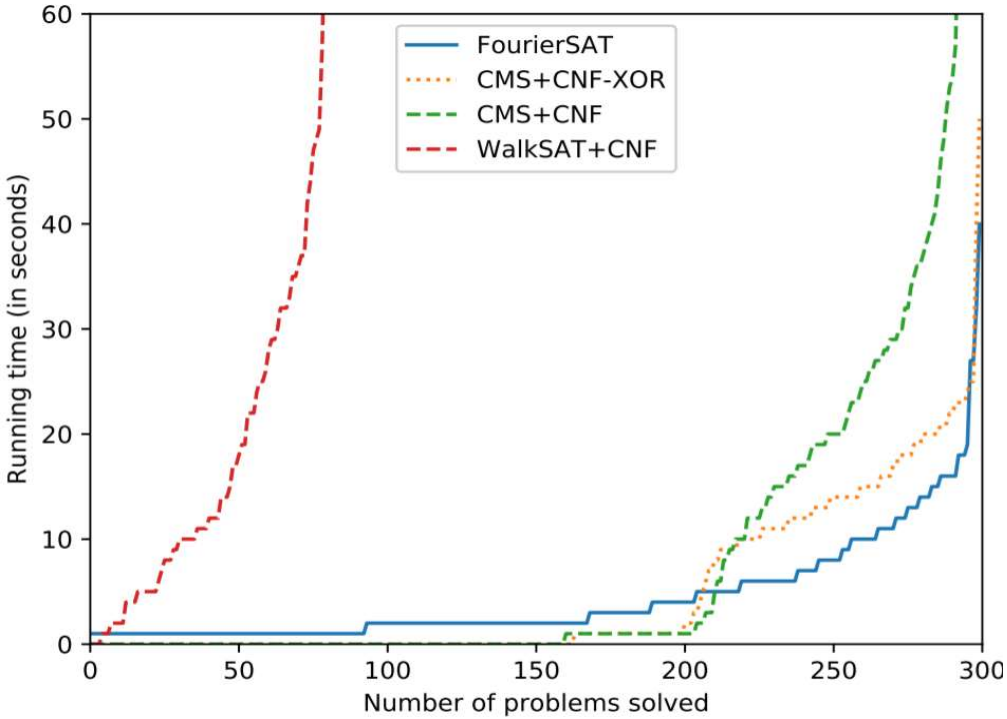
Benchmark 1: Parity Learning with Errors

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

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

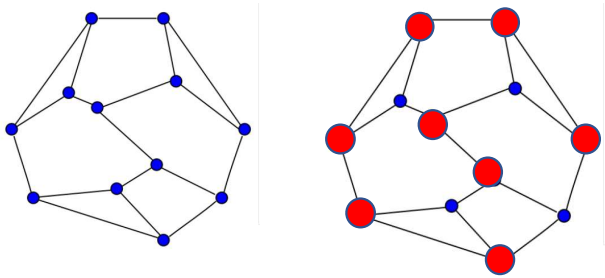
UNSAT for $e = 0$. SAT for $e = 0.25$

- $e = 0$: Gaussian Elimination (P)
  $m > n$: UNSAT w.h.p
- $e > 0$: whether in P is still open
- $m = 2n$, $e = \frac{1}{4}$: Known as hard instances for both DPLL and local search SAT solvers
- XORs + 1 Cardinality Constraint

