Linearizing Intuitionistic Implication

(Appeared in ACM Symposium on Logic in Computer Science 1991)

Patrick Lincoln* Andre Scedrov† Natarajan Shankar‡

June 19, 1991

Abstract

*An embedding of the implicational propositional intuitionistic logic (*IIL*) into the nonmodal fragment of intuitionistic linear logic (*IMALL*) is given. The embedding preserves cut-free proofs in a proof system that is a variant of* IIL*. The embedding is efficient and provides an alternative proof of the* PSPACE*-hardness of* IMALL*. It exploits several proof-theoretic properties of intuitionistic implication that analyze the use of resources in* IIL *proofs.*

1 Overview

Linear logic, invented by Girard [Gir87], is a refinement of classical and intuitionistic logic that provides an intrinsic and natural accounting of resources. In Girard's words [Gir87], "linear logic is a logic behind logic." He provides a conservative translation from intuitionistic logic into linear logic that is compositional on subformulas and subproofs. In Girard's translation, intuitionistic implication $A \Rightarrow B$ becomes $!A \multimap B$, where $!$ is a modality indicating unlimited availability of a resource, and $\multimap$ is *linear implication*. In the propositions-as-type interpretation, linear implication is seen as the type of functions that use their argument exactly once. Girard's embedding in fact covers the full spectrum of the propositions-as-types paradigm: the level of formulas, the level of proofs, and the level of proof reduction (cut-elimination steps). Furthermore, this embedding extends naturally to first-order and second-order logic [Gir87].

The possibility of a dramatic improvement over Girard's embedding is raised by a recent result in [LMSS90], establishing the PSPACE-completeness of the so-called multiplicative additive fragment MALL, *i.e.,* propositional linear logic without the modality $!$ or its dual $?$. Statman [Sta79] has shown that propositional intuitionistic logic, indeed, even its purely implicational fragment, is PSPACE-complete. Hence a natural question arises whether (beyond an immediate Turing reduction) there exists another "logical" embedding of intuitionistic logic into linear logic, that does not rely on the modalities.

Let us be realistic. One cannot hope to have such an embedding which would be too "logical", because on the one hand, first-order multiplicative additive linear logic is PSPACE-complete (this follows from the results in [LMSS90] by using methods similar to [KW84]). On the other hand, first-order intuitionistic logic is undecidable (this is an immediate corollary of the negative interpretation of classical logic in intuitionistic logic and the undecidability of classical first-order logic, both of which may be found, for example, in [Kle52]). Therefore it is impossible to have a desired embedding for first-order quantifiers.

Another, more subtle, obstruction to obtaining a very "logical" embedding is the discrepancy in complexity on the level of cut-elimination (normalization). Already for the purely implicational fragment of propositional intuitionistic logic, cut-elimination is hyperexponential (the equivalent fact about normalization in the simple typed lambda calculus is usually one of the first exercises in a graduate course on the subject). In contrast, cut-elimination for MALL is known to be much lower, at most exponential. In fact, this is true not just in the propositional case, but also for first-order and for second-order MALL. The required

*Lincoln@CS.Stanford.EDU Department of Computer Science, Stanford University, Stanford, CA 94305, and the Computer Science Laboratory, SRI International, Menlo Park, CA 94025. Supported by AT&T Bell Laboratories Doctoral Scholarship, and SRI internal funding.

†Andre@CIS.Upenn.EDU Department of Mathematics, University of Pennsylvania, Philadelphia, PA 19104-6395. Partially supported by NSF Grant CCR-87-05596, by ONR Grant NOOO14-88-K-0635 and by the 1987 Young Faculty Award from the Natural Sciences Association of the University of Pennsylvania. Work begun while on sabbatical leave at the Computer Science Department and Center for the Study of Language and Information, Stanford University.

‡Shankar@CSL.SRI.COM Computer Science Laboratory, SRI International, Menlo Park, CA 94025. Supported by SRI internal funding.

bounds may be extracted from the Small Normalization Theorem in [Gir87] and are also explicitly computed in [LS90].

These results still leave open the possibility of a syntactic translation of propositional intuitionistic logic into MALL so that such a translation does preserve cut-free proofs of a certain normal form. In this paper we construct such a translation. Our translation is an instance of what Girard terms an "asymmetrical interpretation," that is, positive occurrences of formulas are translated differently from negative occurrences [GLT89]. It can therefore only be viewed as a translation on cut-free proofs, unlike Girard's symmetric translation of intuitionistic logic into linear logic.

We only consider propositional systems of intuitionistic and linear logic. We use the following notations that are common to both the intuitionistic and linear formalisms:

l_i, p_i, q_i, r_i	Propositional literals
A, B, C	Arbitrary formulas
Σ, Γ	Arbitrary multisets of formulas
$\Gamma \vdash A$	Sequent with *antecedent* Γ and *consequent* A

We entirely omit the linear negation operation of MALL. Note that a sequent is represented in terms of two multisets, not sets, of formulas. When we speak of a formula in a sequent, we are really referring to an occurrence of the formula. A *reduction* is the process of applying a rule to a sequent matching the conclusion of the rule in order to generate the corresponding premises. The *principal formula* of the rule is then said to be *reduced* by the reduction. The occurrence of an instance of a rule in a proof is said to be an *inference*. The proper subformulas of a principal formula of a rule that appear in the premises of the rule are called the *side formulas*.

The main result of this paper is an efficient embedding of the implicational fragment of propositional intuitionistic logic (IIL) in the intuitionistic fragment of multiplicative-additive linear logic (IMALL). We provide a transformation of an IIL sequent σ to an IMALL sequent ρ so that IMALL proves ρ exactly when IIL proves σ. The sequents σ and ρ are then said to be *equiprovable*. The system IIL is given by a fairly standard sequent formulation of the intuitionistic implicational logic shown in Figure 4. These rules are similar to those of Kleene's G3. The target system, IMALL, is shown in Figure 9. Note that the rules for negation, $\mathcal{P}$, and the constant 0 are absent. Since the presentation is in terms of two sided sequents, cut-elimination for IMALL holds despite these omissions. Cut-elimination is of course a crucial tool in many of our proofs.

