Towards a linear contract logic

Massimo Bartoletti[1], Paolo Di Giamberardino[1], and Roberto Zunino[2]

[1] Università degli Studi di Cagliari, Italy — {bart , digiambe}@unica.it
[2] Università degli Studi di Trento, Italy — roberto.zunino@unitn.it

Abstract. We introduce a linear logic for contracts. The logic (called PCLLW) extends intuitionistic linear affine logic ILLW with a contractual implication connective, along the lines of Propositional Contract Logic (PCL [4]). A proof system for PCLLW is presented, and it is shown sound and complete with respect to a phase structure model. By exploiting the finite model property, we show that PCLLW is decidable.

1 Introduction

Propositional Contract Logic (PCL) was introduced in [4] as an extension of intuitionistic propositional logic IPC with a new connective $\twoheadrightarrow$, called *contractual implication*. Its aim was that of resolving *circular* dependencies among offers and requests in contractual clauses. The archetypical example is that of, say, a buyer offering B in exchange of the promise of obtaining A, and a seller offering A in exchange of a promise of B. In PCL, these contracts lead the two participants to an *agreement*, modelled by the theorem:

$$(A \twoheadrightarrow B) \ \wedge \ (B \twoheadrightarrow A) \ \vdash \ A \ \wedge \ B$$

Of course, an agreement would have been possible also if one of the participants (say, the buyer) were just offering B without asking anything in exchange. In such case, the buyer can wait for the other doing the first step, *before* doing A:

$$B \ \wedge \ (B \to A) \ \vdash \ A \ \wedge \ B$$

The formal justification for the connective $\twoheadrightarrow$ was then given in [3,1], where it is shown that, in the presence of circular offer-request constraints, either the participants reach an agreement, or some of them is not *protected* by her contract. Intuitively, the contract B does not protect the buyer, because it just dictates him to do B, without asking anything in exchange; instead, $A \twoheadrightarrow B$ protects him, by stating that B is an obligation only if A is guaranteed to happen, eventually.

A proof system for PCL was defined in [4] in terms of Gentzen-style rules, which extend those of IPC; decidability of PCL was then established by showing that the proof system enjoys cut elimination and the subformula property.

PCL is a suitable model for contracts when the atomic entities of the logic represent *events*, which can only occur once (as e.g., in event structures [11]). Were atoms used to model resources, which are subject to linearity constraints,

$$\frac{\Gamma \vdash B}{\Gamma \vdash A \multimap B}\ \textsc{Zero} \qquad \frac{\Gamma, B \vdash A \qquad \Gamma, B \vdash C}{\Gamma, A \multimap B \vdash C}\ \textsc{Fix} \qquad \frac{\Gamma, A \vdash C \qquad \Delta, D \vdash B}{\Gamma, \Delta, C \multimap D \vdash A \multimap B}\ \textsc{PrePost}$$

Fig. 1. Sequent calculus for PCLLW (only rules for contractual implication).

PCL would no longer be adequate. For instance, there is no obvious way to model a situation where two occurrences of resource A have to be consumed to produce an occurrence of B.

Linear logic [7] has been described as a *resource-aware* logic [10]. This is evident by the absence of the structural rules of weakening and contraction, which otherwise would allow for free duplication/elimination of resources. It then seems a viable idea that of studying the circularity issues addressed by PCL in the setting of linear logic.

In this paper we start developing this idea, by extending intuitionistic linear affine logic ILLW with a new connective $\multimap$, playing the same role as contractual implication in PCL. Our logic allows for a sound encoding of PCL (Th. 1), and it enjoys some desirable structural properties, e.g. cut elimination (Th. 2). In §3 we combine results of Ciabattoni, Okada and Terui [12,6] to construct a sound and complete model of PCLLW, in the form of affine phase structures (Th. 3 and Th. 4). Along the same lines of [12,6], we show that PCLLW enjoys the finite model property (Th. 5), and we exploit this fact to prove it decidable (Th. 6).

