Semantics of a Relational λ-Calculus[⋆] (Extended Version)

Pablo Barenbaum[1], Federico Lochbaum[2], and Mariana Milicich[3]

[1] Universidad de Buenos Aires and Universidad Nacional de Quilmes, Argentina
pbarenbaum@dc.uba.ar
[2] Universidad Nacional de Quilmes, Argentina
federico.lochbaum@gmail.com
[3] Universidad de Buenos Aires, Argentina
milicichmariana@gmail.com

Abstract. We extend the λ-calculus with constructs suitable for relational and functional–logic programming: non-deterministic choice, fresh variable introduction, and unification of expressions. In order to be able to unify λ-expressions and still obtain a confluent theory, we depart from related approaches, such as λProlog, in that we do not attempt to solve higher-order unification. Instead, abstractions are decorated with a *location*, which intuitively may be understood as its memory address, and we impose a simple *coherence* invariant: abstractions in the same location must be equal. This allows us to formulate a *confluent* small-step operational semantics which only performs first-order unification and does not require *strong* evaluation (below lambdas). We study a simply typed version of the system. Moreover, a denotational semantics for the calculus is proposed and reduction is shown to be sound with respect to the denotational semantics.

Keywords: Lambda Calculus · Semantics · Relational Programming · Functional Programming · Logic Programming · Confluence

1 Introduction

Declarative programming is defined by the ideal that programs should resemble abstract specifications rather than concrete implementations. One of the most significant declarative paradigms is *functional programming*, represented by languages such as Haskell. Some of its salient features are the presence of first-class functions and inductive datatypes manipulated through pattern matching. The fact that the underlying model of computation—the λ-calculus—is *confluent* allows one to reason equationally about the behavior of functional programs.

Another declarative paradigm is *logic programming*, represented by languages such as Prolog. Some of its salient features are the ability to define relations

⋆ Work partially supported by project grants ECOS Sud A17C01, PUNQ 1346/17, and UBACyT 20020170100086BA.

rather than functions, and the presence of existentially quantified *symbolic variables* that become instantiated upon querying. This sometimes allows to use n-ary relations with various patterns of instantiation, *e.g.* `add(3, 2, X)` computes `X := 3 + 2` whereas `add(X, 2, 5)` computes `X := 5 - 2`. The underlying model of computation is based on *unification* and refutation search with *backtracking*.

The idea to marry functional and logic programming has been around for a long time, and there have been many attempts to combine their features gracefully. For example, λProlog (Miller and Nadathur [24,22]) takes Prolog as a starting point, generalizing first-order terms to λ-*terms* and the mechanism of first-order unification to that of *higher-order unification*. Another example is Curry (Hanus et al. [13,12]) in which programs are defined by equations, quite like in functional languages, but evaluation is non-deterministic and evaluation is based on *narrowing*, *i.e.* variables become instantiated in such a way as to fulfill the constraints imposed by equations.

One of the interests of combining functional and logic programming is the fact that the increased expressivity aids declarative programming. For instance, if one writes a parser as a function `parser : String` $\longrightarrow$ `AST`, it should be possible, under the right conditions, to *invert* this function to obtain a pretty-printer `pprint : AST` $\longrightarrow$ `String`:

$$\texttt{pprint ast = } \nu \texttt{ source . ((ast } \overset{\bullet}{=} \texttt{ parse source) ; source)}$$

In this hypothetical functional–logic language, intuitively speaking, the expression $(\nu x.\, t)$ creates a fresh symbolic variable x and proceeds to evaluate t; the expression $(t \overset{\bullet}{=} s)$ unifies t with s; and the expression $(t; s)$ returns the result of evaluating s whenever the evaluation of t succeeds.

Given that unification is a generalization of pattern matching, a functional language with explicit unification should in some sense generalize λ-*calculi with patterns*, such as the Pure Pattern Calculus [16]. For example, by relying on unification one may build *dynamic* or *functional patterns*, *i.e.* patterns that include operations other than constructors. A typical instance is the following function `last : [a]` $\longrightarrow$ `a`, which returns the last element of a non-empty cons-list:

```
last (xs ++ [x]) = x
```

Note that `++` is not a constructor. This definition may be desugared similarly as for the `pprint` example above:

$$\texttt{last lst = } \nu \texttt{ xs . } \nu \texttt{ x. (lst } \overset{\bullet}{=} \texttt{ (xs ++ [x])); x}$$

Still another interest comes from the point of view of the *proposition-as-types correspondence*. Terms of a λ-calculus with types can be understood as encoding proofs, so for instance the identity function $(\lambda x : A.\, x)$ may be understood as a proof of the implication $A \to A$. From this point of view, a functional–logic program may be understood as a *tactic*, as can be found in proof assistants such as Isabelle or Coq (see *e.g.* [31]). A term of type A should then be understood as a non-deterministic procedure which attempts to find a proof of A and it may leave holes in the proof or even fail. For instance if P is a property on natural numbers, p is a proof of $P(0)$ and q is a proof of $P(1)$, then $\lambda n.\,((n \stackrel{\bullet}{=} 0); p) \boxplus ((n \stackrel{\bullet}{=} 1); q)$ is a tactic that given a natural number n produces a proof of $P(n)$ whenever $n \in \{0, 1\}$, and otherwise it fails. Here $(t \boxplus s)$ denotes the *non-deterministic alternative* between t and s.

The goal of this paper is to **provide a foundation for functional–logic programming** by **extending the λ-calculus with relational constructs**. Recall that the syntactic elements of the λ-calculus are λ-terms $(t, s, \ldots)$, which inductively may be *variables* $(x, y, \ldots)$, *abstractions* $(\lambda x.\, t)$, and *applications* $(t\, s)$. Relational programming may be understood as the purest form of logic programming, chiefly represented by the family of miniKanren languages (Byrd et al. [10,7]). The core syntactic elements of miniKanren, following for instance Rozplokhas et al. [27] are goals $(G, G', \ldots)$ which are inductively given by: *relation symbol invocations*, of the form $R(T_1, \ldots, T_n)$, where R is a relation symbol and $T_1, \ldots, T_n$ are terms of a first-order language, *unification* of first-order terms $(T_1 \stackrel{\bullet}{=} T_2)$, *conjunction* of goals $(G; G')$, *disjunction* of goals $(G \boxplus G')$, and *fresh variable introduction* $(\nu x.\, G)$.

Our starting point is a "chimeric creature"—a functional–logic language resulting from cross breeding the λ-calculus and miniKanren, given by the following abstract syntax:

$$
\begin{array}{rlll|lll}
t, s ::= & x & \text{variable} & & \mathbf{c} & \text{constructor} \\
\mid & \lambda x.\, t & \text{abstraction} & & t\, s & \text{application} \\
\mid & \nu x.\, t & \text{fresh variable introduction} & & t \boxplus s & \text{non-deterministic choice} \\
\mid & t; s & \text{guarded expression} & & t \stackrel{\bullet}{=} s & \text{unification}
\end{array}
$$

Its informal semantics has been described above. Variables $(x, y, \ldots)$ may be instantiated by unification, while constructors $(\mathbf{c}, \mathbf{d}, \ldots)$ are constants. For example, if $\texttt{coin} \stackrel{\text{def}}{=} (\mathbf{true} \boxplus \mathbf{false})$ is a non-deterministic boolean with two possible values and $\texttt{not} \stackrel{\text{def}}{=} \lambda x.\,((x \stackrel{\bullet}{=} \mathbf{true}); \mathbf{false}) \boxplus ((x \stackrel{\bullet}{=} \mathbf{false}); \mathbf{true})$ is the usual boolean negation, the following non-deterministic computation:

$$(\lambda x.\, \lambda y.\, (x \stackrel{\bullet}{=} \texttt{not}\, y); \mathbf{pair}\ x\, y)\, \texttt{coin}\, \texttt{coin}$$

should have two results, namely $\mathbf{pair\,true\,false}$ and $\mathbf{pair\,false\,true}$.

Structure of this paper. In Section 2, we discuss some technical difficulties that arise as one intends to provide a formal operational semantics for the informal functional–logic calculus sketched above. In Section 3, we refine this rough proposal into a calculus we call the $\lambda^{\mathtt{U}}$-*calculus*, with a formal small-step operational semantics (Def. 3.1). To do so, we distinguish *terms*, which represent a single choice, from *programs*, which represent a non-deterministic alternative between zero or more terms. Moreover, we adapt the standard first-order unification algorithm to our setting by imposing a *coherence* invariant on programs. In Section 4, we study the operational properties of the $\lambda^{\mathtt{U}}$-calculus: we provide an inductive characterization of the set of normal forms (Prop. 4.1), and we prove that it is confluent (Thm. 4.4) (up to a notion of structural equivalence). In Section 5, we propose a straightforward system of simple types and we show that it enjoys subject reduction (Prop. 5.2). In Section 6, we define a (naive) denotational semantics, and we show that the operational semantics is sound (although it is not complete) with respect to this denotational semantics (Thm. 6.2). In Section 7, we conclude and we lay out avenues of further research.

Note. Most proofs have been left out from the body of the paper. Detailed proofs that can be found in the technical appendix have been marked with ♣.

2 Technical Challenges

This section is devoted to discussing technical stumbling blocks that we encountered as we attempted to define an operational semantics for the functional–logic calculus incorporating all the constructs mentioned in the introduction. These technical issues motivate the design decisions behind the actual $\lambda^{\mathtt{U}}$-calculus defined in Sec. 3. The discussion in this section is thus **informal**. Examples are carried out with their hypothetical or intended semantics.

Locality of symbolic variables. The following program introduces a fresh variable x and then there are two alternatives: either x unifies with $\mathbf{c}$ and the result is x, or x unifies with $\mathbf{d}$ and the result is x. The expected reduction semantics is the following. The constant $\mathbf{ok}$ is the result obtained after a successful unification:

$$\begin{aligned}
\nu x.\ \Big(((x \overset{\bullet}{=} \mathbf{c}); x) \boxplus ((x \overset{\bullet}{=} \mathbf{d}); x)\Big) &\to ((x \overset{\bullet}{=} \mathbf{c}); x) \boxplus ((x \overset{\bullet}{=} \mathbf{d}); x) \text{ with } x \text{ fresh} \\
&\to (\mathbf{ok}; \mathbf{c}) \boxplus ((x \overset{\bullet}{=} \mathbf{d}); x) \qquad (\bigstar) \\
&\to (\mathbf{ok}; \mathbf{c}) \boxplus (\mathbf{ok}; \mathbf{d}) \\
&\twoheadrightarrow \mathbf{c} \boxplus \mathbf{d}
\end{aligned}$$

Note that in the step marked with ($\bigstar$), the variable x becomes instantiated to $\mathbf{c}$, but *only to the left of the choice operator* ($\boxplus$). This suggests that programs should consist of different *threads* fenced by choice operators. Symbolic variables should be local to each thread.

Need of commutative conversions. Redexes may be *blocked* by the choice operator—for example in the application $((t \boxplus \lambda x.\, s)\, u)$, there is a potential β-redex $((\lambda x.\, s)\, u)$ which is blocked. This suggests that *commutative conversions* that distribute the choice operator should be incorporated, allowing for instance a reduction step $(t \boxplus \lambda x.\, s)\, u \to t\, u \boxplus (\lambda x.\, s)\, u$. In our proposal, we force in the syntax that a program is always written, canonically, in the form $t_1 \boxplus \ldots \boxplus t_n$, where each t_i is a deterministic program (*i.e.* choice operators may only appear inside lambdas). This avoids the need to introduce commutative rules.

Confluence only holds up to associativity and commutativity. There are two ways to distribute the choice operators in the following example:

$$\begin{array}{ccccc} t_1(s_1 \boxplus s_2) \boxplus t_2(s_1 \boxplus s_2) & \longleftarrow & (t_1 \boxplus t_2)\,(s_1 \boxplus s_2) & \longrightarrow & (t_1 \boxplus t_2)\,s_1 \boxplus (t_1 \boxplus t_2)\,s_2 \\ \downarrow & & & & \downarrow \\ (t_1\,s_1 \boxplus t_1\,s_2) \boxplus (t_2\,s_1 \boxplus t_2\,s_2) & \cdots\cdots & \equiv & \cdots\cdots & (t_1\,s_1 \boxplus t_2\,s_1) \boxplus (t_1\,s_2 \boxplus t_2\,s_2) \end{array}$$

The resulting programs cannot be equated unless one works up to an equivalence relation that takes into account the associativity and commutativity of the choice operator. As we mentioned, the $\lambda^{\mathtt{U}}$-calculus works with programs in canonical form $t_1 \boxplus \ldots \boxplus t_n$, so there is no need to work modulo associativity. However, we do need commutativity. As a matter of fact, we shall define a notion of *structural equivalence* ($\equiv$) between programs, allowing the arbitrary reordering of threads. This relation will be shown to be well-behaved, namely, a *strong bisimulation* with respect to the reduction relation, *cf.* Lem. 3.3.

Non-deterministic choice is an effect. Consider the program $(\lambda x.\, x\, x)(\mathbf{c} \boxplus \mathbf{d})$, which chooses between $\mathbf{c}$ and $\mathbf{d}$ and then it produces two copies of the chosen value. Its expected reduction semantics is:

$$(\lambda x.\, x\, x)(\mathbf{c} \boxplus \mathbf{d}) \to (\lambda x.\, x\, x)\mathbf{c} \boxplus (\lambda x.\, x\, x)\mathbf{d} \twoheadrightarrow \mathbf{c}\,\mathbf{c} \boxplus \mathbf{d}\,\mathbf{d}$$

This means that the first step in the following reduction, which produces two copies of $(\mathbf{c} \boxplus \mathbf{d})$ cannot be allowed, as it would break confluence:

$$(\lambda x.\, x\, x)(\mathbf{c} \boxplus \mathbf{d}) \not\to (\mathbf{c} \boxplus \mathbf{d})\,(\mathbf{c} \boxplus \mathbf{d}) \twoheadrightarrow \mathbf{c}\,\mathbf{c} \boxplus \mathbf{c}\,\mathbf{d} \boxplus \mathbf{d}\,\mathbf{c} \boxplus \mathbf{d}\,\mathbf{d}$$

The deeper reason is that non-deterministic choice is a side-effect rather than a value. Our design decision, consistent with this remark, is to follow a **call-by-value** discipline. Another consequence of this remark is that the choice operator should not commute with abstraction, given that $\lambda x.\,(t \boxplus s)$ and $(\lambda x.\, t) \boxplus (\lambda x.\, s)$ are not observationally equivalent. In particular, $\lambda x.\,(t \boxplus s)$ is a value, which may be *copied*, while $(\lambda x.\, t) \boxplus (\lambda x.\, s)$ is not a value. On the other hand, if W is any *weak* context, *i.e.* a term with a hole which does *not* lie below a binder, and we write $\mathsf{W}\langle t \rangle$ for the result of plugging a term t into the hole of W, then $\mathsf{W}\langle t \boxplus s \rangle = \mathsf{W}\langle t \rangle \boxplus \mathsf{W}\langle s \rangle$ should hold.

Evaluation should be weak. Consider the term $F \stackrel{\text{def}}{=} \lambda y.\,((y \stackrel{\bullet}{=} x); x)$. Intuitively, it unifies its argument with a (global) symbolic variable x and then returns x. This poses two problems. First, when x becomes instantiated to y, it may be outside the scope of the abstraction binding y, for instance, the step $F\, x = (\lambda y.\,((y \stackrel{\bullet}{=} x); x))\, x \to (\lambda y.\,(\mathbf{ok}; y))\, y$ produces a meaningless free occurrence of y. Second, consider the following example in which two copies of F are used with different arguments. If we do **not** allow evaluation under lambdas, this example fails due to a unification clash, *i.e.* it produces no outputs:

$$\begin{aligned} (\lambda f.\,(f\,\mathbf{c})\,(f\,\mathbf{d}))\, F &\to (F\,\mathbf{c})\,(F\,\mathbf{d}) \\ &\to ((\mathbf{c} \stackrel{\bullet}{=} x); x)\,((\mathbf{d} \stackrel{\bullet}{=} x); x) \\ &\to (\mathbf{ok}; \mathbf{c})\,((\mathbf{d} \stackrel{\bullet}{=} \mathbf{c}); \mathbf{c}) \qquad (\bigstar) \\ &\to \mathtt{fail} \end{aligned}$$

Note that in the step marked with ($\bigstar$), the symbolic variable x has become instantiated to $\mathbf{c}$, leaving us with the unification goal $\mathbf{d} \overset{\bullet}{=} \mathbf{c}$ which fails. On the other hand, if we were to allow reduction under lambdas, given that there are no other occurrences of x anywhere in the term, in one step F becomes $\lambda y. (\mathbf{ok}; y)$, which then behaves as the identity:

$$\begin{aligned}(\lambda f. (f\,\mathbf{c})\,(f\,\mathbf{d}))\,F &\not\to (\lambda f. (f\,\mathbf{c})\,(f\,\mathbf{d}))\,(\lambda y. \mathbf{ok}; y)\\ &\to ((\lambda y. \mathbf{ok}; y)\,\mathbf{c})\,((\lambda y. \mathbf{ok}; y)\,\mathbf{d})\\ &\twoheadrightarrow \mathbf{c}\,\mathbf{d}\end{aligned}$$

Thus allowing reduction below abstractions in this example would break confluence. This suggests that evaluation should be **weak**, *i.e.* it should not proceed below binders.

