The proof equivalence problem for multiplicative linear logic is PSPACE-complete v0.3

Willem Heijltjes and Robin Houston · July 25, 2013

Abstract

MLL proof equivalence is the problem of deciding whether two proofs are related by a series of rule permutations. Previous work has shown the problem to be equivalent to a rewiring problem on proof nets, which are not canonical for full MLL due to the presence of the two units. Drawing from recent work on reconfiguration problems, in this paper it is shown that MLL proof equivalence is PSPACE-complete, using a reduction from Nondeterministic Constraint Logic.

$$\frac{\Gamma}{\Gamma, \bot}\,\bot \qquad \frac{}{1}\,1 \qquad \frac{\Gamma, A, B}{\Gamma, A \parr B}\,\parr \qquad \frac{\Gamma, A \qquad \Delta, B}{\Gamma, \Delta, A \otimes B}\,\otimes$$

Figure 1: Inference rules for unit-only MLL

$$\frac{\dfrac{\Gamma}{\Gamma, \bot^a}\,\bot}{\Gamma, \bot^a, \bot^b}\,\bot \sim \frac{\dfrac{\Gamma}{\Gamma, \bot^b}\,\bot}{\Gamma, \bot^a, \bot^b}\,\bot \qquad \frac{\dfrac{\Gamma, A, B}{\Gamma, A \parr B}\,\parr}{\Gamma, A \parr B, \bot}\,\bot \sim \frac{\dfrac{\Gamma, A, B}{\Gamma, A, B, \bot}\,\bot}{\Gamma, A \parr B, \bot}\,\parr$$

$$\frac{\dfrac{\Gamma, A \qquad \Delta, B}{\Gamma, \Delta, A \otimes B}\,\otimes}{\Gamma, \Delta, A \otimes B, \bot}\,\bot \sim \frac{\dfrac{\Gamma, A}{\Gamma, A, \bot}\,\bot \qquad \Delta, B}{\Gamma, \Delta, A \otimes B, \bot}\,\otimes \sim \frac{\Gamma, A \qquad \dfrac{\Delta, B}{\Delta, B, \bot}\,\bot}{\Gamma, \Delta, A \otimes B, \bot}\,\otimes$$

$$\frac{\dfrac{\Gamma, A, B, C, D}{\Gamma, A \parr B, C, D}\,\parr}{\Gamma, A \parr B, C \parr D}\,\parr \sim \frac{\dfrac{\Gamma, A, B, C, D}{\Gamma, A, B, C \parr D}\,\parr}{\Gamma, A \parr B, C \parr D}\,\parr$$

$$\frac{\dfrac{\Gamma, A \qquad \Delta, B, C, D}{\Gamma, \Delta, A \otimes B, C, D}\,\otimes}{\Gamma, \Delta, A \otimes B, C \parr D}\,\parr \sim \frac{\Gamma, A \qquad \dfrac{\Delta, B, C, D}{\Delta, B, C \parr D}\,\parr}{\Gamma, \Delta, A \otimes B, C \parr D}\,\otimes$$

$$\frac{\Gamma, A \qquad \dfrac{\Delta, B, C \qquad \Lambda, D}{\Delta, \Lambda, B, C \otimes D}\,\otimes}{\Gamma, \Delta, \Lambda, A \otimes B, C \otimes D}\,\otimes \sim \frac{\dfrac{\Gamma, A \qquad \Delta, B, C}{\Gamma, \Delta, A \otimes B, C}\,\otimes \qquad \Lambda, D}{\Gamma, \Delta, \Lambda, A \otimes B, C \otimes D}\,\otimes$$

Figure 2: Permutations

1 MLL

The formulae of unit-only multiplicative linear logic are given by the following grammar.

$$A, B, C := \bot \mid 1 \mid A \parr B \mid A \otimes B$$

The connectives $\otimes$ and $\parr$ will be considered up to associativity, and *duality* $A^\star$ is via DeMorgan. A *sequent* Γ, Δ will be a multiset of formulae. Within a sequent, connectives and units will be *named* with distinct elements from an arbitrary set of names N, e.g. $1^a \parr^b 1^c, \bot^d \otimes^e \bot^f$. This allows to 1) avoid using the notion of *occurrence*, and instead refer to subformulae by the name of their root connective, as e.g. A^b, 2) distinguish the two proofs of the above sequent while using standard multiset sequents, and 3) easily extract proof nets, as graphs using the names of connectives as vertices. Names will mostly be left implicit.

Proofs are constructed from the inference rules in Figure 1. The names of connectives are preserved through inferences. Only cut-free proofs are considered, and no cut-rule is added. *Permutations* of inference rules are displayed in Figure 2; the symmetric variants of the last two permutations, *par-tensor* and *tensor-tensor*, have been omitted.