The main distinction between IIL and IMALL is in their treatment of the structural rules. IIL has an explicit rule of contraction and the rule of weakening is implicitly built into the **I** rule. Furthermore, the principal formula of an $\mathbf{L}\supset$ rule is *copied* into the premise sequents of each IIL rule. IMALL, on the other hand, has neither contraction nor weakening, and expressly forbids the copying of the principal formula of any rule into a premise. What IMALL does allow is the sharing of the non-principal formulas between the two premises of an additive inference rule. The cut rule and the contraction rule of IIL can be shown to be eliminable. In order to further bridge the gap between these two systems, it is important to establish control over the use of structural rules in IIL proofs so that any copying of the principal formulas into the premises is made inessential. Consider the IIL proof of the sequent $l \supset r, (p \supset q) \supset l, (q \supset r) \supset q \vdash r$, where Σ denotes $l \supset r, (p \supset q) \supset l, (q \supset r) \supset q$ given in Figure 1.

One clear difficulty in translating that proof into IMALL is that the multiset Σ appears in every sequent in the proof. In IMALL, a formula can appear as the principal formula of at most one inference along any branch of the proof. In the above proof, the copying of the principal formula of an inference into the premises seems essential. The formulas $(p \supset q) \supset l$ and $l \supset r$ appear twice as principal formulas, and in both cases, these duplicate occurrences are along the same branch of the proof. We can deal with the duplicate use of $l \supset r$ by rearranging the above proof as in Figure 2.

The next step is to deal with the copying of the formula $(p \supset q) \supset l$. For this purpose, we modify the $\mathbf{L}\supset$ rule of IIL to the following two rules:

$$\frac{\Gamma \vdash p \qquad \Gamma, B \vdash C}{\Gamma, (p \supset B) \vdash C}\mathbf{L}\supset\mathbf{1}$$

$$\frac{\Gamma, (B \supset C) \vdash (A \supset B) \qquad \Gamma, C \vdash D}{\Gamma, ((A \supset B) \supset C) \vdash D}\mathbf{L}\supset\mathbf{2}$$

We call the resulting system IIL*. The advantage of IIL* is that there is no copying.[1] An antecedent principal formula of the form $(A \supset B) \supset C$ is replaced

[1] Grigori Mints directed our attention to IIL*. He observes that IIL* provides a direct proof-theoretic explanation for the membership in PSPACE of the decision problem for propositional intuitionistic logic. Cut-free proofs in IIL* have a height that is bounded by the number of connectives in the conclusion sequent. An alternating Turing machine can therefore generate and check the proof of a given sequent in a nondeterministic manner within polynomial time.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma,p,q,p\vdash q}\mathbf{I}}{\Sigma,p,q\vdash p\supset q}\mathbf{R}\supset \quad \dfrac{}{\Sigma,p,q,l\vdash l}\mathbf{I}}{\Sigma,p,q\vdash l}\mathbf{L}\supset \quad \dfrac{}{\Sigma,p,q,r\vdash r}\mathbf{I}}{\Sigma,p,q\vdash r}\mathbf{L}\supset}{\Sigma,p\vdash q\supset r}\mathbf{R}\supset \quad \dfrac{}{\Sigma,p,q\vdash q}\mathbf{I}}{\Sigma,p\vdash q}\mathbf{L}\supset}{\Sigma\vdash p\supset q}\mathbf{R}\supset \quad \dfrac{\dfrac{}{\Sigma,r\vdash r}\mathbf{I} \quad \dfrac{}{\Sigma,l\vdash l}\mathbf{I}}{\Sigma,l\vdash r}\mathbf{L}\supset}{\Sigma\vdash r}\mathbf{L}\supset$$

Figure 1: Proof of $\Sigma \vdash r$ in IIL

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma,p,q,p\vdash q}\mathbf{I}}{\Sigma,p,q\vdash p\supset q}\mathbf{R}\supset \quad \dfrac{\dfrac{}{\Sigma,p,q,l\vdash l}\mathbf{I} \quad \dfrac{}{\Sigma,p,q,l,r\vdash r}\mathbf{I}}{\Sigma,p,q,l\vdash r}\mathbf{L}\supset}{\Sigma,p,q\vdash r}\mathbf{L}\supset}{\Sigma,p\vdash q\supset r}\mathbf{R}\supset \quad \dfrac{}{\Sigma,p,q\vdash q}\mathbf{I}}{\Sigma,p\vdash q}\mathbf{L}\supset}{\Sigma\vdash p\supset q}\mathbf{R}\supset \quad \dfrac{\dfrac{}{\Sigma,r\vdash r}\mathbf{I} \quad \dfrac{}{\Sigma,l\vdash l}\mathbf{I}}{\Sigma,l\vdash r}}{\Sigma\vdash r}\mathbf{L}\supset$$

Figure 2: Modified Proof

by the simpler formula $B \supset C$ in one of the premises of the $\mathbf{L} \supset \mathbf{2}$ rule. Let A, B, C, and D label the formulas $l \supset r$, $r \supset q$, $(q \supset r) \supset q$, and $q \supset l$, respectively. With these new rules, the above proof can be transformed to an IIL* proof as in Figure 3:

The cut-elimination theorem holds for IIL* as well. The absence of contraction and copying in IIL* along with the restriction on weakening make it possible to embed IIL* in IMALL. We defer the discussion of this part of the encoding until Section 3.

In summary, we provide a transformation from IIL sequents to IMALL sequents by transforming IIL proofs. Our main result is:

Theorem 1.1 IIL *can be embedded into* IMALL. *The embedding preserves the structure of cut-free proofs in* IIL*.

IIL proofs are transformed by eliminating any use of the cut and contraction rules, by reducing the depth of any formula in the proof to two or less, permuting the order of the rules, and modifying the $\mathbf{L} \supset$ rule so as to eliminate the need for copying. The resulting IIL* proofs can then be embedded in IMALL.