Avoiding higher-order unification. The calculus proposed in this paper rests on the design choice to *avoid* attempting to solve higher-order unification problems. Higher-order unification problems can be expressed in the syntax: for example in $(f\mathbf{c} \overset{\bullet}{=} \mathbf{c})$ the variable f represents an unknown value which should fulfill the given constraint. From our point of view, however, this program is stuck and its evaluation cannot proceed—it is a normal form. However, note that we **do** want to allow *pattern matching* against functions; for example the following should succeed, instantiating f to the identity:

$$(\mathbf{c}\,f \overset{\bullet}{=} \mathbf{c}(\lambda x. x)); (f \overset{\bullet}{=} f) \to (\lambda x. x) \overset{\bullet}{=} (\lambda x. x) \to \mathbf{ok}$$

The decision to sidestep higher-order unification is a debatable one, as it severely restricts the expressivity of the language. But there are various reasons to explore alternatives. First, higher-order unification is undecidable [14], and even second order unification is known to be undecidable [18]. Huet's semi-decision procedure [15] does find a solution should it exist, but even then higher-order unification problems do not necessarily possess *most general unifiers* [11], which turns confluence hopeless[4]. Second, there are decidable restrictions of higher-order unification which do have most general unifiers, such as *higher-order pattern unification* [21] used in λProlog, and *nominal unification* [32] used in αProlog. But these mechanisms require *strong* evaluation, *i.e.* evaluation below abstractions, departing from the traditional execution model of eager applicative languages such as in the Lisp and ML families, in which closures are opaque values whose bodies cannot be examined. Moreover, they are formulated in a necessarily typed setting.

The calculus studied in this paper relies on a standard first-order unification algorithm, with the only exception that abstractions are deemed to be equal if and only if they have the same "identity". Intuitively speaking, this means that they are stored in the same memory location, *i.e.* they are represented by the same pointer. This is compatible with the usual implementation techniques

[4] Key in our proof of confluence is the fact that if σ and σ' are most general unifiers for unification problems G and G' respectively, then the most general unifier for $(\mathsf{G} \cup \mathsf{G}')$ is an instance of both σ and σ'. See Ex. 4.5.

of eager applicative languages, so it should allow to use standard compilation techniques for λ-abstractions. Also note that the operational semantics does not require to work with typed terms—in fact the system presented in Sec. 3 is untyped, even though we study a typed system in Sec. 5.

3 The $\boldsymbol{\lambda}^{\mathtt{U}}$-Calculus — Operational Semantics

In this section we describe the operational semantics of our proposed calculus, including its syntax, reduction rules (Def. 3.1), an invariant (*coherence*) which is preserved by reduction (Lem. 3.2), and a notion of structural equivalence which is a *strong bisimulation* with respect to reduction (Lem. 3.3).

Syntax of terms and programs. Suppose given denumerably infinite sets of *variables* $\mathsf{Var} = \{x, y, z, \dots\}$, *constructors* $\mathsf{Con} = \{\mathbf{c}, \mathbf{d}, \mathbf{e}, \dots\}$, and *locations* $\mathsf{Loc} = \{\ell, \ell', \ell'', \dots\}$. We assume that there is a distinguished constructor **ok**. The sets of *terms* $t, s, \dots$ and *programs* $P, Q, \dots$ are defined mutually inductively as follows:

$t ::= x$	variable	$\mid \mathbf{c}$	constructor
$\mid \lambda x. P$	abstraction	$\mid \lambda^{\ell} x. P$	allocated abstraction
$\mid t\, t$	application	$\mid \nu x. t$	fresh variable introduction
$\mid t; t$	guarded expression	$\mid t \overset{\bullet}{=} t$	unification

$P ::= \mathtt{fail}$	empty program
$\mid t \oplus P$	non-deterministic choice

The set of *values* $\mathsf{Val} = \{\mathtt{v}, \mathtt{w}, \dots\}$ is a subset of the set of terms, given by the grammar $\mathtt{v} ::= x \mid \lambda^{\ell} x. P \mid \mathbf{c}\, \mathtt{v}_1 \dots \mathtt{v}_n$. Values of the form $\mathbf{c}\, \mathtt{v}_1 \dots \mathtt{v}_n$ are called *structures*.

Intuitively, an (unallocated) abstraction $\lambda x. P$ represents the static code to create a closure, while $\lambda^{\ell} x. P$ represents the closure created in runtime, stored in the memory cell ℓ. When the abstraction is evaluated, it becomes decorated with a location (*allocated*). We will have a rewriting rule like $\lambda x. P \to \lambda^{\ell} x. P$ where ℓ is fresh.

Notational conventions. We write $\mathsf{C}, \mathsf{C}', \dots$ for *arbitrary contexts*, *i.e.* terms with a single free occurrence of a hole $\Box$. We write $\mathsf{W}, \mathsf{W}', \dots$ for *weak contexts*, which do not enter below abstractions nor fresh variable declarations, *i.e.* $\mathsf{W} ::= \Box \mid \mathsf{W}\, t \mid t\, \mathsf{W} \mid \mathsf{W}; t \mid t; \mathsf{W} \mid \mathsf{W} \overset{\bullet}{=} t \mid t \overset{\bullet}{=} \mathsf{W}$. We write $\oplus_{i=1}^{n} t_i$ or also $t_1 \oplus t_2 \dots \oplus t_n$ to stand for the program $t_1 \oplus (t_2 \oplus \dots (t_n \oplus \mathtt{fail}))$. In particular, if t is a term, sometimes we write t for the *singleton* program $t \oplus \mathtt{fail}$. The set of free variables $\mathsf{fv}(t)$ (resp. $\mathsf{fv}(P)$) of a term (resp. program) is defined as expected, noting that fresh variable declarations $\nu x. t$ and both kinds of abstractions $\lambda x. P$ and $\lambda^{\ell} x. P$ bind the free occurrences of x in the body. Expressions are considered up to α-equivalence, *i.e.* renaming of all bound variables. Given a context or weak context C and a term t, we write $\mathsf{C}\langle t \rangle$ for the (capturing) substitution of $\Box$ by t in C. The set of locations $\mathsf{locs}(t)$ (resp. $\mathsf{fv}(P)$) of a term (resp. program) is defined as the set of all locations ℓ decorating any abstraction on t. We write $t\{\ell := \ell'\}$ for the term that results from replacing all occurrences of the location ℓ in t by ℓ'. The program being evaluated is called the *toplevel program*. The toplevel program is always of the form $t_1 \oplus t_2 \ldots \oplus t_n$, and each of the t_i is called a *thread*.

Operations with programs. We define the operations $P \oplus Q$ and $\mathsf{W}\langle P\rangle$ by induction on the structure of P as follows; note that the notation "$\oplus$" is overloaded both for consing a term onto a program and for concatenating programs:

$$\begin{array}{rclrcl}\texttt{fail} \oplus Q & \overset{\text{def}}{=} & Q & \qquad \mathsf{W}\langle\texttt{fail}\rangle & \overset{\text{def}}{=} & \texttt{fail} \\ (t \oplus P) \oplus Q & \overset{\text{def}}{=} & t \oplus (P \oplus Q) & \qquad \mathsf{W}\langle t \oplus P\rangle & \overset{\text{def}}{=} & \mathsf{W}\langle t\rangle \oplus \mathsf{W}\langle P\rangle\end{array}$$

Substitutions. A *substitution* is a function $\sigma : \mathsf{Var} \to \mathsf{Val}$ with *finite support*, *i.e.* such that the set $\mathrm{supp}(\sigma) \overset{\text{def}}{=} \{x \mid \sigma(x) \neq x\}$ is finite. We write $\{x_1 \mapsto \mathtt{v}_1, \ldots, x_n \mapsto \mathtt{v}_n\}$ for the substitution σ such that $\mathrm{supp}(\sigma) = \{x_1, \ldots, x_n\}$ and $\sigma(x_i) = \mathtt{v}_i$ for all $i \in 1..n$. A *renaming* is a substitution mapping each variable to a variable, *i.e.* a substitution of the form $\{x_1 \mapsto y_1, \ldots, x_n \mapsto y_n\}$.

If $\sigma : \mathsf{Var} \to \mathsf{Val}$ is a substitution and t is a term, t^σ denotes the capture-avoiding substitution of each occurrence of a free variable x in t by $\sigma(x)$. Capture-avoiding substitution of a single variable x by a value $\mathtt{v}$ in a term t is written $t\{x := \mathtt{v}\}$ and defined by $t^{\{x \mapsto \mathtt{v}\}}$. Subsitutions ρ, σ may be *composed* as follows: $(\rho \cdot \sigma)(x) \overset{\text{def}}{=} \rho(x)^\sigma$. Substitutions can also be applied to weak contexts, taking $\Box^\sigma \overset{\text{def}}{=} \Box$. A substitution σ is *idempotent* if $\sigma \cdot \sigma = \sigma$. A substitution σ is *more general* than a substitution ρ, written $\sigma \lesssim \rho$ if there is a substitution τ such that $\rho = \sigma \cdot \tau$.

Unification. We describe how to adapt the standard first-order unification algorithm to our setting, in order to deal with unification of λ-abstractions. As mentioned before, our aim is to solve only first-order unification problems. This means that the unification algorithm should only deal with equations involving terms which are already *values*. Note that unallocated abstractions $(\lambda x.\, P)$ are *not* considered values; abstractions are only values when they are allocated $(\lambda^\ell x.\, P)$. Allocated abstractions are to be considered equal if and only if they are decorated with the same location. Note that terms of the form $x\, t_1 \ldots t_n$ are *not* considered values if $n > 0$, as this would pose a higher-order unification problem, possibly requiring to instantiate x as a function of its arguments.

We expand briefly on why a naive approach to first-order unification would not work. Suppose that we did not have locations and we declared that two abstractions $\lambda x.\, P$ and $\lambda y.\, Q$ are equal whenever their bodies are equal, up to α-renaming (*i.e.* $P\{x := y\} = Q$). The problem is that this notion of equality is not preserved by substitution, for example, the unification problem given by the equation $\lambda x.\, y \overset{\bullet}{=} \lambda x.\, z$ would *fail*, as $y \neq z$. However, the variable y may become instantiated into z, and the equation would become $\lambda x.\, z \overset{\bullet}{=} \lambda x.\, z$, which succeeds. This corresponds to the following critical pair in the calculus, which cannot be closed:

$$\texttt{fail} \leftarrow (\lambda x.\, y \overset{\bullet}{=} \lambda x.\, z); (y \overset{\bullet}{=} z) \to (\lambda x.\, z \overset{\bullet}{=} \lambda x.\, z); \mathbf{ok} \to \mathbf{ok}; \mathbf{ok}$$

This is where the notion of *allocated abstraction* plays an important role. We will work with the invariant that if $\lambda^{\ell}x.\,P$ and $\lambda^{\ell'}y.\,Q$ are two allocated abstractions in the same location ($\ell = \ell'$) then their bodies will be equal, up to α-renaming. This ensures that different allocated abstractions are still different after substitution, as they must be decorated with different locations.

Unification goals and unifiers. A *goal* is a term of the form $\mathtt{v} \overset{\bullet}{=} \mathtt{w}$. A *unification problem* is a finite set of goals $\mathsf{G} = \{\mathtt{v}_1 \overset{\bullet}{=} \mathtt{w}_1, \ldots, \mathtt{v}_n \overset{\bullet}{=} \mathtt{w}_n\}$. If σ is a substitution we write G^{σ} for $\{\mathtt{v}_1{}^{\sigma} \overset{\bullet}{=} \mathtt{w}_1{}^{\sigma}, \ldots, \mathtt{v}_n{}^{\sigma} \overset{\bullet}{=} \mathtt{w}_n{}^{\sigma}\}$. A *unifier* for $\mathsf{G} = \{\mathtt{v}_1 \overset{\bullet}{=} \mathtt{w}_1, \ldots, \mathtt{v}_n \overset{\bullet}{=} \mathtt{w}_n\}$ is a substitution σ such that $\mathtt{v}_i{}^{\sigma} = \mathtt{w}_i{}^{\sigma}$ for all $1 \leq i \leq n$. A unifier σ for G is *most general* if for any other unifier ρ one has $\sigma \lesssim \rho$.

Coherence invariant. As mentioned before, we impose an invariant on programs forcing that allocated abstractions decorated with the same location must be syntactically equal. Moreover, we require that allocated abstractions do not refer to variables bound outside of their scope, *i.e.* that they are in fact closures. Note that the source program trivially satisfies this invariant, as it is expected that allocated abstractions are not written by the user but generated at runtime.

More precisely, a set X of terms is **coherent** if the two following conditions hold. **(1)** Consider any allocated abstraction under a context C, *i.e.* let $t \in X$ such that $t = \mathsf{C}\langle\lambda^{\ell}x.\,P\rangle$. Then the context C does not bind any of the free variables of $\lambda^{\ell}x.\,P$. **(2)** Consider any two allocated abstractions in t and s with the same location, *i.e.* let $t, s \in X$ be such that $t = \mathsf{C}\langle\lambda^{\ell}x.\,P\rangle$ and $s = \mathsf{C}'\langle\lambda^{\ell}y.\,Q\rangle$, Then $P\{x := y\} = Q$.

We extend the notion of coherence to other syntactic categories as follows. A term t is coherent if $\{t\}$ is coherent. A program $P = t_1 \oplus \ldots \oplus t_n$ is *coherent* if each thread t_i is coherent. A unification problem G is *coherent* if it is coherent seen as a set. Note that a program may be coherent even if different abstractions in different threads have the same location. For example, $(\lambda^{\ell}x.\,x\,x \overset{\bullet}{=} \lambda^{\ell}y.\,\mathbf{c}) \oplus (\lambda^{\ell'}y.\,y)$ is not coherent, whereas $(\lambda^{\ell}x.\,x\,x \overset{\bullet}{=} \lambda^{\ell}y.\,y\,y) \oplus (\lambda^{\ell}y.\,\mathbf{c})$ is coherent.

Unification algorithm. The standard Martelli–Montanari [19] unification algorithm can be adapted to our setting. In particular, there is a computable function $\mathsf{mgu}(-)$ such that if G is a coherent unification problem then either $\mathsf{mgu}(\mathsf{G}) = \sigma$, *i.e.* $\mathsf{mgu}(\mathsf{G})$ returns a substitution σ which is an idempotent most general unifier for G, or $\mathsf{mgu}(\mathsf{G}) = \bot$, *i.e.* $\mathsf{mgu}(\mathsf{G})$ fails and G has no unifier. Moreover, it can be shown that if the algorithm succeeds, the set $\mathsf{G}^{\sigma} \cup \{\sigma(x) \mid x \in \mathsf{Var}\}$ is coherent. The algorithm, formal statement and proofs are detailed in the appendix ♣Sec. A.1.

Operational semantics. The $\lambda^{\mathtt{U}}$**-calculus** is the rewriting system whose objects are programs, and whose reduction relation is given by the union of the following six rules:

Definition 3.1 (Reduction rules).

$$
\begin{array}{rcll}
P_1 \oplus \mathsf{W}\langle \lambda x.\, P\rangle \oplus P_2 & \xrightarrow{\texttt{alloc}} & P_1 \oplus \mathsf{W}\langle \lambda^{\ell} x.\, P\rangle \oplus P_2 & \textit{if } \ell \notin \mathsf{locs}(\mathsf{W}\langle \lambda x.\, P\rangle) \\
P_1 \oplus \mathsf{W}\langle (\lambda^{\ell} x.\, P)\, \mathtt{v}\rangle \oplus P_2 & \xrightarrow{\texttt{beta}} & P_1 \oplus \mathsf{W}\langle P\{x := \mathtt{v}\}\rangle \oplus P_2 & \\
P_1 \oplus \mathsf{W}\langle \mathtt{v}; t\rangle \oplus P_2 & \xrightarrow{\texttt{guard}} & P_1 \oplus \mathsf{W}\langle t\rangle \oplus P_2 & \\
P_1 \oplus \mathsf{W}\langle \nu x.\, t\rangle \oplus P_2 & \xrightarrow{\texttt{fresh}} & P_1 \oplus \mathsf{W}\langle t\{x := y\}\rangle \oplus P_2 & \textit{if } y \notin \mathsf{fv}(\mathsf{W}) \\
P_1 \oplus \mathsf{W}\langle \mathtt{v} \overset{\bullet}{=} \mathtt{w}\rangle \oplus P_2 & \xrightarrow{\texttt{unif}} & P_1 \oplus \mathsf{W}\langle \mathbf{ok}\rangle^{\sigma} \oplus P_2 & \textit{if } \mathsf{mgu}(\{\mathtt{v} \overset{\bullet}{=} \mathtt{w}\}) = \sigma \\
P_1 \oplus \mathsf{W}\langle \mathtt{v} \overset{\bullet}{=} \mathtt{w}\rangle \oplus P_2 & \xrightarrow{\texttt{fail}} & P_1 \oplus P_2 & \textit{if } \mathsf{mgu}(\{\mathtt{v} \overset{\bullet}{=} \mathtt{w}\}) \textit{ fails}
\end{array}
$$

Note that all rules operate on a single thread and they are **not** closed under any kind of evaluation contexts. The `alloc` rule allocates a closure, *i.e.* whenever a λ-abstraction is found below an evaluation context, it may be assigned a fresh location ℓ. The `beta` rule applies a function to a value. The `guard` rule proceeds with the evaluation of the right part of a guarded expression when the left part is already a value. The `fresh` rule introduces a fresh symbolic variable. The `unif` and `fail` rules solve a unification problem, corresponding to the success and failure cases respectively. If there is a unifier, the substitution is applied to the affected thread. For example:

$$
\begin{array}{rl}
(\lambda x.\, x \oplus (\nu y.\, ((x \overset{\bullet}{=} \mathbf{c}\, y); y)))\, (\mathbf{c}\, \mathbf{d}) & \xrightarrow{\texttt{alloc}} (\lambda^{\ell} x.\, x \oplus (\nu y.\, ((x \overset{\bullet}{=} \mathbf{c}\, y); y)))\, (\mathbf{c}\, \mathbf{d}) \\
& \xrightarrow{\texttt{beta}} \mathbf{c}\, \mathbf{d} \oplus \nu y.\, ((\mathbf{c}\, \mathbf{d} \overset{\bullet}{=} \mathbf{c}\, y); y) \\
& \xrightarrow{\texttt{fresh}} \mathbf{c}\, \mathbf{d} \oplus ((\mathbf{c}\, \mathbf{d} \overset{\bullet}{=} \mathbf{c}\, z); z) \\
& \xrightarrow{\texttt{unif}} \mathbf{c}\, \mathbf{d} \oplus (\mathbf{ok}; \mathbf{d}) \\
& \xrightarrow{\texttt{guard}} \mathbf{c}\, \mathbf{d} \oplus \mathbf{d}
\end{array}
$$

Structural equivalence. As already remarked in Sec. 2, we will not be able to prove that confluence holds strictly speaking, but only *up to reordering of threads* in the toplevel program. Moreover the `alloc` and `fresh` rules introduce fresh names, and, as usual the most general unifier is unique only *up to renaming.* These conditions are expressed formally by means of the following relation of structural equivalence.