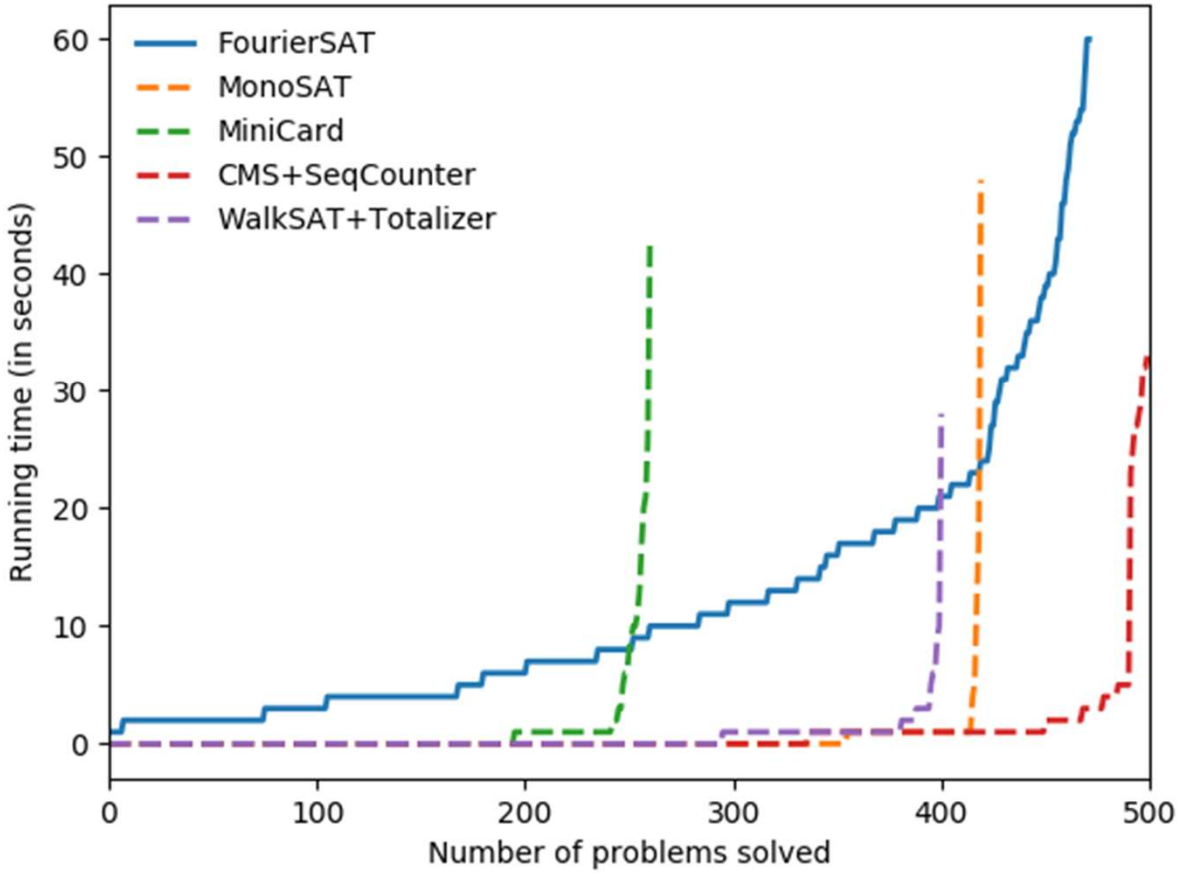


Benchmark 2: Approximate Minimum Vertex Covering

- Finding a vertex set Sol of random cubic graphs s.t. $|Sol| \leq 1.1 \cdot |Opt|$



- CNFs + 1 global cardinality Constraint



Benchmark 3: MaxSAT

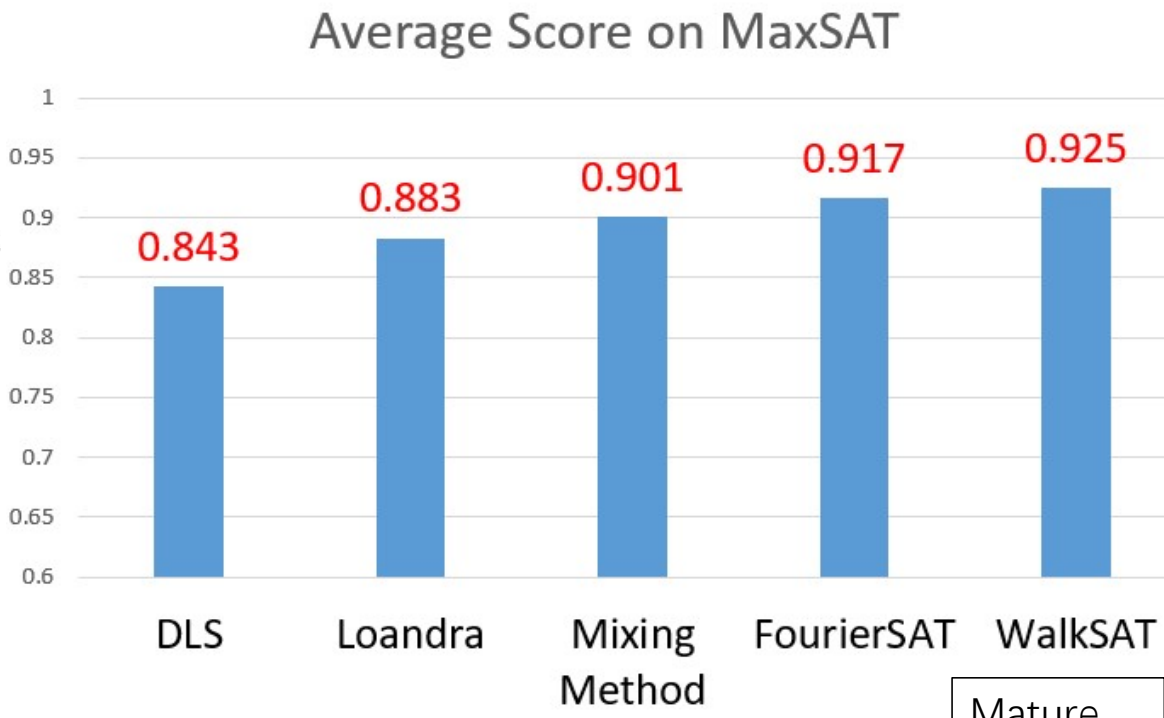
- MaxSAT: solving UNSAT instances with as few violated clauses as possible

