Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science 332 (2017) 39–56

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

Generalized Probabilistic Satisfiability [1]

Carlos Caleiro[a] Filipe Casal[b] Andreia Mordido[a]

[a] *SQIG - Instituto de Telecomunicações*
Dep. Mathematics, Instituto Superior Técnico, Universidade de Lisboa, Portugal

[b] *Centro de Matemática, Aplicações Fundamentais e Investigação Operacional (CMAF-CIO)*
Dep. Mathematics, Instituto Superior Técnico, Universidade de Lisboa, Portugal

Abstract

We analyze a generalized probabilistic satisfiability problem (GenPSAT) which consists in deciding the satisfiability of linear inequalities involving probabilities of classical propositional formulas. GenPSAT is proved to be NP-complete and we present a polynomial reduction to Mixed-Integer Programming. Capitalizing on this translation, we implement and test a solver for the GenPSAT problem. As previously observed for many other NP-complete problems, we are able to detect a phase transition behaviour for GenPSAT.

Keywords: Probabilistic Satisfiability, GenPSAT, Mixed-Integer Programming, Phase Transition

1 Introduction

For many years, the satisfiability problem for propositional logic (SAT) has been extensively studied both for theoretical purposes, such as complexity theory, and for practical purposes. In spite of its NP-completeness [9], modern tools for solving SAT are able to cope with very large problems in a very efficient manner, leading to applications in many different areas and industries [2].

Naturally, people started extending this problem to more expressive frameworks: for instance in Satisfiability Modulo Theories [10], instead of working in propositional logic, one can try to decide if a formula is valid in some specific first-order theory. One other direction is to extend propositional logic with probabilities. The probabilistic satisfiability problem (PSAT) was originally formulated by George

[1] Work done under the scope of R&D Unit 50008, financed by the applicable financial framework (FCT/MEC through national funds and when applicable co-funded by FEDER–PT2020) and partially supported by Fundação para a Ciência e a Tecnologia by way of grant UID/MAT/04561/2013 to Centro de Matemática, Aplicações Fundamentais e Investigação Operacional of Universidade de Lisboa (CMAF-CIO). AM was supported by FCT under the grant SFRH/BD/77648/2011 and by the Calouste Gulbenkian Foundation under *Programa de Estímulo à Investigação* 2011. FC acknowledges the support from the DP-PMI and FCT (Portugal) through scholarship SRFH/BD/52243/2013. CC acknowledges the support of EU FP7 Marie Curie PIRSES-GA-2012-318986 project GeTFun: Generalizing Truth-Functionality.

http://dx.doi.org/10.1016/j.entcs.2017.04.004
1571-0661/

Boole [3] and later by Nilsson [18]. This problem consists in deciding the satisfiability of a set of assignments of probabilities to propositional formulas. There has been a great effort on the analysis of the probabilistic satisfiability problem and on the development of efficient tools for the automated treatment of this problem [11,14,6,1,12].

In this paper we study a Generalized Probabilistic Satisfiability problem (GenPSAT) extending the scope of PSAT by allowing linear combinations of probabilistic assignments of values to propositional formulas, and has applications in the analysis of the security of cryptographic protocols and on estimating the probability of existence of attacks [17]. Intuitively, GenPSAT consists in deciding the existence of a probability distribution satisfying a set of classical propositional formulas with probability 1, and a set of linear inequalities involving probabilities of propositional formulas. The GenPSAT problem was previously identified in the context of the satisfiability of the probabilistic logic in [13], where it was also shown to be NP-complete. Here, we explore the computational behaviour of this problem and present a polynomial reduction from GenPSAT to Mixed-Integer Programming, following the lines of [6,1].

Mixed-Integer Programming (MIP) [19] is a framework to find an optimal solution for a linear objective function subject to a set of linear constraints over real and integer variables. We will exploit the close relation between SAT and MIP [4] in order to reduce GenPSAT problems to suitable MIP problems.

As observed in many NP-complete problems [7], GenPSAT also presents a phase transition behaviour. By solving batches of parametrized random GenPSAT problems, we observe the existence of a threshold splitting a phase where almost every GenPSAT problem is satisfiable, and a phase where almost every GenPSAT problem is not satisfiable. During such transition, the problems become much harder to solve [7].

As the main contribution of this work, we develop the theoretical framework that allows the translation between GenPSAT and MIP problems, which then allows the implementation of a provably correct solver for GenPSAT. This translation is able to encode strict inequalities and disequalities into the MIP context. With the GenPSAT solver in hands, we are able to detect and study the phase transition behaviour.

The paper is outlined as follows: in Section 2 we briefly recall the PSAT problem; in Section 3 we carefully define the GenPSAT problem and establish some results on its complexity; Section 4 is dedicated to finding a polynomial reduction from GenPSAT to MIP and a prototype tool is provided for an automated analysis of the problem; in Section 5 we analyze the presence of phase transition; finally, in Section 6, we assess our contributions and discuss future work.