Formally, **structural equivalence** between programs is written $P \equiv Q$ and defined as the reflexive, symmetric, and transitive closure of the three following axioms:

1. $\equiv$-`swap`: $P \oplus t \oplus s \oplus Q \equiv P \oplus s \oplus t \oplus Q$.
2. $\equiv$-`var`: If $y \notin \mathsf{fv}(t)$ then $P \oplus t \oplus Q \equiv P \oplus t\{x := y\} \oplus Q$.
3. $\equiv$-`loc`: If $\ell' \notin \mathsf{locs}(t)$, then $P \oplus t \oplus Q \equiv P \oplus t\{\ell := \ell'\} \oplus Q$.

In short, $\equiv$-`swap` means that threads may be reordered arbitrarily, $\equiv$-`var` means that symbolic variables are local to each thread, and $\equiv$-`loc` means that locations are local to each thread.

The following lemma establishes that the coherence invariant is closed by reduction and structural equivalence, which means that the $\lambda^{\mathtt{U}}$-calculus is well-defined if restricted to coherent programs. In the rest of this paper, we always assume that **all programs enjoy the coherence invariant**.

Lemma 3.2. *Let P be a coherent program. If $P \equiv Q$ or $P \to Q$, then Q is also coherent.* ♣ *Sec. A.3*

The following lemma establishes that reduction is well-defined modulo structural equivalence (*i.e.* it lifts to $\equiv$-equivalence classes):

Lemma 3.3. *Structural equivalence is a strong bisimulation with respect to $\to$. Precisely, let $P \equiv P' \xrightarrow{\mathtt{x}} Q$ with $\mathtt{x} \in \{\mathtt{alloc}, \mathtt{beta}, \mathtt{guard}, \mathtt{fresh}, \mathtt{unif}, \mathtt{fail}\}$. Then there exists a program Q' such that $P \xrightarrow{\mathtt{x}} Q' \equiv Q$.* ♣ *Sec. A.4*

Example 3.4 (Type inference algorithm). As an illustrative example, the following translation $\mathbb{W}[-]$ converts an untyped λ-term t into a $\lambda^{\mathtt{U}}$-term that calculates the principal type of t according to the usual Hindley–Milner [23] type inference algorithm, or fails if it has no type. Note that an arrow type $(A \to B)$ is encoded as $(\mathbf{f}\, A\, B)$:

$$\mathbb{W}[x] \stackrel{\text{def}}{=} a_x \qquad \mathbb{W}[\lambda x.\, t] \stackrel{\text{def}}{=} \nu a_x.\, \mathbf{f}\, a_x\, \mathbb{W}[t] \qquad \mathbb{W}[t\, s] \stackrel{\text{def}}{=} \nu a.\, ((\mathbb{W}[t] \stackrel{\bullet}{=} \mathbf{f}\, \mathbb{W}[s]\, a); a)$$

For instance, $\mathbb{W}[\lambda x.\, \lambda y.\, y\, x] = \nu a.\, \mathbf{f}\, a\, (\nu b.\, \mathbf{f}\, b\, (\nu c.\, (b \stackrel{\bullet}{=} \mathbf{f}\, a\, c); c)) \twoheadrightarrow \mathbf{f}\, a\, (\mathbf{f}\, (\mathbf{f}\, a\, c)\, c)$.

4 Operational Properties

In this section we study some properties of the operational semantics. First, we characterize the set of *normal forms* of the $\lambda^{\mathtt{U}}$-calculus syntactically, by means of an inductive definition (Prop. 4.1). Then we turn to the main result of this section, proving that it enjoys confluence up to structural equivalence (Thm. 4.4).

Characterization of normal forms. The set of **normal terms** $t^\star, s^\star, \ldots$ and **stuck terms** $S, S', \ldots$ are defined mutually inductively as follows. A normal term is either a value or a stuck term, *i.e.* $t^\star ::= \mathtt{v} \mid S$. A term is stuck if the judgment $t\triangledown$ is derivable with the following rules:

$$\frac{n > 0}{x\, t_1^\star \ldots t_n^\star \triangledown}\ \texttt{stuck-var} \qquad \frac{t_i^\star \triangledown \quad \text{for some } i \in \{1, 2, \ldots, n\}}{\mathbf{c}\, t_1^\star \ldots t_n^\star \triangledown}\ \texttt{stuck-cons}$$

$$\frac{t_1^\star \triangledown \qquad n \geq 0}{(t_1^\star; t_2^\star)\, s_1^\star \ldots s_n^\star \triangledown}\ \texttt{stuck-guard} \qquad \frac{t_i^\star \triangledown \quad \text{for some } i \in \{1, 2\} \qquad n \geq 0}{(t_1^\star \stackrel{\bullet}{=} t_2^\star)\, s_1^\star \ldots s_n^\star \triangledown}\ \texttt{stuck-unif}$$

$$\frac{t^\star \triangledown \qquad n \geq 0}{(\lambda^\ell x.\, P)\, t^\star\, s_1^\star \ldots s_n^\star \triangledown}\ \texttt{stuck-lam}$$

The set of **normal programs** $P^\star, Q^\star, \ldots$ is given by the following grammar: $P^\star ::= \mathtt{fail} \mid t^\star \oplus P^\star$. For example, the program $(\lambda^\ell x.\, x \stackrel{\bullet}{=} x) \oplus ((y\, \mathbf{c} \stackrel{\bullet}{=} \mathbf{d}); \mathbf{e}) \oplus z\, (z\, \mathbf{c})$ is normal, being the non-deterministic alternative of a value and two stuck terms. Normal programs capture the notion of normal form:

Proposition 4.1. *The set of normal programs is exactly the set of $\to$-normal forms.* ♣ *Sec. A.5*

Confluence. In order to prove that the $\lambda^{\mathtt{U}}$-calculus has the Church–Rosser property, we adapt the method due to Tait and Martin-Löf [5, Sec. 3.2] by defining a *simultaneous reduction relation* $\Rightarrow$, and showing that it verifies the diamond property (*i.e.* $\Leftarrow\Rightarrow\,\subseteq\,\Rightarrow\Leftarrow$) and the inclusions $\to\,\subseteq\,\Rightarrow\,\subseteq\,\twoheadrightarrow$, where $\twoheadrightarrow$ denotes the reflexive–transitive closure of $\to$. Actually, these properties only hold up to structural equivalence, so our confluence result, rather than the usual inclusion $\twoheadleftarrow\twoheadrightarrow\,\subseteq\,\twoheadrightarrow\twoheadleftarrow$, expresses the weakened inclusion $\twoheadleftarrow\twoheadrightarrow\,\subseteq\,\twoheadrightarrow\equiv\twoheadleftarrow$.

To define the relation of simultaneous reduction, we use the following notation, to lift the binary operations of unification ($t \overset{\bullet}{=} s$), guarded expression ($t; s$), and application ($t\,s$) from the sort of terms to the sort of programs. Let $\star$ denote a binary term constructor (*e.g.* unification, guarded expression, or application). Then we write $(\bigoplus_{i=1}^{n} t_i) \star (\bigoplus_{j=1}^{m} s_j) \overset{\text{def}}{=} \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m} (t_i \star s_j)$.

First, we define a judgment $t \overset{\mathsf{G}}{\Rightarrow} P$ of simultaneous reduction, relating a term and a program, parameterized by a set G of unification goals representing pending constraints:

$$\frac{}{x \overset{\varnothing}{\Rightarrow} x}\,\mathtt{Var} \qquad \frac{}{\mathbf{c} \overset{\varnothing}{\Rightarrow} \mathbf{c}}\,\mathtt{Cons} \qquad \frac{}{\nu x.\, t \overset{\varnothing}{\Rightarrow} \nu x.\, t}\,\mathtt{Fresh}_1 \qquad \frac{t \overset{\mathsf{G}}{\Rightarrow} P \qquad x \text{ fresh}}{\nu x.\, t \overset{\mathsf{G}}{\Rightarrow} P}\,\mathtt{Fresh}_2$$

$$\frac{}{\lambda x.\, P \overset{\varnothing}{\Rightarrow} \lambda x.\, P}\,\mathtt{Abs}^{\mathtt{C}}_1 \qquad \frac{\ell \text{ fresh}}{\lambda x.\, P \overset{\varnothing}{\Rightarrow} \lambda^{\ell} x.\, P}\,\mathtt{Abs}^{\mathtt{C}}_2 \qquad \frac{}{\lambda^{\ell} x.\, P \overset{\varnothing}{\Rightarrow} \lambda^{\ell} x.\, P}\,\mathtt{Abs}^{\mathtt{A}}$$

$$\frac{t \overset{\mathsf{G}}{\Rightarrow} P \qquad s \overset{\mathsf{H}}{\Rightarrow} Q}{t\, s \xRightarrow{\mathsf{G}\cup\mathsf{H}} P\, Q}\,\mathtt{App}_1 \qquad \frac{}{(\lambda^{\ell} x.\, P)\, \mathtt{v} \overset{\varnothing}{\Rightarrow} P\{x := \mathtt{v}\}}\,\mathtt{App}_2 \qquad \frac{t \overset{\mathsf{G}}{\Rightarrow} P \qquad s \overset{\mathsf{H}}{\Rightarrow} Q}{t; s \xRightarrow{\mathsf{G}\cup\mathsf{H}} P; Q}\,\mathtt{Guard}_1$$

$$\frac{t \overset{\mathsf{G}}{\Rightarrow} P}{\mathtt{v}; t \overset{\mathsf{G}}{\Rightarrow} P}\,\mathtt{Guard}_2 \qquad \frac{t \overset{\mathsf{G}}{\Rightarrow} P \qquad s \overset{\mathsf{H}}{\Rightarrow} Q}{t \overset{\bullet}{=} s \xRightarrow{\mathsf{G}\cup\mathsf{H}} P \overset{\bullet}{=} Q}\,\mathtt{Unif}_1 \qquad \frac{}{\mathtt{v} \overset{\bullet}{=} \mathtt{w} \xRightarrow{\{\mathtt{v} \overset{\bullet}{=} \mathtt{w}\}} \mathbf{ok}}\,\mathtt{Unif}_2$$

As usual, most term constructors have two rules, the rule decorated with "1" is a congruence rule which chooses not to perform any evaluation on the root of the term, while the rule decorated with "2" requires that there is a redex at the root of the term, and contracts it. Note that rule $\mathtt{Unif}_2$ does *not* perform the unification of $\mathtt{v}$ and $\mathtt{w}$ immediately; it merely has the effect of propagating the unification constraint.

Using the relation defined above, we are now able to define the relation of **simultaneous reduction** between programs:

$$\frac{}{\mathtt{fail} \Rightarrow \mathtt{fail}}\,\mathtt{Fail} \qquad \frac{t \overset{\mathsf{G}}{\Rightarrow} P \qquad Q \Rightarrow Q' \qquad P' = \begin{cases} P^{\sigma} & \text{if } \sigma = \mathsf{mgu}(\mathsf{G}) \\ \mathtt{fail} & \text{if } \mathsf{mgu}(\mathsf{G}) \text{ fails} \end{cases}}{t \oplus Q \Rightarrow P' \oplus Q'}\,\mathtt{Alt}$$

The following lemma summarizes some of the key properties of simultaneous reduction. Most are straightforward proofs by induction, except for item 3.:

Lemma 4.2 (Properties of simultaneous reduction).

1. **Reflexivity.** $t \overset{\varnothing}{\Rightarrow} t$ *and* $P \Rightarrow P$.

2. **Context closure.** *If* $t \overset{\mathsf{G}}{\Rightarrow} P$ *then* $\mathsf{W}\langle t\rangle \overset{\mathsf{G}}{\Rightarrow} \mathsf{W}\langle P\rangle$.
3. **Strong bisimulation.** *Structural equivalence is a strong bisimulation with respect to* $\Rightarrow$, i.e. *if* $P \equiv P' \Rightarrow Q$ *then there is a program* Q' *such that* $P \Rightarrow Q' \equiv Q$. ♣ *Sec. A.6*
4. **Substitution.** *If* $t \overset{\mathsf{G}}{\Rightarrow} P$ *then* $t^\sigma \overset{\mathsf{G}^\sigma}{\Longrightarrow} P^\sigma$.

The core argument is the following adaptation of Tait–Martin-Löf's technique, from which confluence comes out as an easy corollary. See ♣ Sec. A.7 in the appendix for details.

Proposition 4.3 (Tait–Martin-Löf's technique, up to $\equiv$).
1. $\to \subseteq \Rightarrow\equiv$
2. $\Rightarrow \subseteq \twoheadrightarrow\equiv$
3. $\Rightarrow$ *has the diamond property, up to* $\equiv$, *that is:*
If $P_1 \Rightarrow P_2$ *and* $P_1 \Rightarrow P_3$ *then* $P_2 \Rightarrow\equiv P_4$ *and* $P_3 \Rightarrow\equiv P_4$ *for some* P_4.

Theorem 4.4 (Confluence). *The reduction relation* $\to$ *is confluent, up to* $\equiv$. *More precisely, if* $P_1 \twoheadrightarrow P_2$ *and* $P_1 \twoheadrightarrow P_3$ *then there is a program* P_4 *such that* $P_2 \twoheadrightarrow\equiv P_4$ *and* $P_3 \twoheadrightarrow\equiv P_4$.

Example 4.5. Suppose that $\sigma = \mathsf{mgu}(\mathtt{v}_1 \overset{\bullet}{=} \mathtt{v}_2)$ and $\tau = \mathsf{mgu}(\mathtt{w}_1 \overset{\bullet}{=} \mathtt{w}_2)$. Consider:

$$(\mathtt{v_1}^\tau \overset{\bullet}{=} \mathtt{v_2}^\tau)\,\mathbf{ok}\,t^\tau \leftarrow (\mathtt{v}_1 \overset{\bullet}{=} \mathtt{v}_2)\,(\mathtt{w}_1 \overset{\bullet}{=} \mathtt{w}_2)\,t \to \mathbf{ok}\,(\mathtt{w_1}^\sigma \overset{\bullet}{=} \mathtt{w_2}^\sigma)\,t^\sigma$$

Then both $\sigma' = \mathsf{mgu}(\mathtt{v_1}^\tau \overset{\bullet}{=} \mathtt{v_2}^\tau)$ and $\tau' = \mathsf{mgu}(\mathtt{w_1}^\sigma \overset{\bullet}{=} \mathtt{w_2}^\sigma)$ must exist, and the peak may be closed as follows:

$$(\mathtt{v_1}^\tau \overset{\bullet}{=} \mathtt{v_2}^\tau)\,\mathbf{ok}\,t^\tau \to \mathbf{ok}\,\mathbf{ok}\,(t^\tau)^{\sigma'} \equiv \mathbf{ok}\,\mathbf{ok}\,(t^\sigma)^{\tau'} \leftarrow \mathbf{ok}\,(\mathtt{w_1}^\sigma \overset{\bullet}{=} \mathtt{w_2}^\sigma)\,t^\sigma$$

the equivalence relies on the fact that $\tau' \circ \sigma$ and $\sigma' \circ \tau$ are both most general unifiers of $\{\mathtt{v}_1 \overset{\bullet}{=} \mathtt{v}_2, \mathtt{w}_1 \overset{\bullet}{=} \mathtt{w}_2\}$, hence $(t^\tau)^{\sigma'} \equiv (t^\sigma)^{\tau'}$, up to renaming.

5 Simple Types for $\lambda^{\mathtt{U}}$

In this section we discuss a simply typed system for the $\lambda^{\mathtt{U}}$-calculus. The system does not present any essential difficulty, but it is a necessary prerequisite to be able to define the denotational semantics of Sec. 6. The main result in this section is subject reduction (Prop. 5.2).

Note that, unlike in the simply typed λ-calculus, reduction may create free variables, due to fresh variable introduction. For instance, in the reduction step $\mathbf{c}(\nu x.\,x) \to \mathbf{c}\,x$, a new variable x appears free on the right-hand side. Therefore the subject reduction lemma has to *extend* the typing context in order to account for freshly created variables. This may be understood only as a matter of notation, *e.g.* in a different presentation of the $\lambda^{\mathtt{U}}$-calculus the step above could be written as $\mathbf{c}(\nu x.\,x) \to \nu x.\,(\mathbf{c}\,x)$, using a *scope extrusion* rule reminiscent of the rule to create new channels in process calculi (*e.g.* π-calculus), avoiding the creation of free variables.

Types and typing contexts. Suppose given a denumerable set of *base types* $\alpha, \beta, \gamma, \ldots$. The sets of *types* $\mathsf{Type} = \{A, B, \ldots\}$ and *typing contexts* $\Gamma, \Delta, \ldots$ are given by:

$$A, B, \ldots ::= \alpha \mid A \to B \qquad \Gamma ::= \varnothing \mid \Gamma, x : A$$

we assume that no variable occurs twice in a typing context. Typing contexts are to be regarded as finite sets of assumptions of the form $(x : A)$, *i.e.* we work implicitly modulo contraction and exchange. We assume that each constructor $\mathbf{c}$ has an associated type $\mathcal{T}_{\mathbf{c}}$.

