

Beyond Q-Resolution and Prenex Form: A Proof System for Quantified Constraint Satisfaction

Hubie Chen

Universidad del País Vasco, E-20018 San Sebastián, Spain
and IKERBASQUE, Basque Foundation for Science, E-48011 Bilbao Spain

Abstract. We consider the quantified constraint satisfaction problem (QCSP) which is to decide, given a structure and a first-order sentence (not assumed here to be in prenex form) built from conjunction and quantification, whether or not the sentence is true on the structure. We present a proof system for certifying the falsity of QCSP instances and develop its basic theory; for instance, we provide an algorithmic interpretation of its behavior. Our proof system places the established Q-resolution proof system in a broader context, and also allows us to derive QCSP tractability results.

Note: a full paper is available at <http://arxiv.org/abs/1403.0222>.

1 Introduction

Background. The study of *propositional proof systems* for certifying the unsatisfiability of quantifier-free propositional formulas is supported by multiple motivations [3, 11]. First, the desire to have an efficiently verifiable certificate of a formula’s unsatisfiability is a natural and basic one, and indeed the field of propositional proof complexity studies, for various proof systems, whether and when succinct proofs exist for unsatisfiable formulas. Next, theorem provers are typically based on such proof systems, and so insight into the behavior of proof systems can yield insight into the behavior of theorem provers. Also, algorithms that perform search to determine the satisfiability of formulas can typically be shown to implicitly generate proofs in a proof system, and thus lower bounds on proof size translate to lower bounds on the running time of such algorithms. Finally, algorithms that check for unsatisfiability proofs of various restricted forms have been shown to yield tractable cases of the propositional satisfiability problem and related problems (see for example [1, 2]).

In recent years, increasing attention has been directed towards the study of *quantified proof systems* that certify the falsity of quantified propositional formulas, which study is also pursued with the motivations similar to those outlined for the quantifier-free case. Indeed, the development of so-called *QBF solvers*, which determine the truth of quantified propositional formulas, has become an active research theme, and the study of quantified proof systems is pursued as a way to understand their behavior, as well as to explore the space of potential certificate formats for verifying their correctness on particular input instances.

Q-resolution [4] is a quantified proof system that can be viewed as a quantified analog of *resolution*, one of the best-known and most customarily considered propositional proof systems. In the context of quantified propositional logic, Q-resolution is a heavily studied and basic proof system on which others are built and to which others are routinely compared, as well as a point of departure for the discussion of suitable certificate formats (see [8, 12, 9] for examples).

However, the Q-resolution proof system has intrinsic shortcomings. First, it is only applicable to quantified propositional sentences that are in prenex form, that is, where all quantifiers appear in front. While it is certainly true that an arbitrary given quantified propositional formula may be efficiently prenexed, the process of prenexing is not canonical: intuitively, it involves choosing a total order of variables consistent with the partial order given by the input formula. As argued by Egly, Seidl, and Woltran [7], this may disrupt the original formula structure, “artificially extend” the scopes of quantifiers, and generate dependencies among variables that were not originally present, unnecessarily increasing the expense of solving; we refer the reader

to their article for a contemporary discussion of this issue. A second shortcoming of Q-resolution is that it is only defined in the propositional setting, despite that some scenarios may be more naturally and cleanly modelled by allowing variables to be quantified over domains of size greater than two.

Contributions. In this article, we introduce a proof system that directly overcomes both of the identified shortcomings of Q-resolution.

We here define the *quantified constraint satisfaction problem (QCSP)* to be the problem of deciding, given a relational structure $\mathbf{B}$ and a first-order sentence ϕ (not necessarily in prenex form) built from the conjunction connective ($\wedge$) and the two quantifiers ($\forall, \exists$), whether or not the sentence is true on the structure. To permit different variables to have different domains, we formalize the QCSP using multi-sorted first-order logic.

Our proof system allows for the certification of falsity of QCSP instances. While Q-resolution provides rules for deriving clauses from a given quantified propositional formula, our proof system provides rules for deriving what we call *constraints* at various formula locations of a given QCSP instance; here, a constraint (V, F) is a set V of variables paired with a set F of assignments, each defined on V . A formula location i paired with a constraint is called a *judgement*; a proof in our system is a sequence of judgements where each is derived from the previous ones via the rules.

Crucially, we formulate and prove a key lemma that shows (essentially) that if a judgement (i, V, F) is derivable from a QCSP instance $(\phi, \mathbf{B})$, then there exists a formula $\psi(V)$ that “defines” the constraint (V, F) over $\mathbf{B}$, such that $\psi(V)$ can be conjoined to the input sentence ϕ at location i while preserving logical equivalence. This key lemma is then swiftly deployed to establish soundness and completeness of our proof system. We view the formulation of our proof system and of this key lemma as conceptual contributions. They offer a broader, deeper, and more general perspective on Q-resolution and what it means for a clause to be derivable by Q-resolution: we show (in a sense made precise) that each clause derivable by Q-resolution is derivable by our proof system. This yields a clear and transparent proof of the soundness of Q-resolution which, interestingly, is carried out in the setting of first-order logic, despite the result concerning propositional logic.

In order to relate our proof system to Q-resolution, we give a proof system for certain quantified propositional formulas and prove that this second proof system is a faithful propositional interpretation of our QCSP proof system. We also provide an algorithmic interpretation of this second proof system. In particular, we give a nondeterministic search algorithm such that traces of execution that result in certifying falsity correspond to refutations in the proof system. As a consequence, the proof system yields a basis for establishing running-time lower bounds for any deterministic algorithm which instantiates the non-deterministic choices of our search algorithm.

References

1. A. Atserias, P. Kolaitis, and M. Vardi. Constraint propagation as a proof system. In *Proceedings of CP*, 2004.
2. L. Barto and M. Kozik. Constraint satisfaction problems of bounded width. In *Proceedings of FOCS’09*, 2009.
3. P. Beame and T. Pitassi. Propositional proof complexity: Past, present and future. *Bulletin of the EATCS*, 65:66–89, 1998.
4. H. K. Büning, M. Karpinski, and A. Flögel. Resolution for quantified Boolean formulas. *Information and Computation*, 117(1):12–18, 1995.
5. H. Chen and V. Dalmau. Decomposing quantified conjunctive (or disjunctive) formulas. In *LICS*, 2012.
6. H. Chen, V. Dalmau, and B. Grüßen. Arc consistency and friends. *J. Log. Comput.*, 23(1):87–108, 2013.
7. U. Egly, M. Seidl, and S. Woltran. A solver for qbfs in negation normal form. *Constraints*, 14(1):38–79, 2009.
8. E. Giunchiglia, M. Narizzano, and A. Tacchella. Clause/term resolution and learning in the evaluation of quantified boolean formulas. *J. Artif. Intell. Res. (JAIR)*, 26:371–416, 2006.
9. M. Janota and J. Marques-Silva. On propositional qbf expansions and q-resolution. In *SAT*, pages 67–82, 2013.
10. P. G. Kolaitis and M. Y. Vardi. A game-theoretic approach to constraint satisfaction. In *Proceedings of the 17th National Conference on AI*, pages 175–181, 2000.
11. N. Segerlind. The complexity of propositional proofs. *Bull. Symbolic Logic*, 13:417–626, 2007.
12. F. Slivovsky and S. Szeider. Computing resolution-path dependencies in linear time. In *SAT*, pages 58–71, 2012.