An open question is whether, neglecting the nice properties it enjoys, PCLLW exactly captures the intuitively valid properties of contracts. We discuss some possible issues in §4.

2 Linear affine contract logic

The logic PCLLW extends ILLW with a connective $\multimap$, which is the linear version of the contractual implication of PCL. Intuitively, we may interpret the linear contractual implication $A \multimap B$ as "I will provide the resource B if the resource A at some point becomes available". A sequent calculus for PCLLW is presented in Fig. 1. Rule Zero states that provable formulae are contractually implied; rule PrePost provides $\multimap$ with the same weakening properties of $\multimap$. The crucial rule is Fix, which is the left rule for $\multimap$. Compared to the rule $\multimap$L of ILL, there are two differences: first, in the leftmost premise we allow for using the consequence B of a contractual implication $A \multimap B$; second, we use the same context Γ in both premises. We now discuss some relevant properties of PCLLW.

1. $(A \multimap B) \otimes (B \multimap A) \vdash A \otimes B$. This is the fundamental property of the system: it represents the handshake between two contracts, resulting in the presence of both the resources A and B at the same time; we stress that, in Linear Logic, from $A \multimap B$ and $B \multimap A$, $A \otimes B$ cannot be deduced.
2. $A \multimap B \nvdash B$. This states that in the absence of the resource A, the resource B cannot be provided by the contract $A \multimap B$.

$$
\begin{array}{rclcrcl}
X^* & = & X & & (A \to B)^* & = & !A^* \multimap B^* \\
(A \wedge B)^* & = & A^* \& B^* & & (A \vee B)^* & = & !A^* \oplus !B^* \\
(A \twoheadrightarrow B)^* & = & !A^* \multimap\!\!\!\circ\, !B^* & & (\Gamma \vdash A)^* & = & !\Gamma^* \vdash A^*
\end{array}
$$

Fig. 2. Translation of PCL formulae into PCLLW formulae.

3. $B \vdash A \multimap\!\!\!\circ\, B$ This states that if the resource B has already been provided, then it can be provided with $\multimap\!\!\!\circ$ under any condition.
4. $A \multimap\!\!\!\circ\, A \vdash A$. This represents the natural property that if the resource A is provided under the condition that the resource A is provided, then A is provided. This is coherent with the fact that $A \twoheadrightarrow A \vdash A$ holds in PCL.
5. $((A \multimap\!\!\!\circ\, B) \otimes ((B \otimes B) \multimap\!\!\!\circ\, A)) \not\vdash (A \otimes B)$. This property and the following one are strictly related to linearity. A contract offering one occurrence of B fails the handshake with a contract requesting two occurrences of B.
6. $(A \multimap\!\!\!\circ !B) \otimes ((B \otimes B) \multimap\!\!\!\circ\, A) \vdash A \otimes B$. Here there is an agreement, since the resource B offered by the first contract is under a !, so is available *ad libitum*.
7. $(A \multimap\!\!\!\circ\, B) \otimes (B \multimap \!\circ\, A) \vdash B \otimes (B \multimap \!\circ\, A)$. Here we have a contract offering the resource B under the condition that A becomes available, in the presence of a contract which produces A from B. In this case the first contract is "enabled", allowing B to interact with the process $B \multimap \!\circ\, A$. Note however that we do not obtain $A \otimes B$, because if the implication $B \multimap \!\circ\, A$ is applied, it consumes B.
8. $A \multimap\!\!\!\circ\, B \vdash A \multimap \!\circ\, B$. This states that linear contractual implication entails linear implication (coherently with the property $A \twoheadrightarrow B \vdash A \to B$ in PCL).
9. $(A \multimap\!\!\!\circ\, B) \otimes A \vdash A \otimes B$. This stresses a difference between $\multimap \!\circ$ and $\multimap\!\!\!\circ$: the latter *does not consume* its antecedent.
10. $(A \multimap\!\!\!\circ\, B) \otimes (B \multimap\!\!\!\circ\, C) \vdash A \multimap\!\!\!\circ\, C$. This states transitivity of $\multimap\!\!\!\circ$.