Typing rules. Judgments are of the form. "$\Gamma \vdash X : A$" where X may be a term or a program, meaning that X has type A under Γ. The typing rules are the following:

$$\frac{(x : A) \in \Gamma}{\Gamma \vdash x : A}\ \texttt{t-var} \qquad \frac{}{\Gamma \vdash \mathbf{c} : \mathcal{T}_{\mathbf{c}}}\ \texttt{t-cons} \qquad \frac{\Gamma, x : A \vdash P : B}{\Gamma \vdash \lambda^{(\ell)} x. P : A \to B}\ \texttt{t-lam(l)}$$

$$\frac{\Gamma \vdash t : A \qquad \Gamma \vdash s : A}{\Gamma \vdash t \overset{\bullet}{=} s : \mathcal{T}_{\mathbf{ok}}}\ \texttt{t-unif} \qquad \frac{\Gamma \vdash t : \mathcal{T}_{\mathbf{ok}} \qquad \Gamma \vdash s : A}{\Gamma \vdash t; s : A}\ \texttt{t-guard}$$

$$\frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \nu x. t : B}\ \texttt{t-fresh} \qquad \frac{}{\Gamma \vdash \texttt{fail} : A}\ \texttt{t-fail} \qquad \frac{\Gamma \vdash t : A \qquad \Gamma \vdash P : A}{\Gamma \vdash t \oplus P : A}\ \texttt{t-alt}$$

Note that all abstractions are typed in the same way, regardless of whether they are allocated or not. A unification has the same type as the constructor **ok**, as does t in the guarded expression $(t; s)$. A freshly introduced variable of type A represents, from the logical point of view, an unjustified assumption of A. The empty program `fail` can also be given any type. All the threads in a program must have the same type. The following properties of the type system are routine:

Lemma 5.1. *Let X stand for either a term or a program. Then:*

1. **Weakening.** *If $\Gamma \vdash X : A$ then $\Gamma, x : B \vdash X : A$.*
2. **Strengthening.** *If $\Gamma, x : A \vdash X : B$ and $x \notin \mathsf{fv}(X)$, then $\Gamma \vdash X : B$.*
3. **Substitution.** *If $\Gamma, x : A \vdash X : B$ and $\Gamma \vdash s : A$ then $\Gamma \vdash X\{x := s\} : B$.*
4. **Contextual substitution.** *$\Gamma \vdash \mathsf{W}\langle t \rangle : A$ holds if and only if there is a type B such that $\Gamma, \Box : B \vdash \mathsf{W} : A$ and $\Gamma \vdash t : B$ hold.*
5. **Program composition/decomposition.** *$\Gamma \vdash P \oplus Q : A$ holds if and only if $\Gamma \vdash P : A$ and $\Gamma \vdash Q : A$ hold.*

Proposition 5.2 (Subject reduction). *Let $\Gamma \vdash P : A$ and $P \to Q$. Then $\Gamma' \vdash Q : A$, where $\Gamma' = \Gamma$ if the step is derived using any reduction rule other than* `fresh`*, and $\Gamma' = (\Gamma, x : B)$ if the step introduces a fresh variable $(x : B)$.*

Proof. By case analysis on the transition $P \to Q$, using Lem. 5.1. The interesting case is the `unif` case, which requires proving that the substitution σ returned by $\mathsf{mgu}(\mathsf{G})$ preserves the types of the instantiated variables. ♣ Sec. A.8

6 Denotational Semantics

In this section we propose a *naive* denotational semantics for the $\lambda^{\mathtt{U}}$-calculus. The semantics is naive in at least three senses: first, types are interpreted merely as sets, rather than as richer structures (*e.g.* complete partial orders) or in a more abstract (*e.g.* categorical) framework. Second, since types are interpreted as sets, the *multiplicities* of results are not taken into account, so for example $[\![x \oplus x]\!] = [\![x]\!] \cup [\![x]\!] = [\![x]\!]$. Third, and most importantly, the denotation of abstractions $(\lambda x.\, P)$ is conflated with the denotation of allocated abstractions $(\lambda^{\ell} x.\, P)$. This means that the operational semantics cannot be complete with respect to the denotational one, given that for example $\lambda^{\ell} x.\, x$ and $\lambda^{\ell'} x.\, x$ have the same denotation but they are not observationally equivalent[5]. Nevertheless, studying this simple denotational semantics already presents some technical challenges, and we regard it as a first necessary step towards formulating a better behaved semantics[6].

Roughly speaking, the idea is that a type A shall be interpreted as a set $[\![A]\!]$, while a program P of type A shall be interpreted as a subset $[\![P]\!] \subseteq [\![A]\!]$. For example, if $[\![\mathtt{Nat}]\!] = \mathbb{N}$, then given constructors $\mathbf{1} : \mathtt{Nat}$, $\mathbf{2} : \mathtt{Nat}$ with their obvious interpretations, and if $\mathit{add} : \mathtt{Nat} \to \mathtt{Nat} \to \mathtt{Nat}$ denotes addition, we expect that:

$$[\![(\lambda f : \mathtt{Nat} \to \mathtt{Nat}.\, \nu y.\, ((y \overset{\bullet}{=} \mathbf{1}); \mathit{add}\, y\, (f\, y)))(\lambda x.\, x \oplus \mathbf{2})]\!] = \{1+1, 1+2\} = \{2, 3\}$$

The soundness result that we shall prove states that if $P \twoheadrightarrow Q$ then $[\![P]\!] \supseteq [\![Q]\!]$. Intuitively, the possible behaviors of Q are among the possible behaviors of P.

To formulate the denotational semantics, for ease of notation, we work with an *à la Church* variant of the type system[7]. That is, we suppose that the set of variables is partitioned in such a way that each variable has an intrinsic type. More precisely, for each type A there is a denumerably infinite set of variables $x^A, y^A, z^A, \ldots$ of that type. We also decorate each occurrence of $\mathtt{fail}$ with its type, *i.e.* we write $\mathtt{fail}^A$ for the empty program of type A. Sometimes we omit the type decoration if it is clear from the context. Under this assumption, it is easy to show that the system enjoys a strong form of *unique typing*, *i.e.* that if X is a typable term or program then there is a unique derivation $\Gamma \vdash X : A$, up to weakening of Γ with variables not in $\mathsf{fv}(X)$. This justifies that we may write $\vdash X : A$ omitting the context.

Domain of interpretation. We suppose given a **non-empty** set S_α for each base type α. The *interpretation* of a type A is a set written $[\![A]\!]$ and defined

[5] *E.g.* $\lambda^{\ell} x.\, x \overset{\bullet}{=} \lambda^{\ell} x.\, x$ succeeds but $\lambda^{\ell} x.\, x \overset{\bullet}{=} \lambda^{\ell'} x.\, x$ fails.

[6] We expect that a less naive semantics should be stateful, involving a *memory*, in such a way that abstractions $(\lambda x.\, P)$ allocate a memory cell and store a closure, whereas allocated abstractions $(\lambda^{\ell} x.\, P)$ denote a memory location in which a closure is already stored.

[7] Transitioning between Church vs. Curry style variants of this system is a straightforward exercise, following for instance [6, Prop. 1.2.19].

recursively as follows, where $\mathcal{P}(X)$ is the usual set-theoretic power set, and Y^X is the set of functions with domain X and codomain Y:

$$[\![\alpha]\!] \stackrel{\text{def}}{=} \mathsf{S}_\alpha \qquad [\![A \to B]\!] \stackrel{\text{def}}{=} \mathcal{P}([\![B]\!])^{[\![A]\!]}$$

Note that, for every type A, the set $[\![A]\!]$ is non-empty, given that we require that S_α be non-empty. This decision is not arbitrary; rather it is necessary for soundness to hold. For instance, operationally we have that $x^A; y^B \xrightarrow{\texttt{guard}} y^B$, so denotationally we would expect $[\![x^A; y^B]\!] \supseteq [\![y^B]\!]$. This would not hold if $[\![A]\!] = \varnothing$ and $[\![B]\!] \neq \varnothing$, as then $[\![x^A; y^B]\!] = \varnothing$ whereas $[\![y^B]\!]$ would be a non-empty set.

Another technical constraint that we must impose is that *the interpretation of a value should always be a singleton*. For example, operationally we have that $(\lambda x : \texttt{Nat}.\, x + x)\, \texttt{v} \twoheadrightarrow \texttt{v} + \texttt{v}$, so denotationally, by soundness, we would expect that $[\![(\lambda x : \texttt{Nat}.\, x + x)\, \texttt{v}]\!] \supseteq [\![\texttt{v} + \texttt{v}]\!]$. If we had that $[\![\texttt{v}]\!] = \{1, 2\}$ is not a singleton, then we would have that $[\![(\lambda x.\, x + x)\, \texttt{v}]\!] = \{1 + 1, 2 + 2\}$ whereas $[\![\texttt{v} + \texttt{v}]\!] = \{1 + 1, 1 + 2, 2 + 1, 2 + 2\}$.

Following this principle, given that terms of the form $\mathbf{c}\, \texttt{v}_1 \dots \texttt{v}_n$ are values, their denotation $[\![\mathbf{c}\, \texttt{v}_1 \dots \texttt{v}_n]\!]$ must always be a singleton. This means that constructors must be interpreted as singletons, and constructors of function type should always return singletons (which in turn should return singletons if they are functions, and so on, recursively). Formally, any element $a \in [\![\alpha]\!]$ is declared to be α**-unitary**, and a function $f \in [\![A \to B]\!]$ is $(A \to B)$**-unitary** if for each $a \in [\![A]\!]$ the set $f(a) = \{b\} \subseteq [\![B]\!]$ is a singleton and b is B-unitary. Sometimes we say that an element a is *unitary* if the type is clear from the context. If f is $(A \to B)$-unitary, and $a \in [\![A]\!]$ sometimes, by abuse of notation, we may write $f(a)$ for the unique element $b \in f(a)$.

Interpretation of terms. For each constructor $\mathbf{c}$, we suppose given a $\mathcal{T}_\mathbf{c}$-unitary element $\underline{\mathbf{c}} \in [\![\mathcal{T}_\mathbf{c}]\!]$. Moreover, we suppose that the interpretation of constructors is *injective*, *i.e.* that $\underline{\mathbf{c}}(a_1) \dots (a_n) = \underline{\mathbf{c}}(b_1) \dots (b_n)$ implies $a_i = b_i$ for all $i = 1..n$.

An *environment* is a function $\rho : \mathsf{Var} \to \bigcup_{A \in \mathsf{Type}} [\![A]\!]$ such that $\rho(x^A) \in [\![A]\!]$ for each variable x^A of each type A. If ρ is an environment and $a \in [\![A]\!]$, we write $\rho[x^A \mapsto a]$ for the environment that maps x^A to a and agrees with ρ on every other variable. We write Env for the set of all environments.

Let $\vdash t : A$ (resp. $\vdash P : A$) be a typable term (resp. program) and let ρ be an environment. If $\vdash X : A$ is a typable term or program, we define its *denotation* *under the environment* ρ, written $[\![X]\!]_\rho$ as a subset of $[\![A]\!]$ as follows:

$$
\begin{array}{rll}
[\![x^A]\!]_\rho & \stackrel{\text{def}}{=} \{\rho(x^A)\} & \\
[\![\mathbf{c}]\!]_\rho & \stackrel{\text{def}}{=} \{\underline{\mathbf{c}}\} & \\
[\![\lambda x^A.\, P]\!]_\rho & \stackrel{\text{def}}{=} \{f\} & \text{where } f : [\![A]\!] \to \mathcal{P}([\![B]\!]) \text{ is given by } f(a) = [\![P]\!]_{\rho[x^A \mapsto a]} \\
[\![\lambda^\ell x^A.\, P]\!]_\rho & \stackrel{\text{def}}{=} \{f\} & \text{where } f : [\![A]\!] \to \mathcal{P}([\![B]\!]) \text{ is given by } f(a) = [\![P]\!]_{\rho[x^A \mapsto a]} \\
[\![t\, s]\!]_\rho & \stackrel{\text{def}}{=} \{b \mid \exists f \in [\![t]\!]_\rho,\ \exists a \in [\![s]\!]_\rho,\ b \in f(a)\} & \\
[\![t \stackrel{\bullet}{=} s]\!]_\rho & \stackrel{\text{def}}{=} \{\underline{\mathbf{ok}} \mid \exists a \in [\![t]\!]_\rho,\ \exists b \in [\![s]\!]_\rho,\ a = b\} & \\
[\![t; s]\!]_\rho & \stackrel{\text{def}}{=} \{a \mid \exists b \in [\![t]\!]_\rho,\ a \in [\![s]\!]_\rho\} & \\
[\![\nu x^A.\, t]\!]_\rho & \stackrel{\text{def}}{=} \{b \mid \exists a \in [\![A]\!],\ b \in [\![t]\!]_{\rho[x^A \mapsto a]}\} & \\
[\![\mathtt{fail}^A]\!]_\rho & \stackrel{\text{def}}{=} \varnothing & \\
[\![t \oplus P]\!]_\rho & \stackrel{\text{def}}{=} [\![t]\!]_\rho \cup [\![P]\!]_\rho &
\end{array}
$$

The denotation of a toplevel program is written $[\![P]\!]$ and defined as the union of its denotations under all possible environments, *i.e.* $[\![P]\!] \stackrel{\text{def}}{=} \bigcup_{\rho \in \mathsf{Env}} [\![P]\!]_\rho$.

Proposition 6.1 (Properties of the denotational semantics).

1. **Irrelevance.** *If* ρ *and* ρ' *agree on* $\mathsf{fv}(X)$*, then* $[\![X]\!]_\rho = [\![X]\!]_{\rho'}$*. Here* X *stands for either a program or a term.* ♣ *Lem. A.1*
2. **Compositionality.** ♣ *Lem. A.2*
   2.1 $[\![P \oplus Q]\!]_\rho = [\![P]\!]_\rho \cup [\![Q]\!]_\rho$.
   2.2 If W *is a context whose hole is of type* A*, then* $[\![\mathsf{W}\langle t\rangle]\!]_\rho = \{b \mid a \in [\![t]\!]_\rho, b \in [\![\mathsf{W}]\!]_{\rho[\Box^A \mapsto a]}\}$.
3. **Interpretation of values.** *If* $\mathtt{v}$ *is a value then* $[\![\mathtt{v}]\!]_\rho$ *is a singleton.* ♣ *Lem. A.4*
4. **Interpretation of substitution.** ♣ *Lem. A.5*
   Let $\sigma = \{x_1^{A_1} \mapsto \mathtt{v}_1, \ldots, x_n^{A_n} \mapsto \mathtt{v}_n\}$ *be a substitution such that* $x_i \notin \mathsf{fv}(\mathtt{v}_j)$ *for all* i, j*. Let* $[\![\mathtt{v}_i]\!]_\rho = \{a_i\}$ *for each* $i = 1..n$ *(noting that values are singletons, by the previous item of this lemma). Then for any program or term* X *we have that* $[\![X^\sigma]\!]_\rho = [\![X]\!]_{\rho[x_1 \mapsto a_1]\ldots[x_n \mapsto a_n]}$.

To conclude this section, the following theorem shows that the operational semantics is sound with respect to the denotational semantics.

Theorem 6.2 (Soundness). *Let* $\Gamma \vdash P : A$ *and* $P \to Q$*. Then* $[\![P]\!] \supseteq [\![Q]\!]$*. The inclusion is an equality for all reduction rules other than the* `fail` *rule.*

Proof. The proof (♣ Thm. A.10.3) is technical by exhaustive case analysis of all possible reduction steps, using Prop. 6.1 throughout. The `unif` rule is non-trivial, as it requires to formulate an invariant for the unification algorithm. The core of the argument is an auxiliary lemma essentially stating that if $\mathsf{G} \rightsquigarrow \mathsf{H}$ is a step of the unification algorithm that does not fail, then the set of environments that fulfill the equality constraints imposed by G are the same environments that fulfill the equality constraints imposed by H.