Definition 1. *Equivalence* of proofs in (cut-free, unit-only) multiplicative linear logic ($\sim$) is the congruence generated by the permutations given in Figure 2. *MLL proof equivalence* is the problem of deciding whether two given proofs are equivalent.

The motivation to consider proofs up to equivalence is three-fold. Firstly, there is the strong intuition that the order of permutable inferences does not contribute to the essential content of the proof. Secondly, a technical motivation is that cut-elimination in MLL incorporates permutation steps, and composition via cut-elimination is only associative up to permutations. Thirdly, equivalent proofs are identified in natural models of multiplicative linear logic such as coherence spaces, and in the categorical semantics of MLL, $\star$-autonomous categories.

In one of several possible definitions, a *$\star$-autonomous category* (Barr, 1979) is a symmetric monoidal category $(\mathcal{C}, \otimes, 1)$ with:

- a *duality*, a contravariant functor $-^\star$ such that $A \cong A^{\star\star}$, and

- *closure*, an adjunction $- \otimes B \dashv (B \otimes -^{\star})^{\star}$ for any object B,

satisfying natural coherence conditions. The category $\textsc{mll}(\varnothing)$ of unit-only $\textsc{mll}$-formulae and equivalence classes of proofs is a $\star$-autonomous category. The formulation used induces various forms of *strictness*, instances where isomorphisms of the definition are identities: DeMorgan duality means $A = A^{\star\star}$, one-sided sequents mean the closure adjunction is an equivalence of categories, and the associativities are identities by decree. Modulo strictness, $\textsc{mll}(\varnothing)$ is the *free* $\star$-autonomous category over the empty category $\varnothing$. This means that *any* $\star$-autonomous category is a model of the logic, and that $\textsc{mll}$ proof equivalence is the *word problem* for $\star$-autonomous categories, the problem of deciding when two representations of morphisms denote the same morphism.

1.1 Proof nets

A partial solution to the $\textsc{mll}$ proof equivalence problem is provided by proof nets.

Definition 2. For a sequent Γ,

- a *linking* ℓ is a function from the names of $\bot$-subformulae to the names of 1-subformulae,
- a *switching graph* for ℓ is an undirected graph over the names of Γ, with for every subformula $A^a \otimes^c B^b$ the edges $a - c$ and $b - c$, for every subformula $A^a \parr^c B^b$ either the edge $a - c$ or the edge $b - c$, and for every subformula $\bot^a$ the edge $a - \ell(a)$,
- a *proof net* ℓ or (Γ, ℓ) is a linking ℓ such that every switching graph is acyclic and connected.

An edge $a - \ell(a)$ in a proof net or switching graph is a *link* or *jump*.

Definition 3. A *permutation* between proof nets is the redirection of exactly one link. *Equivalence* $(\sim)$ of proof nets over a sequent Γ is the congruence generated by permutations.

There is no canonical interpretation of a proof as a proof net, since the introduction rule for $\bot$ in proofs joins a $\bot$ to a sequent, rather than a formula.

Definition 4. The relation $(\mapsto)$ interprets a proof by a linking ℓ as follows: for each $\bot^a$, if Γ is the context of the inference introducing $\bot^a$, as illustrated below, then $\ell(a)$ is the name of some 1 in Γ.

$$\frac{\Gamma}{\Gamma, \bot^a}\,\bot$$

Proposition 5 (Danos and Regnier, 1989). *For a proof* Π *with conclusion* Γ*, if* $\Pi \mapsto \ell$ *then* ℓ *is a proof net for* Γ*. For a net* ℓ *for* Γ*, there is a proof* Π *of* Γ *such that* $\Pi \mapsto \ell$ *(*sequentialisation*).*

Proof nets are canonical representations of proofs in the absence of units: they factor out the permutations among tensor- and par-inferences, which are the last three permutations in Figure 2. Equivalence of proof nets is generated by the remaining equations, the permutations on $\bot$-introduction.

Proposition 6 (Hughes (2012)). *For proofs* Π*,* Π' *and proof nets* ℓ*,* ℓ' *such that* $\Pi \mapsto \ell$ *and* $\Pi' \mapsto \ell'$*,* $\Pi \sim \Pi'$ *if and only if* $\ell \sim \ell'$*.*

$\textsc{mll}$ proof equivalence is the problem of deciding equivalence of proof nets.

References

Michael Barr. **-Autonomous categories*, volume 752 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, Heidelberg, New York, 1979.

Vincent Danos and Laurent Regnier. The structure of multiplicatives. *Archive for Mathematical Logic*, 28:181–203, 1989.

Dominic J.D. Hughes. Simple multiplicative proof nets with units. *Annals of Pure and Applied Logic*, 2012. arXiv:math.LO/0507003.