Encoding of PCL. In Fig. 2 we show an encoding of PCL into PCLLW, extending the one in [7]. Theorem 1 shows the mapping correct and complete.

Theorem 1. *$\Gamma \vdash A$ is derivable in* PCL *iff $!\Gamma^* \vdash A^*$ in* PCLLW*.*

Proof. For $\Rightarrow$, first we use the equivalence between the sequent calculus and the natural deduction system for PCL (shown in [1]) to get from a sequent calculus proof of $\Gamma \vdash A$ a natural deduction proof of A from Γ; then using the translation of the rules in Fig. 3, together with the one given by Girard from natural deduction to intuitionistic linear sequent calculus [7], by induction on the height of the proof we get a proof of $!\Gamma^* \vdash A^*$. The proof of $\Leftarrow$ is straightforward.

Cut elimination. As for PCL, the logic PCLLW enjoys cut elimination. The proof follows the one for ILL provided in [5]. The key cases concerning the connective $\multimap\!\!\!\circ$ are shown in the Appendix. This result is not completely straightforward — e.g. it cannot be deduced using the technique of [6] — because rule PrePost makes the sequent calculus of PCLLW *non-simple* according to [6].

Theorem 2 (Cut elimination). *If $\Gamma \vdash A$ is provable in* PCLLW*, then a cut-free proof of $\Gamma \vdash A$ exists.*

3 Phase structures and decidability

In this section we combine some results of Ciabattoni, Okada and Terui [6,12] on models of linear logic called *phase structures*, in order to define a model and prove decidability of a fragment of PCLLW, namely PCLLW without exponentials and PrePost rules. This restriction is due to the fact that the results of [6] do not extend to rules with the shape of PrePost and to the ones concerning exponentials.

Phase structures. Let $\mathbf{M} = (\mathcal{M}, \bullet, 1)$ be a commutative monoid . For any $P, Q \subseteq \mathcal{M}$, we define:

$$P \multimap Q = \{y \mid \forall x \in P, (x \bullet y \in Q)\}$$

Definition 1 (Affine Phase structure). *A* phase structure *is a pair* $(\mathbf{M}, \mathcal{D}_{\mathbf{M}})$*, where* $\mathcal{D}_{\mathbf{M}}$ *is a subset of* $\wp(\mathcal{M})$*, called the set of* facts*, closed under arbitrary intersections, and such that for all* $A, B \in \mathcal{D}_{\mathbf{M}}$*, the set* $A \multimap B$ *belongs to* $\mathcal{D}_{\mathbf{M}}$*.*

Given a commutative monoid $\mathbf{M}$*, an ideal of* $\mathbf{M}$ *is a subset* A *of* $\mathbf{M}$ *such that* $A \bullet \mathbf{M} = A$ *(where* $P \bullet Q = \{x \bullet y \mid x \in P, y \in Q\}$*). An* affine phase structure *is a phase structure where each fact is an ideal.*

Valuations. Given a connective $A \star B$ of PCLLW, we associate with it two operations on the facts of an affine phase structures, $A^\bullet \star_l B^\bullet$, $A^\bullet \star_r B^\bullet$ (where $A^\bullet, B^\bullet$ are facts), called respectively its *left* and *right* interpretation, defined on the basis of the left and right introduction rules of the connective. See [6] for the actual definitions.