The main result of this paper addresses the issue of replacing copying and reuse in intuitionistic proofs by sharing. We believe that our results contribute to the understanding of the role of linear logic as an expressive and natural framework for describing the control structure of logic programs. Indeed, the cut-free, implicational fragment of intuitionistic logic provides a reasonable framework for logic programming [MNPS90].

2 Properties of IIL

In this section, we present a series of lemmas about IIL that eventually establish the eliminability of contraction, the admissibility of weakening, and the redundancy of copying in IIL proofs.

Proposition 2.1 *For any sequent* $\Sigma \vdash A$ *appearing in any* IIL *proof of* $\Gamma \vdash B$, *the multiset* Γ *is a submultiset of* Σ.

This conservation of hypothesis formulas in IIL proofs provides the key to the elimination of contraction as shown by Propositions 2.2 and 2.3. The *size* of a proof is taken to be the number of inferences in it.

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A,B,p,q \vdash q}\,\mathbf{I} \qquad \dfrac{\dfrac{}{B,p,q,l \vdash l}\,\mathbf{I} \quad \dfrac{}{B,p,q,l,r \vdash r}\,\mathbf{I}}{A,B,p,q,l \vdash r}\,\mathbf{L}\supset\mathbf{1}}{A,D,B,p,q \vdash r}\,\mathbf{L}\supset\mathbf{1}}{A,D,B,p \vdash q \supset r}\,\mathbf{R}\supset \qquad \dfrac{}{A,D,p,q \vdash q}\,\mathbf{I}}{\dfrac{A,D,(q \supset r) \supset q, p \vdash q}{A,D,(q \supset r) \supset q \vdash p \supset q}\,\mathbf{R}\supset}\,\mathbf{L}\supset\mathbf{2} \qquad \dfrac{\dfrac{}{A,C,r \vdash r}\,\mathbf{I} \quad \dfrac{}{A,C,l \vdash l}\,\mathbf{I}}{A,C,l \vdash r}}{\Sigma \vdash r}\,\mathbf{L}\supset\mathbf{2}
$$

Figure 3: "Linear" Proof in IIL*

$$\dfrac{}{\Gamma, p_i \vdash p_i}\,\mathbf{I}$$

$$\dfrac{\Gamma, A \vdash B}{\Gamma \vdash (A \supset B)}\,\mathbf{R}\supset$$

$$\dfrac{\Gamma, (A \supset B) \vdash A \qquad \Gamma, (A \supset B), B \vdash C}{\Gamma, (A \supset B) \vdash C}\,\mathbf{L}\supset$$

$$\dfrac{\Gamma, A, A \vdash B}{\Gamma, A \vdash B}\,\mathbf{Contraction}$$

$$\dfrac{\Gamma \vdash C \qquad \Gamma, C \vdash B}{\Gamma \vdash B}\,\mathbf{Cut}$$

Figure 4: Rules for IIL

Proposition 2.2 *Given a proof of* $\Gamma, A, A \vdash B$ *of size* n *in* IIL*, we can produce a proof of* $\Gamma, A \vdash B$ *of size* n *in* IIL.

Proposition 2.3 *Given a proof of* $\Gamma \vdash A$ *of size* n *in* IIL*, we can construct a proof of* $\Gamma \vdash A$ *in* IIL *of size no greater than* n *that does not employ the contraction rule.*

Proposition 2.4 *If there is a proof of* $\Gamma \vdash A$ *in* IIL *then there is a proof of* $\Gamma \vdash A$ *in* IIL *that does not employ the cut rule.*

(See the proof for G3 in [Kle52].)

Proposition 2.5 *Any proof of* $\Gamma \vdash A$ *in* IIL *can be transformed into a proof of* $\Gamma \vdash A$ *in* IIL *that does not employ the contraction or cut rules.*

Proposition 2.6 *Given a proof of* $\Gamma \vdash B$ *of size* n *in* IIL*, we can produce a proof of* $\Gamma, A \vdash B$ *of size* n *in* IIL.

$$\dfrac{}{\Gamma, p_i \vdash p_i}\,\mathbf{I}$$

$$\dfrac{\Gamma, A \vdash B}{\Gamma \vdash (A \supset B)}\,\mathbf{R}\supset$$

$$\dfrac{\Gamma \vdash p_i \qquad \Gamma, B \vdash C}{\Gamma, (p_i \supset B) \vdash C}\,\mathbf{L}\supset\mathbf{1}$$

$$\dfrac{\Gamma, (B \supset C) \vdash (A \supset B) \qquad \Gamma, C \vdash D}{\Gamma, ((A \supset B) \supset C) \vdash D}\,\mathbf{L}\supset\mathbf{2}$$

Figure 5: Rules for IIL*

Proposition 2.7 *Given a proof of* $\Gamma, A \supset B, B \vdash C$ *of size* n *in* IIL*, we can find a proof of* $\Gamma, B \vdash C$ *of size less than or equal to* n *in* IIL.

Proposition 2.8 *For all* IIL *formulas* A, B, C *the sequent* $(A \supset B) \supset C \vdash B \supset C$ *is provable in* IIL.

Proposition 2.9 *Given an* IIL *proof of* $\Gamma, (A \supset B) \supset C, B \supset C, A \vdash D$ *of size* n*, we can construct an* IIL *proof of* $\Gamma, B \supset C, A \vdash D$ *of size no more than* n.

We now introduce an interesting refinement of IIL called IIL*, and prove that cut-free, contraction-free IIL proofs are easily transformed to proofs in IIL*. The proof rules for IIL* are given in Figure 5. Similar logics have been studied by others [Vor58, Pli65, Hud89, Dyc91].

Note that the identity rule is only applicable to atomic propositions, and that weakening is only allowed at the leaves of a proof, *i.e.*, at an application of identity. Most important, however, is the property that the principal formula is not duplicated in the premises of any of the rules in IIL*.

Proposition 2.10 *Given a proof of* $\Gamma \vdash B$ *of size* n *in* IIL*, *we can produce a proof of* $\Gamma, A \vdash B$ *of size* n *in* IIL*.