Example 6.3. Consider the reduction $\nu x.\, \Big((\lambda z.\, \nu y.\, ((z \overset{\bullet}{=} \mathbf{t}\, \mathbf{1}\, y); (\mathbf{t}\, y\, x)))\, (\mathbf{t}\, x\, \mathbf{2})\Big) \twoheadrightarrow \mathbf{t}\, \mathbf{2}\, \mathbf{1}$. If $[\![\mathtt{Tuple}]\!] = [\![\mathtt{Nat}]\!] \times [\![\mathtt{Nat}]\!] = \mathbb{N} \times \mathbb{N}$, the constructors $\mathbf{1} : \mathtt{Nat}$, $\mathbf{2} : \mathtt{Nat}$ are given their obvious interpretations and $\mathbf{t} : \mathtt{Nat} \to \mathtt{Nat} \to \mathtt{Tuple}$ is the pairing function[8], then for any environment ρ, if we abbreviate $\rho' := \rho[x \mapsto n][z \mapsto p][y \mapsto m]$, we have:

$$
\begin{aligned}
& [\![\nu x.\, \Big((\lambda z.\, \nu y.\, ((z \overset{\bullet}{=} \mathbf{t}\, \mathbf{1}\, y); (\mathbf{t}\, y\, x)))\, (\mathbf{t}\, x\, \mathbf{2})\Big)]\!]_\rho \\
&= \{[\![(\lambda z.\, \nu y.\, ((z \overset{\bullet}{=} \mathbf{t}\, \mathbf{1}\, y); (\mathbf{t}\, y\, x)))\, (\mathbf{t}\, x\, \mathbf{2})]\!]_{\rho[x \mapsto n]} \mid n \in \mathbb{N}\} \\
&= \{r \mid n \in \mathbb{N}, f \in [\![\lambda z.\, \nu y.\, ((z \overset{\bullet}{=} \mathbf{t}\, \mathbf{1}\, y); (\mathbf{t}\, y\, x))]\!]_{\rho[x \mapsto n]}, p \in [\![\mathbf{t}\, x\, \mathbf{2}]\!]_{\rho[x \mapsto n]}, r \in f(p)\} \\
&= \{r \mid n, m \in \mathbb{N}, p \in [\![\mathbf{t}\, x\, \mathbf{2}]\!]_{\rho[x \mapsto n]}, r \in [\![(z \overset{\bullet}{=} \mathbf{t}\, \mathbf{1}\, y); (\mathbf{t}\, y\, x)]\!]_{\rho'}\} \\
&= \{r \mid n, m \in \mathbb{N}, p \in \{(n, 2)\}, r \in [\![(z \overset{\bullet}{=} \mathbf{t}\, \mathbf{1}\, y); (\mathbf{t}\, y\, x)]\!]_{\rho'}\} \\
&= \{r \mid n, m \in \mathbb{N}, p \in \{(n, 2)\}, b \in [\![z \overset{\bullet}{=} \mathbf{t}\, \mathbf{1}\, y]\!]_{\rho'}, r \in [\![\mathbf{t}\, y\, x]\!]_{\rho'}\} \\
&= \{r \mid n, m \in \mathbb{N}, p \in \{(n, 2)\}, p = (1, m), r \in [\![\mathbf{t}\, y\, x]\!]_{\rho'}\} \\
&= \{r \mid n \in \{1\}, m \in \{2\}, p \in \{(1, 2)\}, r \in [\![\mathbf{t}\, y\, x]\!]_{\rho'}\} \\
&= \{(2, 1)\} \\
&= [\![\mathbf{t}\, \mathbf{2}\, \mathbf{1}]\!]_\rho
\end{aligned}
$$

An example in which the inclusion is proper is the reduction step $\lambda^\ell x.\, x \overset{\bullet}{=} \lambda^{\ell'} x.\, x \xrightarrow{\mathtt{fail}} \mathtt{fail}$. Note that $[\![\lambda^\ell x.\, x \overset{\bullet}{=} \lambda^{\ell'} x.\, x]\!] = \{\underline{\mathbf{ok}}\} \supsetneq \varnothing = [\![\mathtt{fail}]\!]$, given that our naive semantics equates the denotations of the abstractions, *i.e.* $[\![\lambda^\ell x.\, x]\!]_= [\![\lambda^{\ell'} x.\, x]\!]$, in spite of the fact that their locations differ.

7 Conclusion

In this work, we have proposed the $\lambda^{\mathtt{U}}$**-calculus** (Def. 3.1) an extension of the λ-calculus with relational features, including non-deterministic choice and first-order unification. We have studied some of its operational properties, providing an inductive **characterization of normal forms** (Prop. 4.1), and proving that it is **confluent** (Thm. 4.4) up to structural equivalence, by adapting the technique by Tait and Martin-Löf. We have proposed a system of simple types enjoying **subject reduction** (Prop. 5.2). We have also proposed a naive denotational semantics, in which a program of type A is interpreted as a set of elements of a set $[\![A]\!]$, for which we have proven **soundness** (Thm. 6.2). The denotational semantics is not complete.

As of the writing of this paper, we are attempting to formulate a refined denotational semantics involving a notion of *memory*, following the ideas mentioned in footnote 6. One difficulty is that in a term like $((x \overset{\bullet}{=} \lambda z.\, z); y)((y \overset{\bullet}{=} \lambda z.\, z); x)$, there seems to be a cyclic dependency between the denotation of the subterm on the left and denotation of the subterm on the right, so it is not clear how to formulate the semantics compositionally.

We have attempted to prove normalization results for the simply typed system, until now unsuccessfully. Given a constructor $\mathbf{c} : (A \to A) \to A$, a self-looping term $\omega(\mathbf{c}\, \omega)$ with $\omega \overset{\text{def}}{=} \lambda x^A.\, \nu y^{A \to A}.\, ((\mathbf{c} y \overset{\bullet}{=} x); y\, x)$ can be built, so

[8] Precisely, $\underline{\mathbf{t}}(n) = \{f_n\}$ with $f_n(m) = \{(n, m)\}$.

some form of *positivity condition* should be imposed. Other possible lines for future work include studying the relationship between calculi with patterns and $\lambda^{\mathtt{U}}$ by means of translations, and formulating richer type systems. For instance, one would like to be able to express *instantiation restrictions*, in such a way that a fresh variable representing a natural number is of type $\mathtt{Nat}^{-}$ while a term of type $\mathtt{Nat}^{+}$ represents a fully instantiated natural number.

Related Work. On **functional–logic** programming, we have mentioned λProlog [24,22] and Curry [13,12]. Other languages combining functional and logic features are Mercury [30] and Mozart/Oz [33]. There is a vast amount of literature on functional–logic programming. We mention a few works which most resemble our own. Miller [20] proposes a language with lambda-abstraction and a decidable extension of first-order unification which admits most general unifiers. Chakravarty et al. [8] and Smolka [29] propose languages in which the functional–logic paradigm is modeled as a concurrent process with communication. Albert et al. [1] formulate a *big-step* semantics for a functional–logic calculus with narrowing. On pure **relational** programming (without λ-abstractions), recently Rozhplokas et al. [27] have studied the operational and denotational semantics of miniKanren. On **λ-calculi with patterns** (without full unification), there have been many different approaches to their formulation [16,2,17,25,3]. On **λ-calculi with non-deterministic choice** (without unification), we should mention works on the λ-calculus extended with *erratic* [28] as well as with *probabilistic* choice [26,9].

Acknowledgements. To Alejandro Díaz-Caro for supporting our interactions. To Eduardo Bonelli, Delia Kesner, and the anonymous reviewers for their feedback and suggestions.

A Technical Appendix

The following lemma summarizes some expected properties of substitution that we use throughout the appendix. We omit the proofs, which are routine:

Lemma A.1 (Properties of substitution). *Let σ be an arbitrary substitution. Then:*

1. $\mathsf{W}\langle t\rangle^{\sigma} = \mathsf{W}^{\sigma}\langle t^{\sigma}\rangle$. *Note that there cannot be capture, given that* W *is a weak context, and it does not bind variables.*
2. $(t^{\sigma})^{\rho} = t^{\sigma\cdot\rho}$
3. $t\{x := \mathtt{v}\}^{\sigma} = t^{\sigma}\{x := \mathtt{v}^{\sigma}\}$ *as long as there is no capture,* i.e. $x \notin \operatorname{supp}\sigma$ *and for all* $y \in \mathsf{fv}(t)$ *we have that* $x \notin \mathsf{fv}(\sigma(y))$.
4. *If* $\mathtt{v}$ *is a value then* $\mathtt{v}^{\sigma}$ *is a value.*
5. *The relation* $\lesssim$ *is a preorder,* i.e. *reflexive and transitive.*

A.1 Unification Algorithm

We define the free variables ($\mathsf{fv}(\mathsf{G})$), locations ($\mathsf{locs}(\mathsf{G})$), and capture-avoiding substitution ($\mathsf{G}\{x := t\}$) for goals as follows:

$$\begin{aligned}
\mathsf{fv}(\{\mathtt{v}_1 \overset{\bullet}{=} \mathtt{w}_1, \dots, \mathtt{v}_n \overset{\bullet}{=} \mathtt{w}_n\}) &\overset{\text{def}}{=} \mathsf{fv}(\mathtt{v}_1 \overset{\bullet}{=} \mathtt{w}_1) \cup \dots \cup \mathsf{fv}(\mathtt{v}_n \overset{\bullet}{=} \mathtt{w}_n) \\
\mathsf{locs}(\{\mathtt{v}_1 \overset{\bullet}{=} \mathtt{w}_1, \dots, \mathtt{v}_n \overset{\bullet}{=} \mathtt{w}_n\}) &\overset{\text{def}}{=} \mathsf{locs}(\mathtt{v}_1 \overset{\bullet}{=} \mathtt{w}_1) \cup \dots \cup \mathsf{locs}(\mathtt{v}_n \overset{\bullet}{=} \mathtt{w}_n) \\
\{\mathtt{v}_1 \overset{\bullet}{=} \mathtt{w}_1, \dots, \mathtt{v}_n \overset{\bullet}{=} \mathtt{w}_n\}\{x := t\} &\overset{\text{def}}{=} \{(\mathtt{v}_1 \overset{\bullet}{=} \mathtt{w}_1)\{x := t\}, \dots, (\mathtt{v}_n \overset{\bullet}{=} \mathtt{w}_n)\{x := t\}\}
\end{aligned}$$

Definition A.1 (Unification algorithm). *The following is a variant of Martelli–Montanari's unification algorithm. We say that two values* $\mathtt{v}, \mathtt{w}$ clash *if any of the following conditions holds:*

1. *Constructor clash:* $\mathtt{v} = \mathbf{c}\,\mathtt{v}_1 \dots \mathtt{v}_n$ *and* $\mathtt{w} = \mathbf{d}\,\mathtt{w}_1 \dots \mathtt{w}_m$ *with* $\mathbf{c} \neq \mathbf{d}$.
2. *Arity clash:* $\mathtt{v} = \mathbf{c}\,\mathtt{v}_1 \dots \mathtt{v}_n$ *and* $\mathtt{w} = \mathbf{c}\,\mathtt{w}_1 \dots \mathtt{w}_m$ *with* $n \neq m$.
3. *Type clash:* $\mathtt{v} = \mathbf{c}\,\mathtt{v}_1 \dots \mathtt{v}_n$ *and* $\mathtt{w} = \lambda^{\ell} x.\, P$ *or vice-versa.*
4. *Location clash:* $\mathtt{v} = \lambda^{\ell} x.\, P$ *and* $\mathtt{w} = \lambda^{\ell'} y.\, Q$ *with* $\ell \neq \ell'$.

We define a rewriting system whose objects are unification problems G*, and the symbol* $\perp$*. The binary rewriting relation* $\rightsquigarrow$ *is given by the union of the following rules. Note that "*$\uplus$*" stands for the disjoint union of sets:*

$$\begin{array}{rlll}
\{x \overset{\bullet}{=} x\} \uplus \mathsf{G} & \rightsquigarrow_{\texttt{u-delete}} & \mathsf{G} & \\
\{\mathtt{v} \overset{\bullet}{=} x\} \uplus \mathsf{G} & \rightsquigarrow_{\texttt{u-orient}} & \{x \overset{\bullet}{=} \mathtt{v}\} \uplus \mathsf{G} & \textit{if } \mathtt{v} \notin \mathsf{Var} \\
\{\lambda^{\ell} x.\, P \overset{\bullet}{=} \lambda^{\ell} x.\, P\} \uplus \mathsf{G} & \rightsquigarrow_{\texttt{u-match-lam}} & \mathsf{G} & \\
\{\mathbf{c}\,\mathtt{v}_1 \dots \mathtt{v}_n \overset{\bullet}{=} \mathbf{c}\,\mathtt{w}_1 \dots \mathtt{w}_n\} \uplus \mathsf{G} & \rightsquigarrow_{\texttt{u-match-cons}} & \{\mathtt{v}_1 \overset{\bullet}{=} \mathtt{w}_1, \dots, \mathtt{v}_n \overset{\bullet}{=} \mathtt{w}_n\} \uplus \mathsf{G} & \\
\{\mathtt{v} \overset{\bullet}{=} \mathtt{w}\} \uplus \mathsf{G} & \rightsquigarrow_{\texttt{u-clash}} & \perp & \textit{if } \mathtt{v} \textit{ and } \mathtt{w} \textit{ clash} \\
\{x \overset{\bullet}{=} \mathtt{v}\} \uplus \mathsf{G} & \rightsquigarrow_{\texttt{u-eliminate}} & \{x \overset{\bullet}{=} \mathtt{v}\} \uplus \mathsf{G}\{x := \mathtt{v}\} & \textit{if } x \in \mathsf{fv}(\mathsf{G}) \setminus \mathsf{fv}(\mathtt{v}) \\
\{x \overset{\bullet}{=} \mathtt{v}\} \uplus \mathsf{G} & \rightsquigarrow_{\texttt{u-occurs-check}} & \perp & \textit{if } x \neq \mathtt{v} \textit{ and } x \in \mathsf{fv}(\mathtt{v})
\end{array}$$

Lemma A.2 (Coherence is invariant by unification). *If* G *is a coherent unification problem and* $\mathsf{G} \rightsquigarrow \mathsf{H}$ *then* H *is coherent.*

Proof. By inspection of the unification rules. The only interesting case is the `u-eliminate` rule:

$$\{x \stackrel{\bullet}{=} \mathtt{v}\} \cup \mathsf{G} \quad \rightsquigarrow_{\mathtt{u\text{-}eliminate}} \quad \{x \stackrel{\bullet}{=} \mathtt{v}\} \cup \mathsf{G}\{x := \mathtt{v}\}$$

Consider two abstractions $\lambda^{\ell} y.\, t$ and $\lambda^{\ell'} z.\, s$ in G such that, after performing the substitution $(\lambda^{\ell} y.\, t)\{x := \mathtt{v}\} = (\lambda^{\ell'} z.\, s)\{x := \mathtt{v}\}$ they have the same location, *i.e.* $\ell = \ell'$. Then since G is coherent we have that $\lambda^{\ell} y.\, t = \lambda^{\ell'} z.\, s$, and this means that $(\lambda^{\ell} y.\, t)\{x := \mathtt{v}\} = (\lambda^{\ell'} z.\, s)\{x := \mathtt{v}\}$, as required.

Theorem A.1.3. *Consider the relation $\rightsquigarrow$ restricted to* coherent *unification problems (Lem. A.2). Then:*

1. *The relation $\rightsquigarrow$ is strongly normalizing.*
2. *The normal forms of $\rightsquigarrow$ are $\bot$ and sets of goals of the form $\{x_1 \stackrel{\bullet}{=} \mathtt{v}_1, \ldots, x_n \stackrel{\bullet}{=} \mathtt{v}_n\}$ where $x_i \neq x_j$ and $x_i \notin \mathsf{fv}(\mathtt{v}_j)$ for every $i, j \in 1..n$.*
   If the normal form of G is $\{x_1 \stackrel{\bullet}{=} \mathtt{v}_1, \ldots, x_n \stackrel{\bullet}{=} \mathtt{v}_n\}$, we say that $\mathsf{mgu}(\mathsf{G})$ exists, and $\mathsf{mgu}(\mathsf{G}) = \{x_1 \mapsto \mathtt{v}_1, \ldots, x_n \mapsto \mathtt{v}_n\}$. If the normal form is $\bot$, we say that $\mathsf{mgu}(\mathsf{G})$ fails.
3. *The substitution $\sigma = \mathsf{mgu}(\mathsf{G})$ exists if and only if there exists a unifier for G. When it exists, $\mathsf{mgu}(\mathsf{G})$ is an* idempotent most general unifier. *Moreover:*
   3.1 The set $\mathsf{G}^{\sigma} \cup \{\sigma(x) \mid x \in \mathsf{Var}\}$ is coherent.
   3.2 For any $x \in \mathsf{Var}$ and any allocated abstraction $\lambda^{\ell} y.\, P$ in $\sigma(x)$, the location ℓ decorates an allocated abstraction in G.

Proof. A straightforward adaptation of standard results, see for example [4, Section 4.6]. We only focus in the interesting differences, namely the two subitems of item 3.:

1. Let us write $\mathsf{G} \rightsquigarrow^*_{\rho} \mathsf{G}'$ if there is a sequence of unification steps from G to G' such that ρ is the composition of all the substitutions performed in the `u-eliminate` steps.
   We claim that if $\mathsf{G} \rightsquigarrow^*_{\rho} \mathsf{G}'$ then $\mathsf{G}^{\rho} \cup \mathsf{G}'$ is coherent. By induction on the length of the sequence. The empty case is immediate, so let us suppose that $\mathsf{G} \rightsquigarrow^*_{\tau} \mathsf{G}'' \rightsquigarrow \mathsf{G}'$. By *i.h.*, $\mathsf{G}^{\tau} \cup \mathsf{G}''$ is coherent. Consider two cases, depending on whether the step $\mathsf{G}'' \rightsquigarrow \mathsf{G}'$ is an `u-eliminate` step or not.
   1.1 If it is an `u-eliminate` step, substituting a variable x for a value $\mathtt{v}$, then we also have a step $\mathsf{G}^{\tau} \cup \mathsf{G}'' \rightsquigarrow_{\mathtt{u\text{-}eliminate}} \mathsf{G}^{\tau \cdot (x \mapsto \mathtt{v})} \cup \mathsf{G}'$ and by Lem. A.2 we have that $\mathsf{G}^{\tau \cdot (x \mapsto \mathtt{v})} \cup \mathsf{G}'$ is coherent, as required.
   1.2 If it is not an `u-eliminate` step, then we also have a step $\mathsf{G}^{\tau} \cup \mathsf{G}'' \rightsquigarrow \mathsf{G}^{\tau} \cup \mathsf{G}'$ and by Lem. A.2 we have that $\mathsf{G}^{\tau} \cup \mathsf{G}'$ is coherent, as required.
   From this claim we have that if $\mathsf{G} \rightsquigarrow^* \{x_1 \stackrel{\bullet}{=} \mathtt{v}_1, \ldots, x_n \stackrel{\bullet}{=} \mathtt{v}_n\}$ and $\sigma := \{x_1 \mapsto \mathtt{v}_1, \ldots, x_n \mapsto \mathtt{v}_n\}$ then $\mathsf{G}^{\sigma} \cup \{x_1 \stackrel{\bullet}{=} \mathtt{v}_1, \ldots, x_n \stackrel{\bullet}{=} \mathtt{v}_n\}$ is coherent, which entails the required property.
2. We claim that if $\mathsf{G} \rightsquigarrow^* \mathsf{G}'$ then for any allocated abstraction $\lambda^{\ell} x.\, P$ in G', the location ℓ decorates an allocated abstraction in G. This is straightforward to prove by induction on the length of the reduction sequence, and it entails the required property.