Definition 2. *Given an affine phase structure* $(\mathbf{M}, \mathcal{D}_{\mathbf{M}})$*, a* valuation *on* $(\mathbf{M}, \mathcal{D}_{\mathbf{M}})$ *is a map* f *from the set of formulas of* PCLLW *to the elements of* $\mathcal{D}_{\mathbf{M}}$*, such that for each formula* $A \star B$*:*

$$(f(A) \star_r f(B)) \subseteq f(A \star B) \subseteq (f(A) \star_l f(B))$$

A valuation f is straightforwardly extended to sequences $\Gamma = A_1, \ldots, A_n$. A sequent $\Gamma \vdash A$ is *valid* iff $f(\Gamma) \subseteq f(A)$ (if Γ is empty then we let $f(\Gamma) = 1$).

Definition 3 (Model). *An* affine phase model *of* PCLLW *is a tuple* $\langle \mathbf{M}, D, f \rangle$ *such that* $(\mathbf{M}, D)$ *is an affine phase structure, and* f *is a valuation on* $(\mathbf{M}, D)$*.*

An affine phase model $\langle \mathbf{M}, D, f \rangle$ *satisfies* a fomula A of PCLLW iff the sequent $\vdash A$ is valid under f; similarly, a formula A of PCLLW is *satisfiable* if there exists an affine phase model which satisfies A.

Theorem 3 (Soundness). *For all affine phase models* $\langle \mathbf{M}, \mathcal{D}_{\mathbf{M}}, f \rangle$*, if* $\Gamma \vdash A$ *is derivable in* PCLLW*, then* $\Gamma \vdash A$ *is valid under* f*.*

Proof. Similar to the one in [6].

To prove completeness, we first have to define a syntactic model of PCLLW in affine phase structures. Let $\mathcal{F}$ be the set of formulas of PCLLW. Let us consider the free monoid $\mathcal{F}^*$ generated by $\mathcal{F}$: we identify a sequence Γ with an element of $\mathcal{F}^*$. By $[\![\Gamma \vdash C]\!]$ we denote the set $\{\Sigma \mid \Sigma, \Gamma \vdash C \text{ is derivable without cut in } \mathcal{L}\}$. By $[\![C]\!]$ we mean $[\![\vdash C]\!]$. We define the *syntactic affine phase structure* of PCLLW taking as monoid the free monoid $\mathcal{F}^*$, and as set of facts the set $D_{\mathcal{F}^*}$ comprising $\bigcap_{i\in\Lambda}[\![\Gamma_i \vdash C_i]\!]$ for any index set Λ. Then we define, by induction on the complexity of a formula of PCLLW, a specific valuation f_0 (see [6] for details).

Theorem 4 (Completeness). *Let $\langle \mathcal{F}^*, D_{\mathcal{F}^*}, f_0\rangle$ be a (syntactic) affine phase model of* PCLLW*. If $\Gamma \vdash C$ is valid under f_0, then $\Gamma \vdash C$ is derivable.*

Proof. Similar to the one in [6].

Decidability. Given an affine phase model $\langle \mathbf{M}, D, f\rangle$, we consider the congruence relation $\equiv$ on the elements of $\mathbf{M}$ defined by $x \equiv y$ *iff* $C\{x\} = C\{y\}$. For an affine phase model, we define its quotient model $\langle \mathbf{M}/\equiv, D', f'\rangle$ where $\mathbf{M}/_\equiv$ is the quotient of $\mathbf{M}$ w.r.t. $\equiv$, $D' = \{F/_\equiv \mid F \in D\}$, and $f'(A) = (f(A))/_\equiv$.

As in [8], we can observe that there is a natural bijection between D and D' (because the facts of D are already closed by $\equiv$), so it is easy to conclude that $\mathbf{M}/_\equiv$ satisfies the same formulas as $\mathbf{M}$. Following [12], we see that the $\mathbf{M}/_\equiv$ is finite whenever the set of facts D is finite.

One can then prove the finite model property of PCLLW by exhibiting a syntactical model where the set of facts is finite. Indeed, it suffices quotienting the syntactic model using $\equiv$. Formally, given a formula A of PCLLW, we define PCLLW(A) as PCLLW restricted to the subformulas of A, and PCLLW$^\bullet(A)$ as the syntactical model induced by PCLLW(A). The following lemma is adapted from [12].