Lemma 2.11 *Given a proof of* $\Gamma \vdash A$ *in* IIL*, *a proof of* $\Gamma \vdash A$ *can be constructed in* IIL.

Proof. By induction on IIL* proofs using Propositions 2.10 and 2.9. ∎

The other direction of the equivalence of IIL and IIL* is somewhat more complicated. We adapt an argument due to Dyckhoff [Dyc91] to achieve this result.

Consider an $\mathbf{L}\supset$ inference in an IIL proof with a principal antecedent formula of the form $p \supset A$. Let $\Gamma \vdash C$ be the conclusion sequent of the inference. The inference is said to be *backward* if p does not occur in Γ. A *forward* proof is one with no backward inferences. These names are chosen to be reminiscent of forward and backward chaining.

Lemma 2.12 *Any cut-free, contraction-free* IIL *proof* Π *of size* n *can be transformed to a cut-free, contraction-free forward proof* Θ *of size no more than* n *with the same conclusion as* Π.

Proof. The proof is by induction on the size of the cut-free, contraction-free proof Π.

If the final inference in Π is not a backward inference, then we have the result immediately by induction.

If the final step is a backward inference in Π, then we use the induction hypothesis to eliminate the backward inferences in the subproofs of the premises. This transforms the proof Π to the form below, where the only backward inference is the final one.

$$\dfrac{\begin{matrix}\Theta_1\\ \vdots\\ \Gamma, p\supset A \vdash p\end{matrix} \qquad \begin{matrix}\Theta_2\\ \vdots\\ \Gamma, p\supset A, A \vdash C\end{matrix}}{\Gamma, p \supset A \vdash C}\ \mathbf{L}\supset$$

The premise $\Gamma, p \supset A \vdash p$ cannot be an axiom since p does not occur in Γ. The final inference in the proof Θ_1 of $\Gamma, p \supset A \vdash p$ must therefore be an $\mathbf{L}\supset$ inference whose principal formula is either of the form $(D \supset E) \supset F$ or of the form $q \supset B$ where q occurs in Γ. In either case, these inferences can be permuted below the final inference in Π, as in Figure 6.

In Figure 6 Θ_2' is obtained from Θ_2 by Proposition 2.6 but has the same size as Θ_2. The backward inference with the subproofs Θ_{12} and Θ_2' is smaller than Π and we can therefore employ the induction hypothesis to eliminate the backward inference from it. The resulting proof is therefore free of backward inferences and has size no larger than Π.

The other possibility is that the principal formula is of the form $q \supset B$ where q occurs in Γ. In this case the inferences permute similarly, and the resulting proof may be seen to be forward by induction, and the fact that q occurs in Γ. ∎

Lemma 2.13 *Given a proof of* $\Gamma \vdash C$ *in* IIL, *a proof of* $\Gamma \vdash C$ *can be constructed in* IIL*.

Proof. By Lemma 2.12, we can restrict our attention to forward proofs. We proceed by induction on $weight(\sigma)$ for a sequent σ, as defined in Figure 7.

It is easy to show by induction on the structure of A that if $0 < c < d$, then $0 < m(A, c) < m(A, d)$.

If the given IIL proof of $\Gamma \vdash C$ is an axiom, then the proof is also an IIL* proof.

If the final inference in the given IIL proof is $\mathbf{R}\supset$ applied to a conclusion of the form $\Gamma \vdash A \supset B$ to generate the premise $\Gamma, A \vdash B$, then this premise is of smaller weight. We can therefore apply the induction hypothesis to the premise to get an IIL* proof of $\Gamma, A \vdash B$ from which the IIL* proof of $\Gamma \vdash A \supset B$ can be completed by the $\mathbf{R}\supset$ rule of IIL*.

If the final inference in the given IIL rule is $\mathbf{L}\supset$ applied to a principal formula of the form $p \supset B$ where Γ has the form $\Sigma, p \supset B$, then p must occur in Σ. The nontrivial premise is then $\Sigma, p \supset B, B \vdash C$. By Proposition 2.7, the sequent $\Sigma, B \vdash C$ must also have an IIL proof and since it is of smaller weight than $\Sigma, p \supset B \vdash C$, the induction hypothesis can be applied to it yielding an IIL* proof of $\Sigma, B \vdash C$. Since p occurs in Σ, the sequent $\Sigma \vdash p$ is an IIL* axiom. The required IIL* proof of $\Sigma, p \supset B \vdash C$ can be constructed using the $\mathbf{L}\supset\mathbf{1}$ rule with the premises $\Sigma, B \vdash C$ and $\Sigma \vdash p$.

If the final inference in the given IIL proof is $\mathbf{L}\supset$ applied to a principal formula of the form $(D \supset E) \supset F$, where Γ is of the form $\Sigma, (D \supset E) \supset F$, then we have IIL proofs for the two premises $\Sigma, (D \supset E) \supset F \vdash D \supset E$ and $\Sigma, (D \supset E) \supset F, F \vdash C$. Proposition 2.7 applied to the second premise yields an IIL proof of $\Sigma, F \vdash C$ to which the induction hypothesis can be applied yielding an IIL* proof of $\Sigma, F \vdash C$. Since in IIL we can prove $D, (E \supset F) \vdash (D \supset E) \supset F$ and $D, (D \supset E) \vdash E$, we can use the cut rule twice with the sequent $\Sigma, (D \supset E) \supset F \vdash D \supset E$ to get an IIL

$$\dfrac{\dfrac{\begin{array}{c}\Theta_{11}\\ \vdots\\ \Gamma, p \supset A \vdash D \supset E\end{array} \qquad \begin{array}{c}\Theta_{12}\\ \vdots\\ \Gamma, p \supset A, F \vdash p\end{array}}{\Gamma, p \supset A \vdash p}\,\mathbf{L}\supset \qquad \begin{array}{c}\Theta_{2}\\ \vdots\\ \Gamma, p \supset A, A \vdash C\end{array}}{\Gamma, p \supset A \vdash C}\,\mathbf{L}\supset$$

becomes

$$\dfrac{\begin{array}{c}\Theta_{11}\\ \vdots\\ \Gamma, p \supset A \vdash D \supset E\end{array} \qquad \dfrac{\begin{array}{c}\Theta_{12}\\ \vdots\\ \Gamma, p \supset A, F \vdash p\end{array} \qquad \begin{array}{c}\Theta_{2}'\\ \vdots\\ \Gamma, p \supset A, F, A \vdash C\end{array}}{\Gamma, p \supset A, F \vdash C}\,\mathbf{L}\supset}{\Gamma, p \supset A \vdash C}\,\mathbf{L}\supset$$

