Solving Hybrid Boolean Constraints by Fourier Expansions and Continuous Optimization

Summary of MS Thesis by Zhiwei Zhang

Vision: Recent decades have witnessed the tremendous success of two areas in computing: 1) machine-learning algorithms based on gradient descent and 2) modern CDCL-based SAT solving. Those two successful stories demonstrate the great power of computational logic (discrete) and numerical (continuous) optimization. While various fundamental theories, practical approaches, and hardware/software tools have been proposed and developed for both of the two areas, algorithmic research on leveraging the interplay between them is not abundant and is a promising research direction. **My research goal is to bridge discrete and continuous optimization by designing algorithms with ideas from both areas**.

Background: Boolean SATisfiability (SAT) is a fundamental problem in computational logic. Solving SAT efficiently is of utmost significance in computer science, both from a theoretical and a practical perspective.

As a special case of SAT, conjunctive normal forms (`CNF`s) are a conjunction (`and`-ing) of disjunctions (`or`-ing) of literals. Despite the NP-completeness of `CNF`-SAT, there has been a lot of progress on the engineering side of `CNF`-SAT solvers. Mainstream SAT solvers can be classified into complete and incomplete ones. Most modern complete SAT solvers are based on the Conflict-Driven Clause Learning (CDCL) algorithm [11]. Overall, CDCL-based SAT solvers constitute a huge success, and have been dominating in the research of SAT solving.

Local search techniques are mostly used in incomplete SAT solvers. The number of unsatisfied clauses is often regarded as the objective function. While practical local-search solvers could be slower than CDCL solvers, local search techniques are still useful for solving a certain class of benchmarks, such as hard random formulas and MaxSAT [16, 9].

Non-`CNF` constraints are playing important roles in theoretical computer science and other engineering areas, *e.g.*, `XOR` constraints in cryptography [1] as well as cardinality constraints (`CARD`) and Not-All-Equal (`NAE`) constraints in discrete optimization [3, 4]. The combination of different types of constraints enhances the practical expressive power of Boolean formulas; e.g., `CARD-XOR` is necessary and sufficient for maximum likelihood decoding (MLD) [6], one of the most crucial problems in coding theory. Nevertheless, compared to that of `CNF`-SAT solving, efficient SAT solvers that can handle non-`CNF` constraints are less well studied.

One way to deal with non-`CNF` constraints is to encode them in `CNF` [8, 14]. Different encodings, however, differ in size, arc consistency, and solution density [15]. It is generally observed that the running time of SAT solvers relies heavily on the details of encodings. Finding the best encoding for a solver usually requires considerable testing and comparison [12].

Another way is to extend existing SAT solvers to adapt to non-`CNF` constraints. Examples of work on this line include Cryptominisat [17] for `CNF-XOR` and RoundingSAT [5] for `CNF`-Pseudo-Boolean constraints. Such specialized extensions, however, often require different techniques for different types of constraints. Meanwhile, general ideas for solving hybrid constraints uniformly are still lacking.

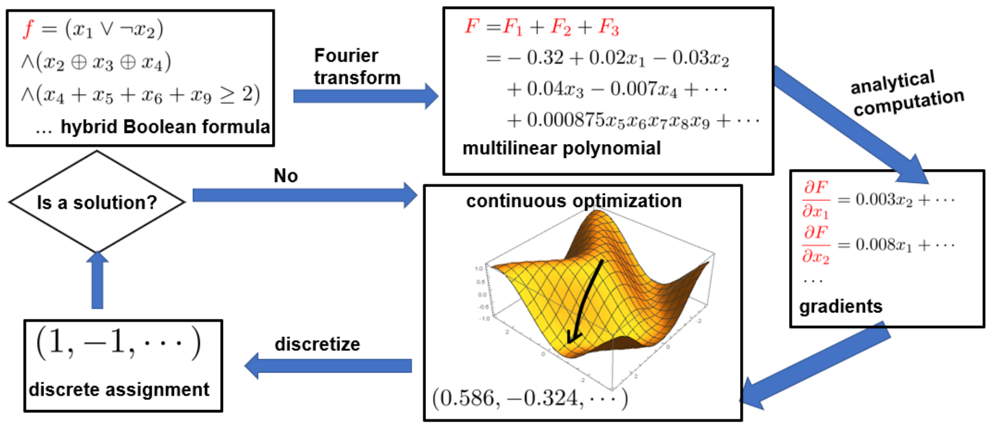

Figure 1: Workflow of `FourierSAT`.

Contributions: The primary contribution of this thesis is the design of a novel algebraic framework as well as a versatile, robust incomplete SAT solver—`FourierSAT`—for solving hybrid Boolean formulas composed of non-CNF constraints. The workflow of our method is illustrated in Figure 1. More specifically, we have the following contributions:

1. A new multi-linear polynomial objective function defined on $\mathbb{R}^n$ is proposed for hybrid Boolean satisfaction, based on Fourier Expansions of Boolean functions [13]. A reduction from Boolean satisfaction to global continuous optimization is obtained by the objective function. The proposed objective function applies to a variety of types of constraints (e.g., XOR, cardinality constraints). Thus, **different types of constraints can be handled uniformly—we no longer design specific methods for each type of constraints.** This objective function is rigorously proved to have interesting theoretical guarantees. For example, rounding from a fractional point to a discrete point does not cost the loss of objective value. Intuitively, the objective function is able to measure the progress towards satisfying more constraints, while a discrete objective can fail to do so.

2. In order to optimize the multi-linear objective function, continuous-local-search algorithms are designed in the thesis. We first consider a natural projected gradient descent (PGD) approach and prove polynomial convergence of PGD. Furthermore, our study on the local landscape of Fourier expansions reveals that the existence of saddle points is an obstacle for us to design algorithms with theoretical guarantees. Previous research shows that gradient-based algorithms are in particular susceptible to saddle point problems [7]. Therefore, we design specialized algorithms for optimizing Fourier Expansions that can escape saddle points and help convergence.