Lemma 1. *The set of facts of* PCLLW$^\bullet(A)$ *is finite. Therefore,* PCLLW$^\bullet(A)/_\equiv$ *is a finite model.*

Theorem 5 (Finite Model Property). *For all formulas A of* PCLLW*, A is provable iff it is satisfied by every finite affine phase model.*

Theorem 6. PCLLW *is decidable.*

Proof. Obviously the set of theorems of PCLLW is recursively enumerable. The set of non-theorems of PCLLW is recursively enumerable too, by the finite model property. Moreover, the property of being a finite affine phase model is decidable, since being a finite affine phase structure and being a valuation over a finite affine phase structure are both decidable properties (the domain is finite so all quantifications are finite). Then we can conclude that PCLLW is decidable.

4 Conclusions

As pointed out in §2, contractual implication $A \multimap B$ should be interpreted as "B can be provided when A is eventually available". Standing by this interpretation, one should expect that the presence of some non-determinism involving

the availability of the resources would also imply non-determinism on the consequences of the contracts. That is, we should have that (and indeed we have):

$$(A\&B) \otimes (A \multimap A') \otimes (B \multimap B') \vdash A'\&B'$$

because, having to choose one resource among A, B, only one of the two contracts should be used. Actually, a stronger property holds with the calculus in Fig. 1:

$$(A\&B) \otimes (A \multimap A') \otimes (B \multimap B') \vdash A' \otimes B'$$

That is, both contracts are enabled at the same time, even though one has to choose between the two resources A, B. So, to enable a contract it does not matter only the fact that eventually a resource *must* become available, but even that it *could*. Refining PCLLW in order to eliminate this undesired feature is an actual work in progress.

An alternative model for dealing with resources and debts is *cancellative linear logic* [9]. It corresponds to *financial games* in Petri nets, where moves allow for creating *debts*, and for annihilating debts with credits. The exact relations with PCL (and with Lending Petri nets [2]) have to be investigated. Some differences are however apparent: for instance, in [9] one can always create new debts (for any resource), while in PCLLW a resource B can be taken on credit only by consuming some $A \multimap B$, and only under the guarantee that the resource A will eventually be available.

References

1. M. Bartoletti, T. Cimoli, P. D. Giamberardino, and R. Zunino. Contract agreements via logic. In *Proc. ICE*, 2013.
2. M. Bartoletti, T. Cimoli, and G. M. Pinna. Lending Petri nets and contracts. In *Proc. FSEN*, 2013. To appear.
3. M. Bartoletti, T. Cimoli, and R. Zunino. A theory of agreements and protection. In *Proc. POST*, volume 7796 of *LNCS*. Springer, 2013.
4. M. Bartoletti and R. Zunino. A calculus of contracting processes. In *LICS*, 2010.
5. G. Bierman. *On Intuitionistic Linear Logic*. PhD thesis, Univ. of Cambridge, 1993.
6. A. Ciabattoni and K. Terui. Towards a semantic characterization of cut-elimination. *Studia Logica*, 82(1):95–119, 2006.
7. J.-Y. Girard. Linear logic. *Theor. Comput. Sci.*, 50:1–102, 1987.
8. Y. Lafont. The finite model property for various fragments of linear logic. *J. Symb. Log.*, 62(4):1202–1208, 1997.
9. N. Martí-Oliet and J. Meseguer. An algebraic axiomatization of linear logic models. In *Topology and category theory in computer science*. Oxford Univ. Press, 1991.
10. N. Martí-Oliet and J. Meseguer. From petri nets to linear logic. *Mathematical Structures in Computer Science*, 1(1):69–101, 1991.
11. M. Nielsen, G. D. Plotkin, and G. Winskel. Petri nets, event structures and domains. In *Semantics of Concurrent Computation*, pages 266–284, 1979.
12. M. Okada and K. Terui. The finite model property for various fragments of intuitionistic linear logic. *J. Symb. Log.*, 64(2):790–802, 1999.