Figure 6: Permuting backward inferences

$$\begin{array}{rcl} \mathit{weight}(A_1, \ldots, A_n \vdash C) & = & m(A_1, 1) + \ldots + m(A_n, 1) + m(C, 1) \\ m(A \supset B, d) & = & m(A, d+1) + (d * m(B, d)) + 1 \\ m(p, d) & = & d \end{array}$$

Figure 7: Definition of *weight*

proof of $\Sigma, E \supset F, D \vdash E$. The difference in weight between this last sequent and the original conclusion sequent $\Sigma, (D \supset E) \supset F \vdash C$ is given in Figure 8.

So the induction hypothesis yields an IIL* proof of $\Sigma, E \supset F, D \vdash E$ which by $\mathbf{R} \supset$ yields an IIL* proof of $\Sigma, E \supset F \vdash D \supset E$. This last sequent with $\Sigma, F \vdash C$ yield an IIL* proof of $\Sigma, (D \supset E) \supset F \vdash C$ by the $\mathbf{L} \supset \mathbf{2}$ rule of IIL*.

■

The lack of contraction in IIL* makes this formulation of the sequent rules for implicational intuitionistic propositional logic amenable to encoding into IMALL.

3 IIL* to IMALL

An intuitionistic linear logic sequent is composed of two multisets of linear logic formulas separated by a $\vdash$. We assume a set of propositional atoms p_i to be given. The rules of IMALL are such that every derivable sequent contains no more than one formula in its consequent multiset. Figure 9 gives the inference rules for the intuitionistic linear sequent calculus, with the slight restriction that the 0 rule is omitted. This omission does not pose problems for cut elimination.

We now give a pair of translation functions which transform any IIL* formula into an IMALL formula. The simultaneous definitions of $[\,]^+$ and $[\,]^-$ given in Figure 10 can be seen to be well defined by induction on the size of the formulas.

For any IIL* sequent $\Gamma \vdash C$ we define

$$\theta(\Gamma \vdash C) \triangleq [\Gamma]^-, k \vdash [C]^+$$

Here $[\Gamma]^-$ stands for the result of the application of $[\,]^-$ to each element of Γ. Note that the "key" k is present in the context of the encoding of a sequent. We have chosen the notations $[\,]^+$ and $[\,]^-$ to suggest the interpretation of positive and negative polarity of occurrences.

Lemma 3.1 *For any* IIL* Γ *and* C*, the sequent* $[\Gamma]^-, k, \bot \vdash [C]^+$ *is provable in* IMALL.

This lemma is proved by induction on the right-hand depth of C. If $C = p_i$ is a proposition, we can construct an IMALL proof as in Figure 11.

In the case that $C = (A \supset B)$ is an implication, we know that B is of smaller depth than C, and we can construct the proof as in Figure 12.

$$
\begin{array}{l}
weight(\Sigma, (D \supset E) \supset F \vdash C) - \;\; weight(\Sigma, E \supset F, D \vdash E) \\
\\
\begin{array}{rl}
= & m((D \supset E) \supset F, 1) + m(C, 1) - m(E \supset F, 1) - m(D, 1) - m(E, 1) \\
= & m(D, 3) + 2m(E, 2) + 2 + m(F, 1) + 1 + m(C, 1) - m(E, 2) - m(F, 1) - 1 - m(D, 1) - m(E, 1) \\
> & 0
\end{array}
\end{array}
$$

Figure 8: Example calculation of weight

$$
\begin{array}{lcclc}
\mathbf{I} & \dfrac{}{A \vdash A} & & \dfrac{\Sigma \vdash A \qquad A, \Gamma \vdash B}{\Sigma, \Gamma \vdash B} & \mathbf{Cut} \\[2ex]
\otimes\mathbf{L} & \dfrac{\Sigma, A, B \vdash C}{\Sigma, (A \otimes B) \vdash C} & & \dfrac{\Sigma \vdash A \qquad \Gamma \vdash B}{\Sigma, \Gamma \vdash (A \otimes B)} & \otimes\mathbf{R} \\[2ex]
\multimap\mathbf{L} & \dfrac{\Sigma \vdash A \qquad \Gamma, B \vdash C}{\Sigma, \Gamma, (A \multimap B) \vdash C} & & \dfrac{\Sigma, A \vdash B}{\Sigma \vdash (A \multimap B)} & \multimap\mathbf{R} \\[2ex]
\oplus\mathbf{L} & \dfrac{\Sigma, A \vdash C \qquad \Sigma, B \vdash C}{\Sigma, (A \oplus B) \vdash C} & & \dfrac{\Sigma \vdash A \qquad \Sigma \vdash B}{\Sigma \vdash (A \& B)} & \&\mathbf{R} \\[2ex]
\&\mathbf{L1} & \dfrac{\Sigma, A \vdash C}{\Sigma, (A \& B) \vdash C} & & \dfrac{\Sigma \vdash A}{\Sigma \vdash (A \oplus B)} & \oplus\mathbf{R1} \\[2ex]
\&\mathbf{L2} & \dfrac{\Sigma, B \vdash C}{\Sigma, (A \& B) \vdash C} & & \dfrac{\Sigma \vdash B}{\Sigma \vdash (A \oplus B)} & \oplus\mathbf{R2} \\[2ex]
\bot\mathbf{L} & \dfrac{}{\bot \vdash} & & \dfrac{\Sigma \vdash}{\Sigma \vdash \bot} & \bot\mathbf{R} \\[2ex]
1\mathbf{L} & \dfrac{\Sigma \vdash A}{\Sigma, 1 \vdash A} & & \dfrac{}{\vdash 1} & 1\mathbf{R} \\[2ex]
 & & & \dfrac{}{\Sigma \vdash \top} & \top\mathbf{R}
\end{array}
$$