A.2 Properties of Most General Unifiers

Lemma A.1 (Properties of most general unifiers).

1. *If* σ, σ' *are idempotent most general unifiers of* G*, there is a* renaming, i.e. *a substitution of the form* $\rho = \{x_1 \mapsto y_1, \ldots, x_n \mapsto y_n\}$*, such that* $\sigma' = \sigma \cdot \rho$*.*
2. *If* σ *is an idempotent most general unifier of* G *and* $y \notin \mathsf{fv}(\mathsf{G})$*, then* $\sigma' := (y \mapsto x) \cdot \sigma$ *is an idempotent most general unifier of* $\mathsf{G}\{x := y\}$*.*
3. *If* σ *is an idempotent most general unifier of* G *and* $\ell' \notin \mathsf{locs}(\mathsf{G})$ *then the substitution* σ' *given by* $\sigma'(x) = \sigma(x)\{\ell := \ell'\}$ *is an idempotent most general unifier of* $\mathsf{G}\{\ell := \ell'\}$*.*

Proof. We prove each item:

1. A standard result, see for example [4, Section 4.6].
2. Indeed:
   2.1 *Unifier:* For each goal $(\mathtt{v} \stackrel{\bullet}{=} \mathtt{w}) \in \mathsf{G}$, we have that $\mathtt{v}\{x := y\}^{\sigma'} = \mathtt{v}^{\sigma} = \mathtt{w}^{\sigma} = \mathtt{w}\{x := y\}^{\sigma'}$ since $y \notin \mathsf{fv}(\mathsf{G})$ and σ is a unifier of G.
   2.2 *Most general:* Let ρ be a unifier of $\mathsf{G}\{x := y\}$, *i.e.* such that $\mathtt{v}\{x := y\}^{\rho} = \mathtt{w}\{x := y\}^{\rho}$ for every goal $(\mathtt{v} \stackrel{\bullet}{=} \mathtt{w}) \in \mathsf{G}$. Then it is easily checked $(x \mapsto y) \cdot \rho$ is a unifier of G. Since σ is a most general unifier of G, we have that $(x \mapsto y) \cdot \rho = \sigma \cdot \tau$ for some τ. Hence $\rho = (y \mapsto x) \cdot (x \mapsto y) \cdot \rho = (y \mapsto x) \cdot \sigma \cdot \tau = \sigma' \cdot \tau$ as required.
3. It suffices to observe that if $\mathsf{G} \rightsquigarrow \mathsf{G}'$ then $\mathsf{G}\{\ell := \ell'\} \rightsquigarrow \mathsf{G}'\{\ell := \ell'\}$. This is easy to check for each rule. The only noteworthy remark is that in the `u-clash` we have that if $\mathtt{v}$ and $\mathtt{w}$ have a location clash, then $\mathtt{v}\{\ell := \ell'\}$ and $\mathtt{w}\{\ell := \ell'\}$ also have a location clash, because $\ell' \notin \mathsf{locs}(\mathsf{G})$.
   Then by induction on the number of $\rightsquigarrow$ steps, we have that if the normal form of G is $\{x_1 \stackrel{\bullet}{=} \mathtt{v}_1, \ldots, x_n \stackrel{\bullet}{=} \mathtt{v}_n\}$, then the normal form of $\mathsf{G}\{\ell := \ell'\}$ is $\{x_1 \stackrel{\bullet}{=} \mathtt{v}_1\{\ell := \ell'\}, \ldots, x_n \stackrel{\bullet}{=} \mathtt{v}_n\{\ell := \ell'\}\}$.

Lemma A.2 (Compositionality of most general unifiers). *The following are equivalent:*

1. $\sigma = \mathsf{mgu}(\mathsf{G} \cup \mathsf{H})$ *exists.*
2. $\sigma_1 = \mathsf{mgu}(\mathsf{G})$ *and* $\sigma_2 = \mathsf{mgu}(\mathsf{H}^{\sigma_1})$ *both exist.*

Moreover, if $\sigma, \sigma_1, \sigma_2$ *exist, then* $\sigma = \sigma_1 \cdot \sigma_2 \cdot \rho$ *for some renaming* ρ*.*

Proof.

$(1 \implies 2)$ Let $\sigma = \mathsf{mgu}(\mathsf{G} \cup \mathsf{H})$. Note in particular that σ is a unifier for G, so $\sigma_1 = \mathsf{mgu}(\mathsf{G})$ exists by Thm. A.1.3. On the other hand, note that σ_1 is more general than σ, so $\sigma = \sigma_1 \cdot \tau$ for some substitution τ. Since σ is a unifier for H, we have that τ is a unifier for H^{σ_1}. This means that $\sigma_2 = \mathsf{mgu}(\mathsf{H}^{\sigma_1})$ exists by Thm. A.1.3.

$(2 \implies 1)$ We claim that $\sigma_1 \cdot \sigma_2$ is a unifier of $\mathsf{G} \cup \mathsf{H}$. Indeed, note if $\mathtt{v} \stackrel{\bullet}{=} \mathtt{w}$ is a goal in G we have that σ_1 is a unifier for G, so $\mathtt{v}^{\sigma_1} = \mathtt{w}^{\sigma_1}$ and $\mathtt{v}^{\sigma_1 \cdot \sigma_2} = \mathtt{w}^{\sigma_1 \cdot \sigma_2}$. Moreover, if $\mathtt{v} \stackrel{\bullet}{=} \mathtt{w}$ is a goal in H, then $\mathtt{v}^{\sigma_1} \stackrel{\bullet}{=} \mathtt{w}^{\sigma_1}$ is a goal in H^{σ_1}, and since σ_2 is a unifier for H^{σ_1} we conclude that $\mathtt{v}^{\sigma_1 \cdot \sigma_2} \stackrel{\bullet}{=} \mathtt{w}^{\sigma_1 \cdot \sigma_2}$, as required.

For the final property in the statement, by Lem. A.1, it suffices to show that $\sigma_1 \cdot \sigma_2$ is more general than σ. Indeed, since σ is a unifier of G, we have that $\sigma = \sigma_1 \cdot \tau$ for some substitution τ, and since τ is a unifier of H^{σ_1}, we have that $\tau = \sigma_2 \cdot \tau'$ for some substitution τ', then $\sigma = \sigma_1 \cdot \sigma_2 \cdot \tau$, which means that $\sigma_1 \cdot \sigma_2$ is more general than σ.

A.3 Proof of Lem. 3.2 — Coherence Invariant

Proof. Item 1. is immediate by inspection of all the possible rules defining $\equiv$. For item 2., rules `guard`, `fresh`, and `fail` are immediate. Let us analyze the remaining cases:

1. `alloc`: $\mathsf{W}\langle \lambda x.\, t\rangle \to \mathsf{W}\langle \lambda^{\ell} x.\, t\rangle$. Immediate, as evaluation is under a weak context W, so the newly allocated abstraction has no variables bound by W. Moreover the new location is fresh so there are no other abstractions in the same location, and the rest of the program remains unmodified.
2. `beta`: $\mathsf{W}\langle (\lambda^{\ell} x.\, P)\mathtt{v}\rangle \to \mathsf{W}\langle P\{x := \mathtt{v}\}\rangle$. First consider an allocated abstraction $\lambda^{\ell'} y.\, Q$ in $\mathsf{W}\langle P\{x := \mathtt{v}\}\rangle$ and let us show that it has no variables bound by the context. If it is disjoint from the contracted redex, it is immediate. If it is in P, *i.e.* $P = \mathsf{C}\langle \lambda^{\ell'} y.\, Q'\rangle$ then $\lambda^{\ell'} y.\, Q'$ has no variables bound by C, so $\lambda^{\ell'} y.\, Q = \lambda^{\ell'} y.\, Q'\{x := \mathtt{v}\}$ also has no variables bound by C. If it is inside one of the copies of $\mathtt{v}$, then it also has no variables bound by C, as substitution is capture-avoiding.
   Consider any two abstractions $\lambda^{\ell'} y.\, Q$ and $\lambda^{\ell'} y.\, R$ in $\mathsf{W}\langle P\{x := \mathtt{v}\}\rangle$ such that they have the same location, and consider three cases, depending on the positions of the lambdas:
   2.1 If each lambda lies inside W or inside one of the copies of $\mathtt{v}$, then they can be traced back to abstractions in the term on the left-hand side, so $Q = R$ by hypothesis.
   2.2 If the lambdas are both in P, *i.e.* $P = \mathsf{C}\langle \lambda^{\ell'} y.\, Q \parallel \lambda^{\ell'} y.\, R\rangle$ then $Q = R$ by hypothesis. Moreover, note that by the invariant $x \notin \mathsf{fv}(Q) \cup \mathsf{fv}(R)$, so the lambdas in the reduct are equal.
   2.3 If one lambda is in P, *i.e.* $P = \mathsf{C}\langle \lambda^{\ell'} y.\, Q\rangle$, and the other one in W or in a copy of $\mathtt{v}$, note that by the invariant $x \notin \mathsf{fv}(Q)$, so $(\lambda^{\ell'} y.\, Q)\{x := \mathtt{v}\} = \lambda^{\ell'} y.\, Q$, so the lambdas in the reduct are equal.
3. `unif`: $\mathsf{W}\langle \mathtt{v} \overset{\bullet}{=} \mathtt{w}\rangle \to \mathsf{W}\langle \mathbf{ok}\rangle^{\sigma}$. First consider an allocated abstraction $\lambda^{\ell} x.\, P$ in $\mathsf{W}\langle \mathbf{ok}\rangle^{\sigma}$. Then $\mathsf{W}\langle \mathbf{ok}\rangle = \mathsf{C}\langle \lambda^{\ell} x.\, P'\rangle$ such that $P'^{\sigma} = P$. Note that P' has no variables bound by C, so P'^{σ} also has no variables bound by C, given that substitution is capture-avoiding, and σ is coherent.
   Consider moreover any two allocated abstractions $\lambda^{\ell} x.\, P$ and $\lambda^{\ell} x.\, Q$, in $\mathsf{W}\langle \mathbf{ok}\rangle^{\sigma}$ such that they have the same location, and consider three cases depending on the positions of the lambdas:
   3.1 If the lambdas are both in W, then their bodies trace back to the term on the left-hand side, $\lambda^{\ell} x.\, P_0$ and $\lambda^{\ell} x.\, Q_0$, so $P_0 = Q_0$ are equal by hypothesis, and moreover $P = {P_0}^{\sigma} = {Q_0}^{\sigma} = Q$, as required.

3.2 If one lambda is in W and the other one in $\sigma(y)$ for some variable $y \in \mathsf{fv}(\mathsf{W}\langle\mathbf{ok}\rangle)$, suppose without loss of generality that the position of the lambda of $\lambda^{\ell}x.\,P$ is inside W. Then there is an abstraction $\lambda^{\ell}x.\,P_0$ in the term of the left-hand side of the rule such that $P = P_0{}^{\sigma}$. Moreover, $\lambda^{\ell}x.\,Q$ is an abstraction of the term $\sigma(y)$. By Thm. A.1.3, there must be an abstraction $\lambda^{\ell}x.\,Q_0$ of $\mathtt{v} \overset{\bullet}{=} \mathtt{w}$ such that, moreover, $Q_0{}^{\sigma} = Q$. Then since $\lambda^{\ell}x.\,P_0$ and $\lambda^{\ell}x.\,Q_0$ are abstractions on the left-hand side, we have by hypothesis that $P_0 = Q_0$, hence $P = P_0{}^{\sigma} = Q_0{}^{\sigma} = Q$, as required.

3.3 If the lambdas are in the terms $\sigma(y)$ and $\sigma(z)$, for certain variables $y, z \in \mathsf{fv}(\mathsf{W}\langle\mathbf{ok}\rangle)$, then by Thm. A.1.3, there must terms $\lambda^{\ell}x.\,P_0$ and $\lambda^{\ell}x.\,Q_0$ each of which is an abstraction of $\mathtt{v} \overset{\bullet}{=} \mathtt{w}$, and such that moreover $P_0{}^{\sigma} = P$ and $Q_0{}^{\sigma} = Q$. Then since $\lambda^{\ell}x.\,P_0$ and $\lambda^{\ell}x.\,Q_0$ are abstractions on the left-hand side, we have by hypothesis that $P_0 = Q_0$, hence $P = P_0{}^{\sigma} = Q_0{}^{\sigma} = Q$, as required.

A.4 Proof of Lem. 3.3 — Reduction modulo structural equivalence

Lemma A.1. *Basic properties of structural equivalence The following properties hold:*

1. $P \oplus Q \equiv Q \oplus P$
2. *If* $P \equiv P'$ *then* $Q_1 \oplus P \oplus Q_2 \equiv Q_1 \oplus P' \oplus Q_2$

Proof. Straightforward, by induction on the derivation of the corresponding equivalences.

We turn to the proof of Lem. 3.3:

Proof. By induction on the derivation of $P \equiv P'$. The reflexivity and transitivity cases are immediate. Moreover, it is easy to check that the axioms are symmetric. So it suffices to show that the property holds when $P \equiv P'$ is derived using one of the axioms:

1. $\equiv$-`swap`: Let $t \to Q$. The situation is:

$$\begin{array}{ccc} P_1 \oplus t \oplus s \oplus P_2 & \equiv & P_1 \oplus s \oplus t \oplus P_2 \\ \downarrow & & \downarrow \\ P_1 \oplus Q \oplus s \oplus P_2 & \equiv & P_1 \oplus s \oplus Q \oplus P_2 \end{array}$$

   The equivalence at the bottom is justified by Lem. A.1.
2. $\equiv$-`var`: Let $t \to Q$, $z \notin \mathsf{fv}(t)$. Then we argue that $t\{y := z\} \to Q\{y := z\} \equiv Q$. By case analysis on the reduction rule applied.

   2.1 `alloc`: The situation is:

$$\begin{array}{ccc} P_1 \oplus \mathsf{W}\langle\lambda x.\,P\rangle \oplus P_2 & \equiv & P_1 \oplus \mathsf{W}\{y := z\}\langle\lambda x.\,P\{y := z\}\rangle \oplus P_2 \\ \downarrow & & \downarrow \\ P_1 \oplus \mathsf{W}\langle\lambda^{\ell}x.\,P\rangle \oplus P_2 & \equiv & P_1 \oplus \mathsf{W}\{y := z\}\langle\lambda^{\ell'}x.\,P\{y := z\}\rangle \oplus P_2 \end{array}$$

   For the equivalence at the bottom is justified using $\equiv$-`var` to rename y to z, and $\equiv$-`loc` if necessary to rename ℓ to ℓ'.

2.2 `beta`: The situation is:

$$\begin{array}{ccc}
P_1 \oplus \mathsf{W}\langle(\lambda^\ell x.\, P)\,\mathtt{v}\rangle \oplus P_2 & \equiv & P_1 \oplus \mathsf{W}\{y := z\}\langle(\lambda^\ell x.\, P\{y := z\})\,\mathtt{v}\{y := z\}\rangle \oplus P_2 \\
\downarrow & & \downarrow \\
P_1 \oplus \mathsf{W}\langle P\{x := \mathtt{v}\}\rangle \oplus P_2 & \equiv & P_1 \oplus \mathsf{W}\{y := z\}\langle P\{x := \mathtt{v}\}\{y := z\}\rangle \oplus P_2
\end{array}$$

For the equivalence at the bottom, note that by Lem. A.1, $P\{x := \mathtt{v}\}\{y := z\} = P\{y := z\}\{x := \mathtt{v}\{y := z\}\}$.

2.3 `guard`: This case is straightforward.

2.4 `fresh`: The situation is:

$$\begin{array}{ccc}
P_1 \oplus \mathsf{W}\langle \nu x.\, t\rangle \oplus P_2 & \equiv & P_1 \oplus \mathsf{W}\{y := z\}\langle \nu x.\, t\{y := z\}\rangle \oplus P_2 \\
\downarrow & & \downarrow \\
P_1 \oplus \mathsf{W}\langle t\rangle \oplus P_2 & \equiv & P_1 \oplus \mathsf{W}\{y := z\}\langle t\{y := z\}\rangle \oplus P_2
\end{array}$$

Note that assume $x \neq y$ by Barendregt's variable convention.

2.5 `unif`: Let $\mathsf{mgu}(\mathtt{v} \stackrel{\bullet}{=} \mathtt{w}) = \sigma$. Then $\sigma' := (z \mapsto y)\cdot\sigma$ is an idempotent most general unifier of the single goal $\mathtt{v}\{y := z\} \stackrel{\bullet}{=} \mathtt{w}\{y := z\}$ by Lem. A.1. So $\sigma'' = \mathsf{mgu}(\mathtt{v}\{y := z\} \stackrel{\bullet}{=} \mathtt{w}\{y := z\})$ exists and $\sigma'' = \sigma' \cdot \rho = (z \mapsto y)\cdot\sigma\cdot\rho$ for some renaming ρ.

$$\begin{array}{ccc}
P_1 \oplus \mathsf{W}\langle \mathtt{v} \stackrel{\bullet}{=} \mathtt{w}\rangle \oplus P_2 & \equiv & P_1 \oplus \mathsf{W}\{y := z\}\langle \mathtt{v}\{y := z\} \stackrel{\bullet}{=} \mathtt{w}\{y := z\}\rangle \oplus P_2 \\
\Big\downarrow & & \downarrow \\
 & & P_1 \oplus \mathsf{W}\{y := z\}\langle \mathbf{ok}\rangle^{\sigma''} \oplus P_2 \\
\Big\downarrow & & \Vert \\
P_1 \oplus \mathsf{W}\langle \mathbf{ok}\rangle^{\sigma} \oplus P_2 & \equiv & P_1 \oplus \mathsf{W}\langle \mathbf{ok}\rangle^{\sigma\cdot\rho} \oplus P_2
\end{array}$$

The equivalence at the bottom may be deduced by repeatedly applying the $\equiv$-`var` rule to perform the renaming ρ.