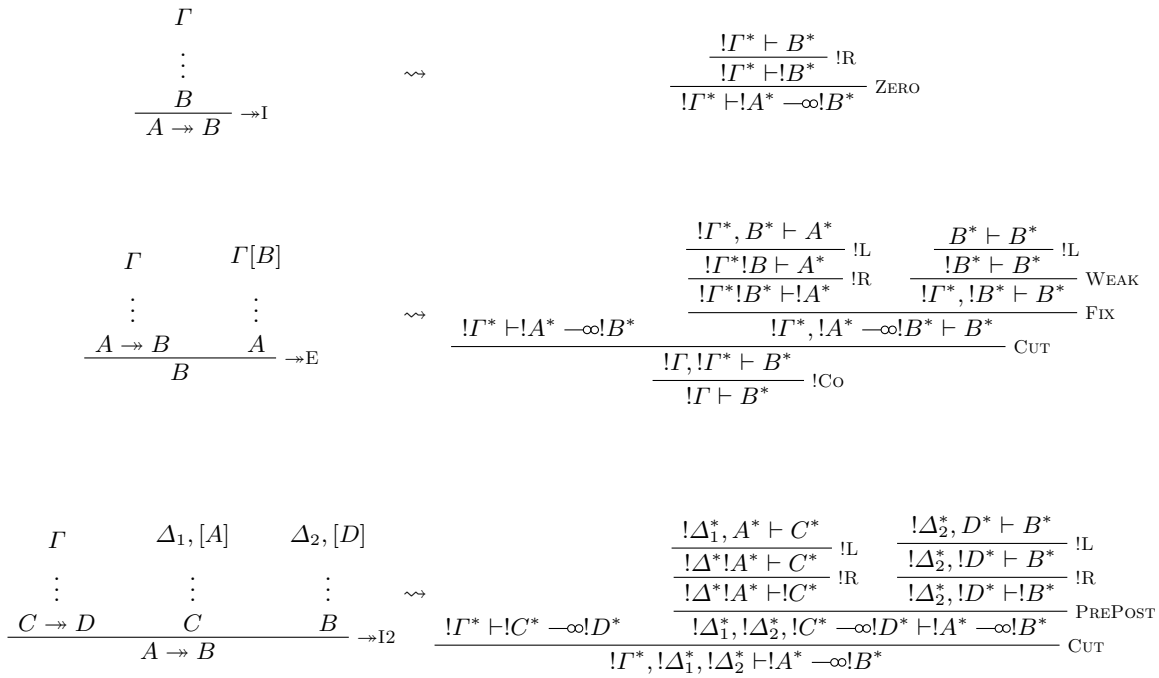

Fig. 3. Translation of PCL proofs into PCLLW proofs.

Proof of cut elimination (cases for $\multimap$)

– (Zero, Fix)

$$\dfrac{\dfrac{\dfrac{\overset{\pi_1}{\Gamma \vdash B}}{\Gamma \vdash A \multimap B}\,\textsc{Zero} \qquad \dfrac{\overset{\pi_2}{\Delta, B \vdash A} \qquad \overset{\pi_3}{\Delta, B \vdash C}}{\Delta, A \multimap B \vdash C}\,\textsc{Fix}}{\Gamma, \Delta \vdash C}\,\textsc{Cut}$$

The cut above is reduced as follows:

$$\dfrac{\overset{\pi_1}{\Gamma \vdash B} \qquad \overset{\pi_3}{\Delta, B \vdash C}}{\Gamma, \Delta, \vdash C}\,\textsc{Cut}$$

