Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science 323 (2016) 93–108

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

Proof Certificates for Equality Reasoning

Zakaria Chihani and Dale Miller

Inria & LIX/École polytechnique, Palaiseau, France

Abstract

The kinds of inference rules and decision procedures that one writes for proofs involving equality and rewriting are rather different from proofs that one might write in first-order logic using, say, sequent calculus or natural deduction. For example, equational logic proofs are often chains of replacements or applications of oriented rewriting and normal forms. In contrast, proofs involving logical connectives are trees of introduction and elimination rules. We shall illustrate here how it is possible to check various equality-based proof systems with a programmable proof checker (the *kernel* checker) for first-order logic. Our proof checker's design is based on the implementation of *focused proof search* and on making calls to (user-supplied) *clerks and experts* predicates that are tied to the two phases found in focused proofs. It is the specification of these clerks and experts that provide a formal definition of the structure of proof evidence. As we shall show, such formal definitions work just as well in the equational setting as in the logic setting where this scheme for proof checking was originally developed. Additionally, executing such a formal definition on top of a kernel provides an actual proof checker that can also do a degree of proof reconstruction. We shall illustrate the flexibility of this approach by showing how to formally define (and check) rewriting proofs of a variety of designs.

Keywords: proof certificates, equational proofs, proof checking, rewriting proofs

1 Introduction

Equality is central not only to computer science but also to other hard sciences such as mathematics and physics. It is therefore understandable that handling equality in theorem proving has also been at the core of an important research effort in the field of formal logics. Term Rewriting is a generic label that designates a plethora of methods for replacing subterms with other terms that are considered equal and is an effective tool for reasoning with equality. A rewriting rule is a restriction of an equality in that it is used as a directed replacement rule. A set of such rules forms a Term Rewriting System (or TRS). Much research in the area of TRS involves proving properties *about* TRSs—such as confluence, termination, completion, and the decidability of certain set of equalities. We shall focus here, instead, on a simpler and more "infrastructure" topic: certifying reasoning that takes place *within* a TRS, using various forms of proof, and with checking proofs that merge equality reasoning with logical deduction, including, for example, deduction modulo [8] and paramodulation [18].

http://dx.doi.org/10.1016/j.entcs.2016.06.007

1.1 Equality and equality proofs

The question "what is equality" is often answered in different ways. Occasionally, equality is taken as a primitive logical symbol [2,11,19]. Sometimes it is defined using Leibniz's (higher-order) rule: two terms are equal if they satisfy exactly the same predicates. More commonly, equality is taken to be a non-logical binary predicate symbol that is axiomatized with rules for reflexivity, symmetry, transitivity, and congruence (for predicates and functions). We choose this latter approach to equality in this paper.

There are a myriad of techniques and ideas that are deployed to deal with equality in theorem proving: these include paramodulation, superposition, narrowing, ρ-calculus and E-unification, as well as practical methods to implement them, such as generating a converging term rewriting system as a decision procedure, saturation methods, redundancy elimination, and heuristics (see [13] for an overview of these topics). Given that there are so many ways to discover and represent equality proofs, a scheme for checking such proofs needs to be flexible.

To be more specific, our first concern will be attempting to check that a formal proof Ξ justifies that the equality $t = s$ follows from some equational (possibly oriented) assumptions $\mathcal{E}$. We give informal descriptions of a few possible ways that Ξ might be structured.

(i) Ξ might provide a decomposition of $t = C[u]$ into a context $C[\cdot]$ and subterm u and an instance of a equality in $\mathcal{E}$, say, $u = v$ so that $s = C[v]$.

(ii) Ξ might contain a number, say n, and the claim that there is some chain of length n or less of equational rewritings of t to s.

(iii) Ξ might contain a partitioning of $\mathcal{E}$ (into $\mathcal{E}_1$ and $\mathcal{E}_2$) and a proof Ξ' such that normalizing both t and s with respect to (an oriented variant of) $\mathcal{E}_1$ yields normal form terms that are equal modulo $\mathcal{E}_2$, which is justified by Ξ'.

It stands to reason that once the proof, say Ξ above, is found it should survive the test of time. At least two conditions seem necessary to support such eternal existence. Firstly, the proof should constitute a *document* that can be *communicated*. Indeed, if a prover claims to have found a proof that it does not actually deliver as a document because, for example, it is too large or too expensive to produce, can we trust that prover? To what extent can one have faith in the claim "I have a truly marvelous demonstration of this proposition which this margin is too narrow to contain."? Secondly, the format in which the proof is written must allow *independent checking*. Indeed, if the description of a proof can only be "understood" by the prover that produces it, can that constitute an acceptable means of communication and of instilling trust?

1.2 Foundational proof certificates

In this paper, we employ the *foundational proof certificate* (FPC) framework [7,15] for defining the semantics of proof evidence in intuitionistic and classical first-order logics. The generality of the FPC framework makes it possible, as we hope to show