3. Extensive experimental results are provided in the thesis by comparing `FourierSAT` with state-of-the-art SAT/MaxSAT solvers on a number of benchmarks. We demonstrate that for certain classes of hybrid formulas and MaxSAT instances, `FourierSAT` shows promising potential to be a reliable solver.

We believe that the natural reduction from SAT to continuous optimization, combined with state-of-the-art constrained-continuous optimization techniques, opens a new line of research on SAT solving.

Novelty: We summarize the novel points of the work in this thesis below.

1. To our best knowledge, this thesis is the first algorithmic work to study Fourier Expansions of Boolean functions as polynomials in the real domain instead of only Boolean domain. While a successful tool in theoretical computer science [10, 18], the *Fourier analysis on Boolean functions* [13] has found fewer algorithmic applications. In this thesis, considering Fourier expansions as real polynomials exhibits a great promise as an algorithmic tool.

2. This work provides a new incomplete algorithm for SAT/MaxSAT solving by finding a real relaxation for SAT and a way to reduce SAT to continuous optimization. As CDCL-based SAT solvers are dominating on industrial benchmarks in recent decades, non-CDCL solvers are still valuable for handling specific problems [16, 9], providing theoretical results [2], and enhancing the diversity of the SAT solver family.

3. To our best knowledge, this thesis is the first work to analyze the performance of traditional gradient-based methods on optimizing general multi-linear polynomials. In addition, novel algorithms for further improving the solution quality are designed and analyzed, which also apply to multi-linear polynomials generated from other problems.

Relevance to the areas of interest:

1. Computational logic: Boolean Satisfiability and Max-Satisfiability are central problems in computational logic. Given the remarkable success of gradient-based methods in machine learning (ML), the thesis sheds some light on how logical problem solving can benefit from prevalent technologies and the development of corresponding mature tools.

2. Algorithms and computational complexity: The thesis contains multiple new optimization algorithms and rich theoretical analysis regarding discrete-continuous reduction, randomized rounding, local/global optima, saddle points, and convergence speed. We believe that the framework of `FourierSAT` built by the theory creates promising opportunities for more new theoretical and practical work.

References

[1] A. Bogdanov, D. Khovratovich, and C. Rechberger. Biclique Cryptanalysis of the Full AES. In *ASIACRYPT 2011*, 2011.

[2] T. Brueggemann and W. Kern. An Improved Deterministic Local Search Algorithm for 3-SAT. *Theoretical Computer Science*, 329(1):303 – 313, 2004.

[3] M.-C. Costa, D. de Werra, C. Picouleau, and B. Ries. Graph Coloring with Cardinality Constraints on the Neighborhoods. *Discrete Optimization*, 6(4):362 – 369, 2009.

[4] I. Dinur, O. Regev, and C. Smyth. The Hardness of 3-Uniform Hypergraph Coloring. *Combinatorica*, 25(5):519–535, Sep 2005.

[5] J. Elffers and J. Nordström. Divide and Conquer: Towards Faster Pseudo-Boolean Solving, 7 2018.

[6] J. Feldman, M. J. Wainwright, and D. R. Karger. Using Linear Programming to Decode Binary Linear Codes. *IEEE Transactions on Information Theory*, 51(3):954–972, March 2005.

[7] R. Ge, F. Huang, C. Jin, and Y. Yuan. Escaping From Saddle Points — Online Stochastic Gradient for Tensor Decomposition. *arXiv e-prints*, page arXiv:1503.02101, Mar 2015.

[8] M. Gwynne and O. Kullmann. On sat representations of xor constraints. In A.-H. Dediu, C. Martín-Vide, J.-L. Sierra-Rodríguez, and B. Truthe, editors, *Language and Automata Theory and Applications*, pages 409–420, Cham, 2014. Springer International Publishing.

[9] Z. Lei and S. Cai. Solving (weighted) partial maxsat by dynamic local search for sat. In *Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence, IJCAI-18*, pages 1346–1352. International Joint Conferences on Artificial Intelligence Organization, 7 2018.

[10] N. Linial, Y. Mansour, and N. Nisan. Constant Depth Circuits, Fourier Transform, and Learnability. In *ASFCS*, Oct 1989.

[11] J. P. Marques-Silva and K. A. Sakallah. GRASP: A Search Algorithm For Propositional Satisfiability. *IEEE Transactions on Computers*, 48(5):506–521, 1999.

[12] R. Martins, V. Manquinho, and I. Lynce. Exploiting Cardinality Encodings in Parallel Maximum Satisfiability. In *ICTAI*, pages 313–320, Nov 2011.

[13] R. O'Donnell. *Analysis of Boolean Functions*. Cambridge University Press, New York, NY, USA, 2014.

[14] T. Philipp and P. Steinke. Pblib – a library for encoding pseudo-boolean constraints into cnf. In M. Heule and S. Weaver, editors, *Theory and Applications of Satisfiability Testing – SAT 2015*, pages 9–16, Cham, 2015. Springer International Publishing.

[15] S. Prestwich. CNF Encodings, Handbook of Satisfiability: Volume 185 Frontiers in Artificial Intelligence and Applications, 2009.

[16] B. Selman, H. Levesque, and D. Mitchell. A New Method for Solving Hard Satisfiability Problems, 1992.

[17] M. Soos, K. Nohl, and C. Castelluccia. Extending SAT Solvers to Cryptographic Problems. In *SAT*, pages 244–257, 2009.

[18] C. Wei and S. Ermon. General Bounds on Satisfiability Thresholds for Random CSPs via Fourier Analysis, 2017.