Figure 9: Rules for IMALL

$$
\begin{array}{rcl}
[A \supset B]^+ & \triangleq & k \otimes ([A]^- \multimap (k \multimap [B]^+)) \\
{[p_i]^+} & \triangleq & k \otimes ((p_i \oplus \bot) \otimes \top) \\
\\
{[p_i]^-} & \triangleq & p_i \\
{[p_i \supset A]^-} & \triangleq & k \multimap (((k \multimap [p_i]^+) \multimap (k \otimes \bot)) \oplus (k \otimes [A]^-)) \\
{[(A \supset B) \supset C]^-} & \triangleq & k \multimap ((([(B \supset C)]^- \multimap (k \multimap [(A \supset B)]^+)) \multimap (k \otimes \bot)) \oplus (k \otimes [C]^-))
\end{array}
$$

Figure 10: Definition of translation

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\bot \vdash}\bot\mathbf{L}}{\bot \vdash \bot}\bot\mathbf{R}}{\bot \vdash p_i \oplus \bot}\oplus R \qquad \dfrac{}{[\Gamma]^- \vdash \top}\top R}{[\Gamma]^-, \bot \vdash (p_i \oplus \bot) \otimes \top}\otimes R \qquad \dfrac{}{k \vdash k}\mathbf{I}}{[\Gamma]^-, k, \bot \vdash k \otimes ((p_i \oplus \bot) \otimes \top)}\otimes R$$

Figure 11: Case one of Lemma 3.1.

$$\dfrac{\dfrac{\dfrac{\begin{array}{c}\vdots\\ [\Gamma]^-, [A]^-, k, \bot \vdash [B]^+\end{array}}{[\Gamma]^-, [A]^-, \bot \vdash k \multimap [B]^+}\multimap\mathbf{R}}{[\Gamma]^-, \bot \vdash [A]^- \multimap (k \multimap [B]^+)}\multimap\mathbf{R} \qquad \dfrac{}{k \vdash k}\mathbf{I}}{[\Gamma]^-, k, \bot \vdash k \otimes ([A]^- \multimap (k \multimap [B]^+))}\otimes\mathbf{R}$$

Figure 12: Case two of Lemma 3.1.

Lemma 3.2 *For any* IIL* *multiset* Γ *and proposition* p_i*, the sequent* $[\Gamma]^-, [p_i]^-, k \vdash [p_i]^+$ *is provable in* IMALL.

This lemma is proved by expanding the definition of $[p_i]^+$, as seen in Figure 13.

In order to show that the translation is correct and faithful, we need to show that there exists a cut-free proof of $\Gamma \vdash C$ in IIL* if and only if there is a cut-free proof of $\theta(\Gamma \vdash C)$ in IMALL. We demonstrate this in two steps below, after demonstrating how parts of our example IIL* sequent are translated into IMALL.

Consider the sequent $\Sigma', (p \supset q) \supset l \vdash r$, where Σ' abbreviates $l \supset r, (q \supset r) \supset q$. This sequent has the θ-translation $[\Sigma']^-, [(p \supset q) \supset l]^-, k \vdash [r]^+$. By the above definition, $[(p \supset q) \supset l]^- = k \multimap ((([(q \supset l)]^- \multimap (k \multimap [(p \supset q)]^+)) \multimap (k \otimes \bot)) \oplus (k \otimes [l]^-))$. In the example IIL* proof given in Figure 3, the proof of this sequent ends in an application of the $\mathbf{L} \supset \mathbf{2}$ rule.

The intuitive structure of the proof in Figure 14 is as follows. The leftmost application of **I** and the bottommost application of $\multimap$**L** correspond to "unlocking" the formula of interest. The unlocked formula corresponding to $(p \supset q) \supset l$ has $\oplus$ as its main connective. The proof tree therefore forks, and after a simple application of $\otimes$**L**, the rightmost branch can be seen to be the translation of the rightmost branch of the IIL* proof.

The left main branch of the proof progresses by applying the $\multimap$**L** rule. Here there is a choice to be made in the way we split the context Σ' among the branches of the proof. However, because of the form of our translation, we can without loss of generality choose to keep the entire context on the left branch. By lemma 3.1 $k, \bot \vdash [r]^+$, the upper right branch, is provable. And finally, we see that after two applications of $\mathbf{R} \supset$ we are left with the translation of the right hand branch of the IIL* proof.

In fact, the encoding is such that there are essentially no choices to be made in the proof of the IMALL translation that cannot be made in the proof of an IIL* formula. For example, once a formula is unlocked with the "key" k, no other formula may be unlocked until the unlocked formula is reduced completely, at which point it provides another key k. We argue that there is a proof of an IIL* formula if and only if there is a proof its translation in IMALL.

Lemma 3.3 *If there is a cut-free proof of* $\Sigma \vdash C$ *in* IIL**, then there is a cut-free proof of* $\theta(\Sigma \vdash C)$ *in* IMALL.

This lemma is proved by induction on the height of proof in IIL*.