2.6 `fail`: Suppose that $\mathsf{mgu}(\mathtt{v} \stackrel{\bullet}{=} \mathtt{w})$ fails. Then $\mathsf{mgu}(\mathtt{v}\{y := z\} \stackrel{\bullet}{=} \mathtt{w}\{y := z\})$ must also fail, for if σ were a unifier of $(\mathtt{v}\{y := z\} \stackrel{\bullet}{=} \mathtt{w}\{y := z\})$ then $(y \mapsto z)\cdot\sigma$ would be a unifier of $\mathtt{v} \stackrel{\bullet}{=} \mathtt{w}$ by Lem. A.1. So we have:

$$\begin{array}{ccc}
P_1 \oplus \mathsf{W}\langle \mathtt{v} \stackrel{\bullet}{=} \mathtt{w}\rangle \oplus P_2 & \equiv & P_1 \oplus \mathsf{W}\{y := z\}\langle \mathtt{v}\{y := z\} \stackrel{\bullet}{=} \mathtt{w}\{y := z\}\rangle \oplus P_2 \\
\downarrow & & \downarrow \\
P_1 \oplus P_2 & \equiv & P_1 \oplus P_2
\end{array}$$

3. $\equiv$-`loc`: If the $\equiv$-`loc` rule and the rewriting rule are applied on different threads, it is straightforward. Otherwise we proceed by case analysis on the reduction rule applied:

3.1 `alloc`: Let us write $\mathsf{W}' := \mathsf{W}\{\ell_1 := \ell_2\}$ and $Q' := Q\{\ell_1 := \ell_2\}$. Then:

$$\begin{array}{ccc}
P_1 \oplus \mathsf{W}\langle \lambda x.\, Q\rangle \oplus P_2 & \equiv & P_1 \oplus \mathsf{W}'\langle \lambda x.\, Q'\rangle \oplus P_2 \\
\downarrow & & \downarrow \\
P_1 \oplus \mathsf{W}\langle \lambda^\ell x.\, Q\rangle \oplus P_2 & \equiv & P_1 \oplus \mathsf{W}'\langle \lambda^{\ell'} x.\, Q'\rangle \oplus P_2
\end{array}$$

The equivalence on the bottom may be deduced by applying the $\equiv$-`loc` rule to rename ℓ_1 to ℓ_2, and possibly the $\equiv$-`loc` again to rename ℓ to ℓ'. Note that there is no possibility of conflict because ℓ and ℓ' are fresh.

3.2 `beta`: Let us write $\mathsf{W}' := \mathsf{W}\{\ell_1 := \ell_2\}$, $Q' := Q\{\ell_1 := \ell_2\}$, and $\mathtt{v}' := \mathtt{v}\{\ell_1 := \ell_2\}$. Then we have:

$$\begin{tikzcd} P_1 \oplus \mathsf{W}\langle(\lambda^{\ell} x.\, Q)\,\mathtt{v}\rangle \oplus P_2 \arrow[d] & \equiv & P_1 \oplus \mathsf{W}'\langle(\lambda^{\ell\{\ell_1:=\ell_2\}} x.\, Q')\,\mathtt{v}'\rangle \oplus P_2 \arrow[d] \\ P_1 \oplus \mathsf{W}\langle Q\{x := \mathtt{v}\}\rangle \oplus P_2 & \equiv & P_1 \oplus \mathsf{W}'\langle Q'\{x := \mathtt{v}'\}\rangle \oplus P_2 \end{tikzcd}$$

The equivalence on the bottom may be deduced by repeatedly applying the $\equiv$-`loc` rule.

3.3 `guard`: This case is straightforward.

3.4 `fresh`: This case is straightforward.

3.5 `unif`: Consider a thread of the form $\mathsf{W}\langle \mathtt{v} \overset{\bullet}{=} \mathtt{w}\rangle$, and suppose that $\sigma = \mathsf{mgu}(\mathtt{v} \overset{\bullet}{=} \mathtt{w})$ exists. Let us write $\mathsf{W}' := \mathsf{W}\{\ell := \ell'\}$, $\mathtt{v}' := \mathtt{v}\{\ell := \ell'\}$, and $\mathtt{w}' := \mathtt{w}\{\ell := \ell'\}$. By Lem. A.1, the substitution σ' given by $\sigma'(x) = \sigma(x)\{\ell := \ell'\}$ is an idempotent most general unifier of $\{\mathtt{v}' \overset{\bullet}{=} \mathtt{w}'\}$ so $\sigma'' = \mathsf{mgu}(\mathtt{v}' \overset{\bullet}{=} \mathtt{w}')$ exists and moreover, by Lem. A.1, we have $\sigma'' = \sigma' \cdot \rho$ for some renaming ρ. Note that $\mathsf{W}'\langle\mathbf{ok}\rangle^{\sigma'} = \mathsf{W}\langle\mathbf{ok}\rangle^{\sigma}\{\ell := \ell'\}$; so:

$$\begin{tikzcd} P_1 \oplus \mathsf{W}\langle \mathtt{v} \overset{\bullet}{=} \mathtt{w}\rangle \oplus P_2 \arrow[dd] & \equiv & P_1 \oplus \mathsf{W}'\langle \mathtt{v}' \overset{\bullet}{=} \mathtt{w}'\rangle \oplus P_2 \arrow[d] \\ & & P_1 \oplus \mathsf{W}'\langle\mathbf{ok}\rangle^{\sigma'\cdot\rho} \oplus P_2 \arrow[d, equal] \\ P_1 \oplus \mathsf{W}\langle\mathbf{ok}\rangle^{\sigma} \oplus P_2 & \equiv & P_1 \oplus \mathsf{W}\langle\mathbf{ok}\rangle^{\sigma}\{\ell := \ell'\}^{\rho} \oplus P_2 \end{tikzcd}$$

The equivalence at the bottom may be deduced applying the $\equiv$-`loc` rule to rename ℓ to ℓ' and then repeatedly applying the $\equiv$-`var` rule to perform the renaming ρ.

3.6 `fail`: Consider a thread of the form $\mathsf{W}\langle \mathtt{v} \overset{\bullet}{=} \mathtt{w}\rangle$, and let us write $\mathsf{W}' := \mathsf{W}\{\ell := \ell'\}$, $\mathtt{v}' := \mathtt{v}\{\ell := \ell'\}$, and $\mathtt{w}' := \mathtt{w}\{\ell := \ell'\}$. Suppose moreover that $\mathsf{mgu}(\mathtt{v} \overset{\bullet}{=} \mathtt{w})$ fails. Then $\mathsf{mgu}(\mathtt{v}' \overset{\bullet}{=} \mathtt{w}')$ must also fail, for if σ were a unifier of $\mathtt{v}' \overset{\bullet}{=} \mathtt{w}'$, the substitution σ' given by $\sigma'(x) = \sigma(x)\{\ell' := \ell\}$ would be a unifier of $\mathtt{v} \overset{\bullet}{=} \mathtt{w}$. Hence:

$$\begin{tikzcd} P_1 \oplus \mathsf{W}\langle \mathtt{v} \overset{\bullet}{=} \mathtt{w}\rangle \oplus P_2 \arrow[d] & \equiv & P_1 \oplus \mathsf{W}'\langle \mathtt{v}' \overset{\bullet}{=} \mathtt{w}'\rangle \oplus P_2 \arrow[d] \\ P_1 \oplus P_2 & \equiv & P_1 \oplus P_2 \end{tikzcd}$$

A.5 Proof of Prop. 4.1 — Characterization of Normal Forms

Lemma A.1 (Values are irreducible). *If* $\mathtt{v}$ *is a value, then it is a normal form.*

Proof. Straightforward by induction on $\mathtt{v}$.

Lemma A.2 (Application of a stuck term). *If S is stuck and $t^\star$ is a normal term, then $S\,t^\star$ is stuck.*

Proof. Straightforward by case analysis on the derivation of the judgment "$S\triangledown$".

Lemma A.3 (Values and stuck terms are disjoint). *A stuck term S is not a value.*

Proof. By induction on the derivation of the judgment "$S\triangledown$". First, note that if $S = x\,t_1^\star \dots t_n^\star$ is stuck, it cannot be value because $n > 0$. Second, note that if $S = \mathbf{c}\,t_1^\star \dots t_n^\star$ is stuck, it cannot be value because by *i.h.* there is an i such that $t_i^\star$ is not a value. In the remaining cases, we have either $S = (t_1^\star; t_2^\star)\,s_1^\star \dots s_n^\star$, $S = (t_1^\star \overset{\bullet}{=} t_2^\star)\,s_1^\star \dots s_n^\star$ or $S = (\lambda^\ell x.\,P)\,t^\star\,s_1^\star \dots s_n^\star$, so the term S is clearly not a value.

We turn to the proof of Prop. 4.1. We prove the two inclusions. For the ($\subseteq$) inclusion, by induction on a given normal program, it suffices to show that any normal term $t^\star$ is a $\rightarrow$-normal form, which can be seen by induction on the derivation that $t^\star$ is a normal term. Recall that values are $\rightarrow$-normal forms (Lem. A.1) so we are left to check that any stuck term is a $\rightarrow$-normal form. If $t^\star$ is stuck, it is straightforward to check, in each case of the definition of the judgment $t^\star\triangledown$, that the resulting term has no $\rightarrow$-redexes. Using the fact that a stuck term S cannot be a value (Lem. A.3), the key remarks are that:

1. `stuck-guard`: $t_1^\star; t_2^\star$ cannot be a $\xrightarrow{\mathtt{guard}}$-redex because $t_1^\star$ is stuck (hence not a value);
2. `stuck-unif`: $t_1^\star \overset{\bullet}{=} t_2^\star$ cannot be a $\xrightarrow{\mathtt{unif}}$-redex nor a $\xrightarrow{\mathtt{fail}}$-redex because for some $i \in \{1, 2\}$ the term $t_i^\star$ is stuck (hence not a value);
3. `stuck-lam`: $(\lambda^\ell x.\,P)\,t^\star$ cannot be a $\xrightarrow{\mathtt{beta}}$-redex because the term $t^\star$ is stuck (hence not a value).

For the ($\supseteq$) inclusion, by induction on a given program, it suffices to show that any term t in $\rightarrow$-normal form is actually a normal term. By induction on t:

1. *Variable, $t = x$.* Then t is a value.
2. *Constructor, $t = \mathbf{c}$.* Then t is a value.
3. *Fresh variable declaration, $t = \nu x.\,s$.* Impossible, as it is not a $\rightarrow$-normal form.
4. *Abstraction code, $t = \lambda x.\,s$.* Impossible, as it is not a $\rightarrow$-normal form.
5. *Allocated abstraction, $t = \lambda^\ell x.\,s$.* Then t is a value.
6. *Application, $t = s\,u$.* Note that s and u are $\rightarrow$-normal forms. By *i.h.*, s and u are normal terms, that is they are either a value or a stuck term. We consider the following four cases, depending on the shape of s:
   6.1 If $s = x$, then $x\,u$ is stuck by `stuck-var`.
   6.2 If $s = \mathbf{c}\mathtt{v}_1 \dots \mathtt{v}_n$, then:
      6.2.1 If u is a value, $\mathbf{c}\,\mathtt{v}_1 \dots \mathtt{v}_n\,u$ is a value.

6.2.2 If u is stuck, $\mathbf{c}\,\mathtt{v}_1 \ldots \mathtt{v}_n\, u$ is stuck by `stuck-cons`.

6.3 If $s = \lambda^\ell x.\, P$ then:

6.3.1 If u is a value, this case is impossible because $(\lambda^\ell x.\, P)\, u$ has a $\xrightarrow{\mathtt{beta}}$-redex.

6.3.2 If u is stuck, then $(\lambda^\ell x.\, P)\, u$ is stuck by `stuck-lam`.

6.4 If s is stuck, then $s\, u$ is stuck by Lem. A.2.

7. *Guarded expression,* $t = (s; u)$. Note that s and u are $\rightarrow$-normal forms. By *i.h.*, s and u are normal terms, that is they are either a value or a stuck term. Note that s cannot be a value, because $s; u$ would have a $\xrightarrow{\mathtt{guard}}$-redex, so s is stuck and $s; u$ is stuck by `stuck-guard`.
8. *Unification,* $t = (s \overset{\bullet}{=} u)$. Note that s and u are $\rightarrow$-normal forms. By *i.h.*, s and u are normal terms, that is they are either a value or a stuck term. Note that s and u cannot both be values, because $s \overset{\bullet}{=} u$ would have either a $\xrightarrow{\mathtt{unif}}$-redex (if $\mathsf{mgu}(s \overset{\bullet}{=} u)$ exists) or a $\xrightarrow{\mathtt{unif}}$-redex (if $\mathsf{mgu}(s \overset{\bullet}{=} u)$ fails). So either s is stuck or u is stuck, so we have that $s \overset{\bullet}{=} u$ is stuck by `stuck-unif`.

A.6 Proof of Lem. 4.2, item 3. — Simultaneous reduction modulo structural equivalence

Lemma A.1 (Goals in a simultaneous reduction are in the term). *Let* $t \overset{\mathsf{G}}{\Rightarrow} P$. *Then* G *is a subset of the set:*

$$\{\mathtt{v} \overset{\bullet}{=} \mathtt{w} \mid \exists \mathsf{W}.\ t = \mathsf{W}\langle \mathtt{v} \overset{\bullet}{=} \mathtt{w}\rangle\}$$

In particular, $\mathsf{fv}(\mathsf{G}) \subseteq \mathsf{fv}(t)$ *and* $\mathsf{locs}(\mathsf{G}) \subseteq \mathsf{locs}(t)$.

Proof. Straightforward by induction on the derivation of $t \overset{\mathsf{G}}{\Rightarrow} P$.

Lemma A.2 (Simultaneous evaluation of an alternative). *The following are equivalent:*

1. $P \oplus Q \Rightarrow R$
2. R *can be written as* $P' \oplus Q'$, *where* $P \Rightarrow P'$ *and* $Q \Rightarrow Q'$.

Proof. Straightforward, by induction on P.

Lemma A.3 (Action of renaming on simultaneous evaluation).

1. *If* $t \overset{\mathsf{G}}{\Rightarrow} P$ *then* $t\{x := y\} \xRightarrow{\mathsf{G}\{x:=y\}} P\{x := y\}$.
2. *If* $t \overset{\mathsf{G}}{\Rightarrow} P$ *then* $t\{\ell := \ell'\} \xRightarrow{\mathsf{G}\{\ell:=\ell'\}} P\{\ell := \ell'\}$.

Proof. Straightforward by induction on the derivation of $t \overset{\mathsf{G}}{\Rightarrow} P$.

We turn to the proof of Lem. 4.2, item 3:

Proof. By induction on the derivation of $P \equiv P'$. It suffices to show that the property holds when $P \equiv P'$ is derived using one of the axioms:

1. $\equiv$-`swap`: The situation is

$$\begin{array}{ccc} P_1 \oplus t_1 \oplus t_2 \oplus P_2 & \equiv & P_1 \oplus t_2 \oplus t_1 \oplus P_2 \\ \Downarrow & & \Downarrow \\ P_1' \oplus Q_1 \oplus Q_2 \oplus P_2' & \equiv & P_1' \oplus Q_2 \oplus Q_1 \oplus P_2' \end{array}$$

   where by Lem. A.2 we have that $P_1 \Rightarrow P_1'$, $t_1 \Rightarrow Q_1$, $t_2 \Rightarrow Q_2$, and $P_2 \Rightarrow P_2'$. The equivalence at the bottom is justified by Lem. A.1.
2. $\equiv$-`var`: Consider a program of the form $P_1 \oplus t \oplus P_2$, and let $y \notin \mathsf{fv}(t)$. Moreover, suppose that $P_1 \oplus t \oplus P_2 \Rightarrow R$. By Lem. A.2 we have that $R = P_1' \oplus Q \oplus P_2'$ where $P_1 \Rightarrow P_1'$, $t \Rightarrow Q$, and $P_2 \Rightarrow P_2'$. The simultaneous reduction step $t \Rightarrow Q$ is deduced from $t \overset{\mathsf{G}}{\Rightarrow} Q'$ for some set of goals G, in such a way that:

$$Q = \begin{cases} Q'^{\sigma} & \text{if } \sigma = \mathsf{mgu}(\mathsf{G}) \\ \mathtt{fail} & \text{if } \mathsf{mgu}(\mathsf{G}) \text{ fails} \end{cases}$$

   By Lem. A.3, this means that $t\{x := y\} \xRightarrow{\mathsf{G}\{x:=y\}} Q'\{x := y\}$. Note that $\mathsf{fv}(\mathsf{G}) \subseteq \mathsf{fv}(t)$ by Lem. A.1, so in particular $y \notin \mathsf{fv}(\mathsf{G})$. This implies by Lem. A.1 that $\sigma = \mathsf{mgu}(\mathsf{G})$ exists if and only if $\sigma' = \mathsf{mgu}(\mathsf{G}\{x := y\})$ exists.
   If $\sigma = \mathsf{mgu}(\mathsf{G})$ exists, moreover by Lem. A.1 we have that $\sigma' = (y \mapsto x) \cdot \sigma \cdot \rho$ for some renaming ρ, and the situation is:

$$\begin{array}{ccc} P_1 \oplus t \oplus P_2 & \equiv & P_1 \oplus t\{x := y\} \oplus P_2 \\ \Bigg\Downarrow & & \Downarrow \\ & & P_1 \oplus Q'\{x := y\}^{(y\mapsto x)\cdot\sigma\cdot\rho} \oplus P_2 \\ & & \Vert \\ P_1 \oplus Q'^{\sigma} \oplus P_2 & \equiv & P_1 \oplus (Q'^{\sigma})^{\rho} \oplus P_2 \end{array}$$

   The equivalence at the bottom is justified using $\equiv$-`var` to apply the renaming ρ. If $\mathsf{mgu}(\mathsf{G})$ fails, the situation is:

$$\begin{array}{ccc} P_1 \oplus t \oplus P_2 & \equiv & P_1 \oplus t\{x := y\} \oplus P_2 \\ \Downarrow & & \Downarrow \\ P_1 \oplus P_2 & \equiv & P_1 \oplus P_2 \end{array}$$

3. $\equiv$-`loc`: Similar as the previous case. Let $\ell' \notin \mathsf{locs}(t)$. By Lem. A.3 we may conclude that if $t \overset{\mathsf{G}}{\Rightarrow} Q'$ then $t\{\ell := \ell'\} \xRightarrow{\mathsf{G}\{\ell:=\ell'\}} Q'\{\ell := \ell'\}$. Note that $\mathsf{locs}(\mathsf{G}) \subseteq \mathsf{locs}(t)$ by Lem. A.1, so in particular $\ell' \notin \mathsf{fv}(\mathsf{G})$. This implies by Lem. A.1 that $\sigma = \mathsf{mgu}(\mathsf{G})$ exists if and only if $\sigma' = \mathsf{mgu}(\mathsf{G}\{\ell := \ell'\})$ exists. If $\sigma = \mathsf{mgu}(\mathsf{G})$ exists, moreover by Lem. A.1 we have that $\sigma' = \sigma'' \cdot \rho$ where ρ is a renaming, and σ'' is a substitution such that $\sigma''(x) = \sigma(x)\{\ell := \ell'\}$.

