Maximum Satisfiability Approach to Game Theory and Network Security

廖, 暁鵬

https://doi.org/10.15017/1441264

出版情報：九州大学, 2013, 博士（工学）, 課程博士
バージョン：
権利関係：全文ファイル公表済

（別紙様式２）

氏　　名　：廖 暁鵑

論文題名　：　Maximum Satisfiability Approach to Game Theory and Network Security

（ゲーム理論と通信網の安全性への最大充足可能性アプローチ）

区　　分　：甲

論　文　内　容　の　要　旨

The problem of determining whether a propositional Boolean formula can evaluate to true is called Boolean Satisfiability Problem (SAT). Maximum Satisfiability Problem (MaxSAT), as well as its extensions: partial MaxSAT, weighted MaxSAT, and weighted partial MaxSAT, are optimization versions of the famous SAT problem. To date, there have been a variety of MaxSAT applications such as planning and scheduling. This thesis is concerned with a well-suited way of representing and solving real-world problems with MaxSAT, in terms of multi-agent systems and cryptographic areas.

Generally, a propositional Boolean formula is expressed in Conjunctive Normal Form (CNF), which is a conjunction of clauses that are disjunctions of literals. A literal is either a positive or negative Boolean variable. Weighted partial MaxSAT (WPM) distinguishes clauses between hard and soft, where each soft clause is associated with a positive weight. The WPM problem is to satisfy all hard clauses and maximize the sum of weights of all the satisfied soft clauses. The positive weights in WPM sometimes become impediment to solve problems where positive and negative weights co-exist. To avoid this difficulty, in this thesis, an extended WPM (EWPM) for handling non-zero weights is presented and the relationship between EWPM and WPM solution is examined. The design of EWPM paves the way for a wider range of WPM applications.

One application of EWPM is the coalition structure generation problem (CSG), which tries to partition a set of agents into coalitions so that the total value of all coalitions is maximized. In the CSG problem, values of coalitions can be both positive and negative. This thesis provides two WPM encodings for solving the CSG problem. The first encoding is derived from the existing optimization frameworks and the second one is a brand-new encoding making use of the developed EWPM. Both encodings validate the effectiveness of the WPM solvers in solving the CSG problem.

If all soft clauses in WPM have weight 1, the problem is regarded as partial MaxSAT. The goal of partial MaxSAT is to satisfy all hard clauses and the maximal number of soft clauses. In this thesis, the potential of partial MaxSAT is exploited for reconstructing corrupted key schedule images of advanced encryption standard (AES) extracted from the dynamic random access memory after power is removed. An AES key is a series of 0-1 bits closely related to each other. The relations among key bits are naturally expressed with a

set of Boolean formulas, and rectifying the faults in the corrupted AES key schedule is formulated as a Maximum satisfiability problem which can be solved efficiently by off-the-shelf MaxSAT solvers. Experiments show that the partial MaxSAT encoding can greatly improve the efficiency of AES key recovery from corrupted key bits.

Specifically, this thesis is organized as follows.

Chapter 1 presents the background and motivation of this research, and also summarizes our main works and contributions in this chapter.

Chapter 2 provides an introduction to the preliminaries used in the remainder of the this thesis, including the basic concepts and notions related to SAT and MaxSAT, various techniques used for MaxSAT solving, and encodings that transform from a propositional formula to CNF formula. MaxSAT solving techniques play a crucial role in improving the efficiency of problem solving, and the choice of CNF encoding is as important as that of MaxSAT solving algorithms, since currently, many MaxSAT solvers are designed to solve problems represented typically in CNF formulas.

In Chapter 3, WPM is extended for handling not only positive weights but also negative weights. The original intension of the extension is to describe the real-world problems that are associated with both positive and negative values, and then employ the off-the-shelf WPM solvers to these problems. To this end, this chapter first shows the way of transforming from EWPM to the standard one, and provides a rigorous proof on the relation between EWPM and WPM solutions.

Chapter 4 presents a WPM encoding on solving the CSG problem. The encoding provided in this chapter is directly derived from the previous work by Yokoo et. al. First an overview of the previous work that is the most related to our encodings is provided, which has been shown sound and more efficient than other works. This forms the basis for the WPM encoding discussed subsequently. A procedure to encode the previous work into WPM formulas is provided, including the encoding of the basic CSG problem as well as its extension. Experimental results are used to show the efficiency and scalability of the WPM encoding.

Chapter 5 provides a brand-new WPM encoding for the CSG problem, taking advantage of the EWPM-to-WPM transformation described in Chapter 3. The notion of agent relations is introduced and the encodings of the CSG problem based on agent relations are defined. In the rest of this chapter, the WPM encoding towards solving the CSG problem with positive values and negative values are discussed step by step. Experimental data and comparison results are provided to demonstrate the effectiveness of the proposed encoding.

In Chapter 6, two propositional logical encodings for recovering AES key schedules are provided. There are two different assumptions for key recovery, i.e., perfect assumption and realistic assumption. Perfect assumption assumes all memory bits tend to decay to the ground state after power is removed, while in the realistic assumption, the phenomenon of decaying to the ground state and flipping to the charged state may co-exist. The works for recovering the AES keys under different assumptions are analyzed. Since the realistic assumption is more suitable for the real-world case, this chapter presents two approaches for recovering AES keys under realistic assumption, respectively with SAT and partial MaxSAT solvers. Experimental results and comparisons are provided to demonstrate the effectiveness of the proposed approaches.

Finally, Chapter 7 contains a summary of this thesis and a discussion of some future research directions that may be worth exploring.