For a solver i on instance j

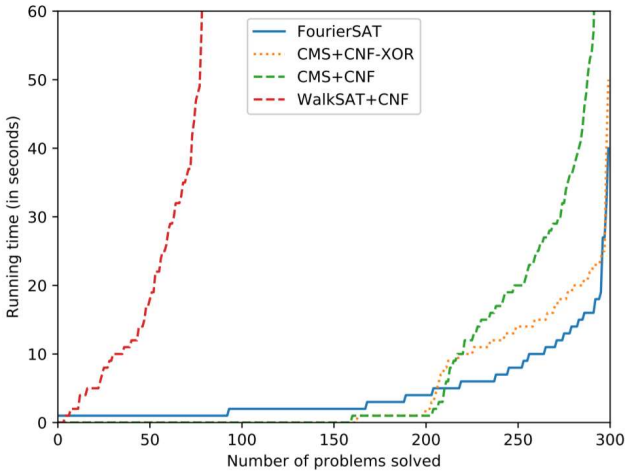
$$S_{ij} = \frac{(\text{least \#violated clauses by all solvers})+1}{(\#\text{violated clauses by solver i})+1}$$

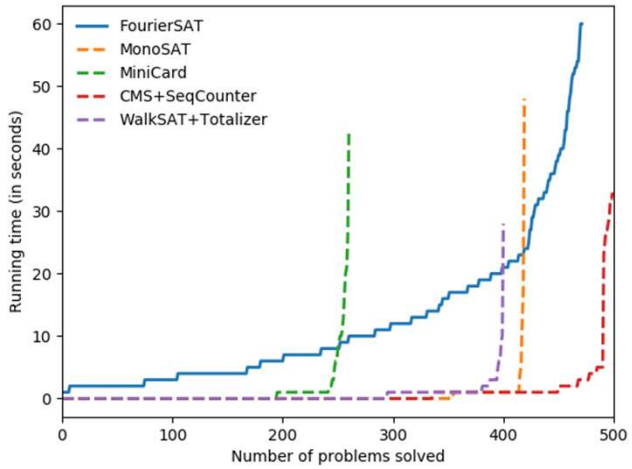
Solver	A	B	C	D
# violated clauses	2	3	10	6
Score	1	0.75	0.27	0.43

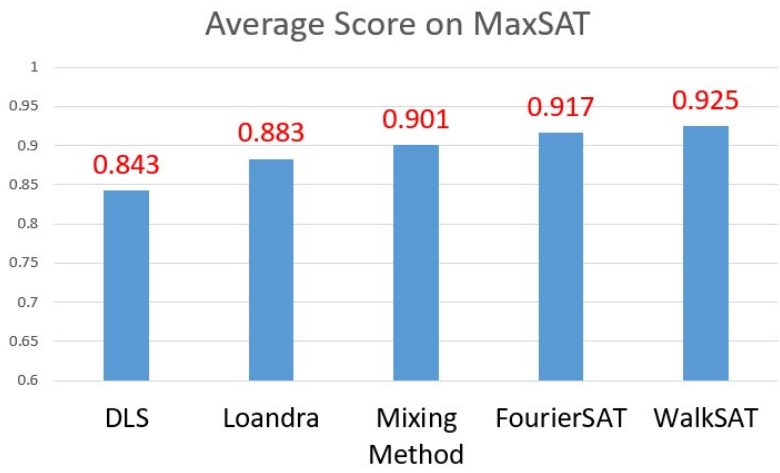
- Relatively small benchmarks form MAXSAT competition 2016



FourierSAT is Versatile and Shows Great Potential







- FourierSAT is comparable with state-of-the-art SAT/MaxSAT solvers even without lots of engineering

Conclusion

- 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 local search SAT solvers
  - Alternative object function: approximate, efficient gradient