– (Zero, PrePost)

$$\dfrac{\dfrac{\dfrac{\overset{\pi_1}{\Gamma \vdash B}}{\Gamma \vdash A \multimap B}\,\textsc{Zero} \qquad \dfrac{\overset{\pi_2}{\Delta, C \vdash A} \qquad \overset{\pi_3}{\Theta, B \vdash D}}{\Delta, \Theta, A \multimap B \vdash C \multimap D}\,\textsc{PrePost}}{\Gamma, \Delta, \Theta \vdash C \multimap D}\,\textsc{Cut}$$

The cut above is reduced as follows:

$$\dfrac{\dfrac{\dfrac{\overset{\pi_1}{\Gamma \vdash B} \qquad \overset{\pi_3}{\Theta, B \vdash D}}{\Gamma, \Theta, \vdash D}\,\textsc{Cut}}{\Gamma, \Theta \vdash C \multimap D}\,\textsc{Zero}}{\Gamma, \Theta, \Delta \vdash C \multimap D}\,\textsc{Weak}$$

– (PrePost, PrePost)

$$\dfrac{\dfrac{\dfrac{\overset{\pi_1}{\Gamma, A \vdash E} \qquad \overset{\pi_2}{\Lambda, F \vdash B}}{\Gamma, \Lambda, E \multimap F \vdash A \multimap B}\,\textsc{PrePost} \qquad \dfrac{\overset{\pi_3}{\Delta, C \vdash A} \qquad \overset{\pi_4}{\Theta, B \vdash D}}{\Delta, \Theta, A \multimap B \vdash C \multimap D}\,\textsc{PrePost}}{\Gamma, \Delta, \Theta, E \multimap F \vdash C \multimap D}\,\textsc{Cut}$$

The cut above is reduced as follows:

$$\dfrac{\dfrac{\overset{\pi_3}{\Delta, C \vdash A} \qquad \overset{\pi_1}{\Gamma, A \vdash E}}{\Gamma, \Delta, C \vdash E}\,\textsc{Cut} \qquad \dfrac{\overset{\pi_2}{\Lambda, F \vdash B} \qquad \overset{\pi_4}{\Theta, B \vdash D}}{\Lambda, \Theta, F \vdash D}\,\textsc{Cut}}{\Gamma, \Delta, \Lambda, \Theta, E \multimap F \vdash C \multimap D}\,\textsc{PrePost}$$

– (Prepost, Fix)

$$\dfrac{\dfrac{\dfrac{\overset{\pi_1}{\Gamma, A \vdash C} \qquad \overset{\pi_2}{\Lambda, D \vdash B}}{\Gamma, \Lambda, C \multimap D \vdash A \multimap B}\,\textsc{PrePost} \qquad \dfrac{\overset{\pi_3}{\Delta, B \vdash A} \qquad \overset{\pi_4}{\Delta, B \vdash E}}{\Delta, A \multimap B \vdash E}\,\textsc{Fix}}{\Gamma, \Lambda, \Delta, C \multimap D \vdash E}\,\textsc{Cut}$$

The cut above is reduced as follows:

$$\dfrac{\dfrac{\overset{\pi_2}{\Lambda, D \vdash B} \qquad \dfrac{\overset{\pi_3}{\Delta, B \vdash A} \qquad \overset{\pi_1}{\Gamma, A \vdash C}}{\Gamma, \Delta, B \vdash C}\,\textsc{Cut}}{\Lambda, \Gamma, \Delta, D \vdash C}\,\textsc{Cut} \qquad \dfrac{\dfrac{\overset{\pi_2}{\Lambda, D \vdash B} \qquad \overset{\pi_4}{\Delta, B \vdash E}}{\Lambda, \Delta, D \vdash E}\,\textsc{Cut}}{\Gamma, \Lambda, \Delta, D \vdash E}\,\textsc{Weak}}{\Lambda, \Delta, C \multimap D \vdash E}\,\textsc{Fix}$$