NP-Completeness of Reflected Fragments of Justification Logics

Sam Buss (UCSD) and Roman Kuznets (Bern)
sbuss@math.ucsd.edu and kuzents@iam.unibe.ch

Logical Foundations of Computer Science, 2009

Logic of Proofs (LP)

The Logic of Proofs, LP, is a Justification Logic [Artemov, 1995] and provides an explicit analogue of modal logic, where necessitation ($\Box$) is replaced by explicit proof terms.

Definition (Propositional Justification Logic)

Formulas. $F \ := \ p \mid \bot \mid (F \to F) \mid t\!:\!F$.
Terms. $t \ := \ x \mid c \mid (t \cdot t) \mid (t + t) \mid\, !t$.

$t\!:\!F$ is intended to mean that "t is a justification or proof of F".

Axioms and rules of LP

A1. Finite set of axiom schemes for propositional logic

A2. $s:(F \to G) \to t:F \to (s \cdot t):G$ *Application*

A3. $s:F \to (s+t):F, \qquad t:F \to (s+t):F$ *Monotonicity*

A4. $t:F \to F$ *Factivity*

A5. $t:F \to\, !t:t:F$ *Positive Introspection*

R4. $\dfrac{}{c:A}$ where A is an axiom and c is a justification constant

R5. Modus ponens

Forgetful projection

The *forgetful projection* $F \mapsto F^\circ$ on formulas respects Boolean connectives and replaces $t\!:\!G$ with $\Box G$.

Theorem (Realization Theorem, Artemov, 1995)

$\mathrm{LP}^\circ = \mathrm{S4}$.

When transforming S4-proofs to LP-proofs, the justfication terms may be exponentially large in the size of the formula, but can be polynomially bounded by the size of a cut-free S4-proof. [Brezhnev-Kuznets, 2008.]

Reflected Logic of Proofs, rLP

Definition (Krupski, 2006)

$\mathsf{rLP} = \{t{:}F \mid \mathsf{LP} \vDash t{:}F\}$.

Theorem

LP $\vdash F$ *if and only if* rLP $\vdash t{:}F$ *for some* t*.*

Definition (Constant Specification, $\mathcal{CS}$)

It is convenient to restrict the Internalization rule to allow exactly one constant symbol to justify each particular schematic axiom A1-A5. E.g., $c_\wedge$ justifies any instance of $A \to B \to A \wedge B$ and similarly for the other usual axiom schemes for propositional logic.

The notations $\mathsf{LP}_{\mathcal{CS}}$ and $\mathsf{rLP}_{\mathcal{CS}}$ are used for the Logic of Proofs under the constant specification $\mathcal{CS}$.

Theorem (Realization Theorem, again)

$\mathsf{LP}^{\circ}_{\mathcal{CS}} = \mathsf{S4}$.

Theorem (Ladner, 1977)

The derivability problem for S4 is PSPACE complete.

Theorem (Kuznets, 2000; Milnikel, 2007)

The derivability problem for $\mathsf{LP}_{\mathcal{CS}}$ *is* Π^p_2*-complete.*

Theorem (Kuznets, 2006)

The derivability problem for $\mathrm{rLP}_{\mathcal{CS}}$ *is in NP.*

Theorem (this talk)

The derivability problem for $\mathrm{rLP}_{\mathcal{CS}}$ *is NP-hard, and hence NP-complete.*

Since the $\mathrm{rLP}_{\mathcal{CS}}$ proofs are polynomial size, we obtain

Corollary

The k-provability problem *of deciding if* rLP *has a proof of* $t\!:\!F$ *of length* $\leq k$ *symbols is* NP*-complete.*

The following provides a normalization theorem for $\mathrm{rLP}_{\mathcal{CS}}$.

Theorem (Krupski, 2006)

The reflected system $\mathrm{rLP}_{\mathcal{CS}}$ *is axiomatized by the *-calculus:*

*$\mathcal{CS}$ *Axioms* $c\!:\!A$ *for any* $c\!:\!A \in \mathcal{CS}$.