We now introduce two propositions which simplify the other direction of the main theorem. These propositions are mild alterations of lemmas used to establish the PSPACE-completeness of IMALL [LMSS90]. The first proposition is only used to prove the second, and

$$\dfrac{\dfrac{\dfrac{\dfrac{}{p_i \vdash p_i}\mathbf{I}}{p_i \vdash p_i \oplus \bot}\oplus R \qquad \dfrac{}{[\Gamma]^- \vdash \top}\top R}{[\Gamma]^-, p_i, \vdash (p_i \oplus \bot) \otimes \top}\otimes R \qquad \dfrac{}{k \vdash k}\mathbf{I}}{[\Gamma]^-, p_i, k \vdash k \otimes ((p_i \oplus \bot) \otimes \top)}\otimes R$$

Figure 13: Proof of Proposition 3.2.

$$\dfrac{\begin{array}{c}\vdots\\ \Sigma', (q \supset l) \vdash (p \supset q)\end{array} \qquad \begin{array}{c}\vdots\\ \Sigma', l \vdash r\end{array}}{\Sigma', ((p \supset q) \supset l) \vdash r}\mathbf{L} \supset \mathbf{2}$$

$$\Downarrow$$

$$\dfrac{\dfrac{}{k \vdash k}\mathbf{I} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\begin{array}{c}\vdots\\ [\Sigma']^-, [(q \supset l)]^-, k \vdash [(p \supset q)]^+\end{array}}{[\Sigma']^-, [(q \supset l)]^- \vdash k \multimap [(p \supset q)]^+}\multimap\mathbf{R}}{[\Sigma']^- \vdash ([(q \supset l)]^- \multimap (k \multimap [(p \supset q)]^+))}\multimap\mathbf{R} \qquad \dfrac{\begin{array}{c}\vdots\\ k, \bot \vdash [r]^+\end{array}}{k \otimes \bot \vdash [r]^+}\otimes\mathbf{L}}{[\Sigma']^-, ([(q \supset l)]^- \multimap (k \multimap [(p \supset q)]^+)) \multimap (k \otimes \bot) \vdash [r]^+}\multimap\mathbf{L} \qquad \dfrac{\begin{array}{c}\vdots\\ [\Sigma']^-, k, [l]^- \vdash [r]^+\end{array}}{[\Sigma']^-, k \otimes [l]^- \vdash [r]^+}\otimes\mathbf{L}}{[\Sigma']^-, (([(q \supset l)]^- \multimap (k \multimap [(p \supset q)]^+)) \multimap (k \otimes \bot)) \oplus (k \otimes [l]^-) \vdash [r]^+}\oplus\mathbf{L}}{[\Sigma']^-, k, k \multimap ((([(q \supset l)]^- \multimap (k \multimap [(p \supset q)]^+)) \multimap (k \otimes \bot)) \oplus (k \otimes [l]^-)) \vdash [r]^+}\multimap\mathbf{L}$$

Figure 14: IIL* and IMALL proofs of example.

the second proposition formally states that in a cut-free IMALL proof no lock can be opened before there is a key available at top level.

Proposition 3.4 *For any atomic proposition p, and sequence Δ not containing the constant 1 or the constant 0 the sequent $\Delta \vdash p$ is not provable in* IMALL *unless Δ is identically p, or contains a subformula of the form $p\&A$, $A\&p$, $p \oplus A$, $A \oplus p$, or $A \multimap p$ for some formula A.*

Note that the clause about the constant 0 is not actually needed in our formulation of IMALL. However, this property could be of interest outside the scope of this paper, and thus we state it exactly for full intuitionistic two-sided multiplicative additive linear logic.

Proposition 3.5 *For any formula F which is a subformula of an encoding $[\,]^-$ or $[\,]^+$ and which is not identically k, F must be reduced below any other formula in any* IMALL *proof of $[\Gamma]^-, F \vdash [C]^+$ or $[\Gamma]^- \vdash F$.*

Lemma 3.6 *If there is a proof of $\theta(\Gamma \vdash C)$ in* IMALL*, then there is a proof of $\Gamma \vdash C$ in* IIL*.

Proof. (Sketch) To prove this lemma, we perform cut-elimination on the given IMALL proof, and then observe that the resulting proof must be of a very special form. In fact, an IIL* proof can be directly read from any such proof. The action of the "locks and keys" encoded by the positive and negative occurrences of k in the IMALL translations forces any cut-free IMALL proof of a sequent to have a very specific form. Proposition 3.5 states this formally. It is exactly this sort of control over the shape of a proof which one can encode in linear logic sequents, but which is impossible to encode in intuitionistic and classical logic. The proof of this lemma proceeds by induction on the size of cut-free IMALL proof.

Given a cut-free IMALL proof of a sequent $\theta(\Gamma \vdash C)$, we see which IMALL proof rule was applied last. Because the proof is cut-free, the last rule cannot be cut. Investigating the forms of IMALL formulas which can appear in a θ-translation, we see that the last proof rule applied must be either $\multimap$L, $\otimes$R, or identity. However, even identity cannot apply, since k always appears on the left in any θ-translation, and k never appears at top level on the right in such a translation. Thus there are only two cases to consider, left implication, and right tensor.

For example, consider the case when $\otimes$R is the last rule applied in a proof, and the principal formula is of the form $k \otimes ([A]^- \multimap (k \multimap [B]^+))$. The IMALL proof must then have the form:

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{[\Gamma]^-, [A]^-, k \vdash [B]^+}}{[\Gamma]^-, [A]^- \vdash k \multimap [B]^+}{\multimap}\mathbf{R}}{[\Gamma]^- \vdash [A]^- \multimap (k \multimap [B]^+)}{\multimap}\mathbf{R} \qquad \dfrac{}{k \vdash k}\mathbf{I}}{[\Gamma]^-, k \vdash k \otimes ([A]^- \multimap (k \multimap [B]^+))}{\otimes}\mathbf{R}$$

We know that the IMALL proof takes this form, since if any part of $[\Gamma]^-$ were to be included in the right premise, IMALL identity would not apply, and in fact there could be no proof of that branch of the proof, as stated in proposition 3.4. Also, since there is no k at top level in the left premise of the $\otimes$R rule, reducing any formulas in $[\Gamma]^-$ could not lead to a proof by proposition 3.5. This reasoning applies twice, leaving us with the proof displayed above. This proof can be simulated in IIL* by applying the $\mathbf{R} \supset$ rule, and the hypothesis, itself a θ-translation, can be simulated by induction.

The other case of $\otimes$R and the two cases of $\multimap$L are similar. ∎

4 Efficiency of Transformation

For any IIL sequent ρ we have provided an equiprovable IMALL sequent $\theta(\rho)$. This encoding into IMALL could be exponential in the size of ρ, but if ρ is of depth two or less, then $\theta(\rho)$ is linear in the size of ρ. Below we give a depth-reduction procedure which takes polynomial time and which produces a depth two term $\Xi(\rho)$ which is only linearly larger than ρ. The transformation $\theta(\Xi(\rho))$ therefore provides an argument for the PSPACE-hardness of the decision problem for IMALL. The argument for membership of this problem in PSPACE is immediate and appears in [LMSS90].

The transformation from IIL* to IMALL is efficient in another stronger manner. It preserves the structure of IIL* proofs. The IMALL translation of an IIL* proof is linear in the size of the given IIL* proof. Note that our transformation from IIL to IIL* does not necessarily preserve the structure of cut-free proofs in IIL due to the permutations that are needed to achieve make copying redundant. Neither of our transformations preserves the structure of proofs with cut.

4.1 Depth Reduction in IIL

An IIL formula of depth one is either an atom p or has the form $(p_i \supset p_j)$. A formula of depth two is one of the form $(p_i \supset (p_j \supset p_k))$, or the form $((p_i \supset p_j) \supset p_k)$. Given a sequent $\Gamma \vdash D$, we define $\Xi(\Gamma \vdash D)$ to be the result of repeatedly applying any of the the set of transformations given in Figure 15 until none of them apply.

These transformations each reduce the depth of implications, at the expense of building a new implication (which is also shallower than the original). Thus this sequence of reductions always terminates. Notice that the only kinds of formulas left after the Ξ transformation are of the form: $p_i, p_i \supset p_j, p_i \supset (p_j \supset p_k)$, or $(p_i \supset p_j) \supset p_k$, where p_i, p_j, and p_k are atomic propositions. Although all the formulas appearing are very small, there may be many more of them. This technique goes back to [Waj38], see also [Min90].

The following lemma is stated, without proof, for IIL. The analogous lemma holds for IIL* as well.

Lemma 4.1 *For any* IIL *sequent* σ*, the* IIL *sequent* $\Xi(\sigma)$ *contains formulas of depth at most two, and* $\Xi(\sigma)$ *is provable exactly when* σ *is provable.*

Depth reduction, Ξ, defined above takes place in polynomial time and the size of $\Xi(\sigma)$ is linear in the size of σ since, in the worst case, we introduce a constant number of new formulas for each subformula of σ.

5 Conclusion

Linear logic has already found a number of fruitful applications in computing. One reason for this is that linear logic is a well-motivated refinement of both classical and intuitionistic logic. It admits a Curry-Howard isomorphism that provides a mechanism for typing programs in such a way that intensional aspects of the program are made explicit in its type. The sequent formulation of linear logic admits a cut-elimination theorem. An interesting aspect of cut elimination is that it is possible in linear logic to encode constraints on the form of a cut-free proof in the conclusion sequent. Linear logic is therefore expressive in a manner that intuitionistic and classical logic are not. Our classification of the complexity and decidability of fragments of linear logic highlights some of this expressiveness [LMSS90].

Our embedding of the implicational fragment of propositional intuitionistic logic in the IMALL fragment of linear logic provides an alternative proof for the PSPACE-hardness of IMALL. More importantly, it provides insight into the use and elimination of the structural rules from IIL through the embedding of IIL into IIL*. The system IIL* is an interesting optimization of intuitionistic logic that could be useful

$$
\begin{array}{rcl}
\Gamma, (A \supset B) \supset (C \supset D) \vdash Z & \Rightarrow & x \supset (C \supset D), \Gamma, (A \supset B) \supset x \vdash Z \\
\Gamma, p_i \supset ((A \supset B) \supset C) \vdash Z & \Rightarrow & (A \supset B) \supset x, \Gamma, p_i \supset (x \supset C) \vdash Z \\
\Gamma, p_i \supset (A \supset (B \supset C)) \vdash Z & \Rightarrow & x \supset (B \supset C), \Gamma, p_i \supset (A \supset x) \vdash Z \\
\Gamma, ((A \supset B) \supset C) \supset p_i \vdash Z & \Rightarrow & x \supset (A \supset B), \Gamma, (x \supset C) \supset p_i \vdash Z \\
\Gamma, (A \supset (B \supset C)) \supset p_i \vdash Z & \Rightarrow & (B \supset C) \supset x, \Gamma, (A \supset x) \supset p_i \vdash Z \\
\Gamma \vdash (A \supset B) \supset (C \supset D) & \Rightarrow & (C \supset D) \supset x, \Gamma \vdash (A \supset B) \supset x \\
\Gamma \vdash p_i \supset (A \supset (B \supset C)) & \Rightarrow & (B \supset C) \supset x, \Gamma \vdash p_i \supset (A \supset x) \\
\Gamma \vdash p_i \supset ((A \supset B) \supset C)) & \Rightarrow & x \supset (A \supset B), \Gamma \vdash p_i \supset (x \supset C) \\
\Gamma \vdash (A \supset (B \supset C)) \supset p_i & \Rightarrow & x \supset (B \supset C), \Gamma \vdash (A \supset x) \supset p_i \\
\Gamma \vdash ((A \supset B) \supset C)) \supset p_i & \Rightarrow & (A \supset B) \supset x, \Gamma \vdash (x \supset C) \supset p_i
\end{array}
$$

Figure 15: Definition of Ξ

in theorem proving and logic programming applications [Mil90].

A number of questions remain open. An extension of our techniques to all intuitionistic propositional connectives should be investigated. On the other hand, it would be interesting to know whether there is an embedding of intuitionistic implication in IMALL that preserves the structure of all cut-free proofs. We would also like to know the complexity of cut-elimination for the system IIL* with a cut rule. It is worth examining what transformations such as depth reduction mean at the level of proof terms given by the Curry-Howard isomorphism, and whether there are some useful optimizations in the evaluation of proof terms arising from such a study.

We would like to thank Jean-Yves Girard, Grigori Mints, and John Mitchell for very stimulating discussions. We are also grateful to Grigori Mints for help in investigating the literature.