*A2 $\dfrac{s\!:\!F \to G \quad t\!:\!F}{s \cdot t\!:\!G}$

*A3 $\dfrac{s\!:\!F}{s + t\!:\!F} \qquad \dfrac{t\!:\!F}{s + t\!:\!F}$

*A5 $\dfrac{t\!:\!F}{!t\!:\!t\!:\!f}$

This allows a very direct proof search algorithm, where the only non-deterministic component is choosing how to apply the Sum $(+)$ rule, and choosing a formula F when applying the Application $(\cdot)$ rule.

We use a reduction to the *Binary Vertex Cover* problem, which is a Vertex Cover problem in which the number of nodes, the number of edges, and the sought-for vertex cover are all powers of 2.

Lemma

The Binary Vertex Cover is NP-complete.

Given an instance $G = (V, E)$ of Binary Vertex Cover, we use

- Variables p_i, one for each vertex x_i of the graph.
- $F_e := (p_a \vee p_b)$ for each edge $e = \{x_a, x_b\}$.
- $F_G := F_{e_1} \wedge F_{e_1} \wedge \cdots \wedge F_{e_{2^m}}$.
- $F_V := p_1 \wedge p_2 \wedge \cdots \wedge p_{2^k}$.
- $F_C := p_{i_1} \wedge p_{i_2} \wedge \cdots \wedge p_{i_{2^\ell}}$,, for $\{p_{i_j}\}_j$ a potential vertex cover.

The conjunctions are all balanced.

Lemma

The following are valid:

- $F_V \to F_G$.
- $F_V \to F_C$.
- $F_C \to F_G$, *if and only if* C *is a vertex cover for* G.

The proof of $F_V \to F_G$ will proceed by choosing a vertex cover C and proving proving

- $F_V \to F_C$
- $F_C \to F_G$, (works if C is vertex cover),

and then combining the two proofs with a cut.

Lemma

There is a proof term t such that $t{:}G$ holds for exactly the formulas $t{:}(A \wedge B) \rightarrow A$ and $t{:}(A \wedge B) \rightarrow B$, for A and B any formulas.

Proof: Let $c_{\wedge_1}{:}A \wedge B \rightarrow A$ and $c_{\wedge_2}{:}A \wedge B \rightarrow B$ be from the constant specification $\mathcal{CS}$. Set $t := c_{\wedge 1} + c_{\wedge_2}$.

Lemma

There is a proof term $\mathrm{syl}(s,t)$ which justifies exactly the formulas $A \rightarrow C$ such that $t{:}A \rightarrow B$ and $s{:}B \rightarrow C$.

Proof: Let $c_1{:}A \rightarrow B \rightarrow A$ and
$c_2{:}(A \rightarrow B \rightarrow C) \rightarrow (A \rightarrow B) \rightarrow (A \rightarrow C)$.
Set $\mathrm{syl}(s,t) := (c_2 \cdot (c_1 \cdot s)) \cdot t$.

Lemma

There is a term t such that $t : F_V \to p_i$ for all i, and t justifies only (substitution instances of) these formulas.

Proof: Iterate the construction of first lemma k times combining terms with the syl term..

Lemma

There is a term $s_{k,\ell}$ such that t justifies exactly the formulas $F_V \to F_C$ where F_C and F_V are balanced conjunctions of depth ℓ and depth k.

Proof: Use the previous lemma 2^ℓ times, and combine these with a term that justifies precisely the formulas
$(A \to B) \to (A \to C) \to (A \to B \wedge C)$.

Lemma

There is a term t such that, if C is a vertex cover and if e is an edge, then $t : F_C \to F_e$.

The term t depends only the depth ℓ of F_C.

Lemma

There is a term $t_{\ell,m}$ such that, if C a vertex cover, then $t : F_C \to F_G$.

Lemma

We have $\mathrm{syl}(t_{\ell,m}, s_{k,\ell}) : F_V \to F_G$ if and only if G has a vertex cover C of size $\leq k$.

This completes the proof of NP-hardness of $\mathrm{rLP}_{\mathcal{CS}}$.

Other justification logics, J, JD, JT, JD4 correspond to modal logics K, D, T, D4 [Brezhnev, 2000]. Hybrid logics combine justifications and epistemic modalities for multiple agents.

Similar constructions apply to these theories.

- The reflected fragments admit a *-calculus. [Kuznets, 2008]
- The reflected fragments are in NP. [K'08].
- The reflected fragments are NP-complete.

the end