Hence the situation is:

$$\begin{array}{ccc}
P_1 \oplus t \oplus P_2 & \equiv & P_1 \oplus t\{\ell := \ell'\} \oplus P_2 \\
\Big\Downarrow & & \Downarrow \\
 & & P_1 \oplus Q'\{\ell := \ell'\}^{\sigma''\cdot\rho} \oplus P_2 \\
 & & \| \\
P_1 \oplus Q'^{\sigma} \oplus P_2 & \equiv & P_1 \oplus Q'^{\sigma}\{\ell := \ell'\}^{\rho} \oplus P_2
\end{array}$$

The equivalence at the bottom is justified using $\equiv$-`loc` to rename ℓ to ℓ', and $\equiv$-`var` to apply the renaming ρ. If $\mathsf{mgu}(\mathsf{G})$ fails, the situation is:

$$\begin{array}{ccc}
P_1 \oplus t \oplus P_2 & \equiv & P_1 \oplus t\{x := y\} \oplus P_2 \\
\Downarrow & & \Downarrow \\
P_1 \oplus P_2 & \equiv & P_1 \oplus P_2
\end{array}$$

A.7 Proof of Prop. 4.3 — Tait–Martin-Löf's Technique

For the proofs, we work with the following `Thread` rule and the following variant of the `Alt` rule, which is obviously equivalent to the one in the main body of the paper:

$$\frac{t \overset{\mathsf{G}}{\Rightarrow} P \qquad P' = \begin{cases} P^{\sigma} & \text{if } \sigma = \mathsf{mgu}(\mathsf{G}) \\ \mathtt{fail} & \text{if } \mathsf{mgu}(\mathsf{G}) \text{ fails} \end{cases}}{t \Rightarrow P'}\ \mathtt{Thread} \qquad \frac{t \Rightarrow P \qquad Q \Rightarrow Q'}{t \oplus Q \Rightarrow P \oplus Q'}\ \mathtt{Alt'}$$

Lemma A.1 ("$\to\ \subseteq\ \Rightarrow\equiv$"). *If $t \to P$ then $t \Rightarrow\equiv P$.*

Proof. By case analysis on the rule used to conclude $t \to P$.

1. `alloc`: $\mathsf{W}\langle\lambda x.\,P\rangle \to \mathsf{W}\langle\lambda^{\ell} x.\,P\rangle$ for some location $\ell \notin \mathsf{locs}(\mathsf{W}\langle\lambda x.\,P\rangle)$. Note that $\lambda x.\,P \overset{\varnothing}{\Rightarrow} \lambda^{\ell'} x.\,P$ for an (a priori different) fresh location ℓ' by rule $\mathtt{Abs}_2^{\mathsf{C}}$. By context closure (Lem. 4.2), applying the `Thread` rule once, we have that $\mathsf{W}\langle\lambda x.\,P\rangle \Rightarrow \mathsf{W}\langle\lambda^{\ell'} x.\,P\rangle \equiv \mathsf{W}\langle\lambda^{\ell} x.\,P\rangle$ as required. The last equivalence is justified renaming ℓ' to ℓ.
2. `beta`: $\mathsf{W}\langle(\lambda^{\ell} x.\,P)\,\mathtt{v}\rangle \to \mathsf{W}\langle P\{x := \mathtt{v}\}\rangle$. Note that $(\lambda^{\ell} x.\,P)\,\mathtt{v} \overset{\varnothing}{\Rightarrow} P\{x := \mathtt{v}\}$ by rule $\mathtt{App}_2$, so by context closure (Lem. 4.2), applying the `Thread` rule once, we conclude.
3. `fresh`: $\mathsf{W}\langle\nu x.\,t\rangle \to \mathsf{W}\langle t\{x := y_1\}\rangle$ for some variable $y_1 \notin \mathsf{fv}(\mathsf{W})$. Note that $\nu x.\,t \overset{\varnothing}{\Rightarrow} t\{x := y_2\}$ for an (a priori different) fresh variable y_2 by rule $\mathtt{Fresh}_2$. By context closure (Lem. 4.2), applying the `Thread` rule once, we have that $\mathsf{W}\langle\nu x.\,t\rangle \Rightarrow \mathsf{W}\langle t\{x := y_2\}\rangle \equiv \mathsf{W}\langle t\{x := y_1\}\rangle$ The last equivalence is justified renaming y_2 to y_1.
4. `guard`: $\mathsf{W}\langle\mathtt{v};t\rangle \to \mathsf{W}\langle t\rangle$. Note that $\mathtt{v};t \overset{\varnothing}{\Rightarrow} t$ by rule $\mathtt{Guard}_2$. By context closure (Lem. 4.2), applying the `Thread` rule once, we have that $\mathsf{W}\langle\mathtt{v};t\rangle \Rightarrow \mathsf{W}\langle t\rangle$ as required.

5. $\mathtt{unif}$: Suppose that $\sigma = \mathsf{mgu}(\mathtt{v} \stackrel{\bullet}{=} \mathtt{w})$, and let $\mathsf{W}\langle \mathtt{v} \stackrel{\bullet}{=} \mathtt{w} \rangle \to \mathsf{W}\langle \mathbf{ok} \rangle^{\sigma}$. Note that $\mathtt{v} \stackrel{\bullet}{=} \mathtt{w} \xRightarrow{\{\mathtt{v} \stackrel{\bullet}{=} \mathtt{w}\}} \mathbf{ok}$ by rule $\mathtt{Unif}_2$, so by context closure and applying the $\mathtt{Thread}$ rule once we have that $\mathsf{W}\langle \mathtt{v} \stackrel{\bullet}{=} \mathtt{w} \rangle \Rightarrow \mathsf{W}\langle \mathbf{ok} \rangle^{\sigma}$, as required.
6. $\mathtt{fail}$: Suppose that $\mathsf{mgu}(\mathtt{v} \stackrel{\bullet}{=} \mathtt{w})$ fails, and let $\mathsf{W}\langle \mathtt{v} \stackrel{\bullet}{=} \mathtt{w} \rangle \to \mathsf{W}\langle \mathbf{ok} \rangle^{\sigma}$. Note that $\mathtt{v} \stackrel{\bullet}{=} \mathtt{w} \xRightarrow{\{\mathtt{v} \stackrel{\bullet}{=} \mathtt{w}\}} \mathbf{ok}$ by rule $\mathtt{Unif}_2$, so by context closure and applying the $\mathtt{Thread}$ rule once we have that $\mathsf{W}\langle \mathtt{v} \stackrel{\bullet}{=} \mathtt{w} \rangle \Rightarrow \mathtt{fail}$, as required.

Lemma A.2 ("$\Rightarrow\ \subseteq\ \twoheadrightarrow\equiv$"). *Let $t \stackrel{\mathsf{G}}{\Rightarrow} P$. Given any weak context W and any substitution α we have:*

1. *If $\sigma = \mathsf{mgu}(\mathsf{G}^{\alpha})$, then $\mathsf{W}\langle t \rangle^{\alpha} \twoheadrightarrow\equiv \mathsf{W}\langle P \rangle^{\alpha\cdot\sigma}$.*
2. *If $\mathsf{mgu}(\mathsf{G}^{\alpha})$ fails, then $\mathsf{W}\langle t \rangle^{\alpha} \twoheadrightarrow\equiv \mathtt{fail}$.*

Proof. By induction on the derivation of $t \stackrel{\mathsf{G}}{\Rightarrow} P$:

1. $\mathtt{Var}$: Note that $\mathsf{mgu}(\varnothing)$ is the identity substitution, so $\mathsf{W}\langle x \rangle^{\alpha} \twoheadrightarrow \mathsf{W}\langle x \rangle^{\alpha}$ in zero steps.
2. $\mathtt{Cons}$: Immediate, similar to the $\mathtt{Var}$ case.
3. $\mathtt{Fresh}_1$: Immediate, similar to the $\mathtt{Var}$ case.
4. $\mathtt{Fresh}_2$: Let $\nu x.\, t \stackrel{\mathsf{G}}{\Rightarrow} P$ be derived from $t \stackrel{\mathsf{G}}{\Rightarrow} P$, where x is a fresh variable. Moreover, let $x' \notin \mathsf{fv}(\mathsf{W}^{\alpha})$. Then we have that:

$$\mathsf{W}\langle \nu x.\, t \rangle^{\alpha} = \mathsf{W}^{\alpha}\langle \nu x'.\, t\{x := x'\}^{\alpha} \rangle \xrightarrow{\mathtt{fresh}} \mathsf{W}^{\alpha}\langle t\{x := x'\}^{\alpha} \rangle = \mathsf{W}\langle t\{x := x'\} \rangle^{\alpha} \equiv \mathsf{W}\langle t \rangle^{\alpha}$$

   There are two subcases, depending on whether $\mathsf{mgu}(\mathsf{G}^{\alpha})$ exists:
   4.1 If $\sigma = \mathsf{mgu}(\mathsf{G}^{\alpha})$, then by *i.h.*, $\mathsf{W}\langle t \rangle^{\alpha} \twoheadrightarrow\equiv \mathsf{W}\langle P \rangle^{\alpha\cdot\sigma}$, so since $\equiv$ is a strong bisimulation (Lem. 3.3), $\mathsf{W}\langle \nu x.\, t \rangle^{\alpha} \twoheadrightarrow\equiv \mathsf{W}\langle P \rangle^{\alpha\cdot\sigma}$ as required.
   4.2 If $\mathsf{mgu}(\mathsf{G}^{\alpha})$ fails, then by *i.h.*, $\mathsf{W}\langle t \rangle^{\alpha} \twoheadrightarrow\equiv \mathtt{fail}$, so since $\equiv$ is a strong bisimulation (Lem. 3.3), $\mathsf{W}\langle \nu x.\, t \rangle^{\alpha} \twoheadrightarrow\equiv \mathtt{fail}$ as required.
5. $\mathtt{Abs}^{\mathtt{C}}_1$: Immediate, similar to the $\mathtt{Var}$ case.
6. $\mathtt{Abs}^{\mathtt{C}}_2$: Let $\lambda x.\, P \stackrel{\varnothing}{\Rightarrow} \lambda^{\ell} x.\, P$, where ℓ is a fresh location. Moreover, let $\ell' \notin \mathsf{locs}(\mathsf{W}\langle \lambda x.\, P \rangle^{\alpha})$. Then:

$$\mathsf{W}\langle \lambda x.\, P \rangle^{\alpha} = \mathsf{W}^{\alpha}\langle \lambda x.\, P^{\alpha} \rangle \xrightarrow{\mathtt{alloc}} \mathsf{W}^{\alpha}\langle \lambda^{\ell'} x.\, P^{\alpha} \rangle \equiv \mathsf{W}^{\alpha}\langle \lambda^{\ell} x.\, P^{\alpha} \rangle = \mathsf{W}\langle \lambda^{\ell} x.\, P \rangle^{\alpha}$$

   so $\mathsf{W}\langle \lambda x.\, P \rangle^{\alpha} \twoheadrightarrow\equiv \mathsf{W}\langle \lambda^{\ell} x.\, P \rangle^{\alpha}$. Note that $\mathsf{mgu}(\varnothing)$ is the identity substitution, so we are done.
7. $\mathtt{Abs}^{\mathtt{A}}$: Immediate, similar to the $\mathtt{Var}$ case.
8. $\mathtt{App}_1$: Let $t\, s \xRightarrow{\mathsf{G} \cup \mathsf{H}} P\, Q$ be derived from $t \stackrel{\mathsf{G}}{\Rightarrow} P$ and $s \stackrel{\mathsf{H}}{\Rightarrow} Q$. We consider two subcases, depending on whether $\mathsf{mgu}(\mathsf{G}^{\alpha})$ exists:
   8.1 If $\sigma = \mathsf{mgu}(\mathsf{G}^{\alpha})$ exists. Let us write $P = \bigoplus_{i=1}^{n} t_i$. Then applying the *i.h.* for the term t under the weak context $\mathsf{W}\langle \Box\, s \rangle$, we have that $\mathsf{W}\langle t\, s \rangle^{\alpha} \twoheadrightarrow\equiv \mathsf{W}\langle P\, s \rangle^{\alpha\cdot\sigma} = \bigoplus_{i=1}^{n} \mathsf{W}\langle t_i\, s \rangle^{\alpha\cdot\sigma}$. We consider two further subcases, depending on whether $\mathsf{mgu}(\mathsf{H}^{\alpha\cdot\sigma})$ exists:

8.1.1 If $\rho = \mathsf{mgu}(\mathsf{H}^{\alpha\cdot\sigma})$ exists, then applying the *i.h.* for each $1 \leq i \leq n$, for the term s under the weak context $\mathsf{W}\langle t_i\,\Box\rangle$, we have that $\mathsf{W}\langle t_i\,s\rangle^{\alpha\cdot\sigma} \twoheadrightarrow\equiv \mathsf{W}\langle t_i\,Q\rangle^{\alpha\cdot\sigma\cdot\rho}$. Moreover, by the compositionality property (Lem. A.2) we have that $\tau = \mathsf{mgu}(\mathsf{G}^\alpha \cup \mathsf{H}^\alpha)$ exists, and it is a renaming of $\sigma\cdot\rho$. In summary, we have:

$$\begin{array}{rll} \mathsf{W}\langle t\,s\rangle^\alpha & \twoheadrightarrow\equiv \mathsf{W}\langle P\,s\rangle^{\alpha\cdot\sigma} & \text{by } \textit{i.h.} \text{ on } t \\ & = \bigoplus_{i=1}^n \mathsf{W}\langle t_i\,s\rangle^{\alpha\cdot\sigma} & \\ & \twoheadrightarrow\equiv \bigoplus_{i=1}^n \mathsf{W}\langle t_i\,Q\rangle^{\alpha\cdot\sigma\cdot\rho} & \text{by } \textit{i.h.} \text{ on } s \\ & = \mathsf{W}\langle P\,Q\rangle^{\alpha\cdot\sigma\cdot\rho} & \\ & \equiv \mathsf{W}\langle P\,Q\rangle^{\alpha\cdot\tau} & \end{array}$$

so since $\equiv$ is a strong bisimulation (Lem. 3.3), $\mathsf{W}\langle t\,s\rangle^\alpha \twoheadrightarrow\equiv \mathsf{W}\langle P\,Q\rangle^{\alpha\cdot\tau}$, as required.

8.1.2 If $\mathsf{mgu}(\mathsf{H}^{\alpha\cdot\sigma})$ fails, then applying the *i.h.* for each $1 \leq i \leq n$, for the term s under the weak context $\mathsf{W}\langle t_i\,s\rangle$, we have that $\mathsf{W}\langle t_i\,s\rangle^{\alpha\cdot\sigma} \twoheadrightarrow\equiv$ `fail`. Moreover, by the compositionality property (Lem. A.2) we have that $\mathsf{mgu}(\mathsf{G}^\alpha \cup \mathsf{H}^\alpha)$ also fails, so we have:

$$\begin{array}{rll} \mathsf{W}\langle t\,s\rangle^\alpha & \twoheadrightarrow\equiv \mathsf{W}\langle P\,s\rangle^{\alpha\cdot\sigma} & \text{by } \textit{i.h.} \text{ on } t \\ & = \bigoplus_{i=1}^n \mathsf{W}\langle t_i\,s\rangle^{\alpha\cdot\sigma} & \\ & \twoheadrightarrow\equiv \bigoplus_{i=1}^n \mathtt{fail} & \text{by } \textit{i.h.} \text{ on } s \\ & = \mathtt{fail} & \end{array}$$

so since $\equiv$ is a strong bisimulation (Lem. 3.3), $\mathsf{W}\langle t\,s\rangle^\alpha \twoheadrightarrow\equiv$ `fail`, as required.

8.2 If $\mathsf{mgu}(\mathsf{G}^\alpha)$ fails, then applying the *i.h.* for the term t under the weak context $\mathsf{W}\langle\Box\,s\rangle$ we have that $\mathsf{W}\langle t\,s\rangle^\alpha \twoheadrightarrow\equiv$ `fail`. Moreover, by the compositionality property (Lem. A.2) we have that $\mathsf{mgu}(\mathsf{G}^\alpha \cup \mathsf{H}^\alpha)$ also fails, so we are done.

9. $\mathtt{App}_2$: Let $(\lambda x.\,P)\,\mathtt{v} \overset{\varnothing}{\Rightarrow} P\{x := \mathtt{v}\}$. Then since $\mathsf{mgu}(\varnothing)$ is the identity substitution we have:

$$\mathsf{W}\langle(\lambda x.\,P)\,\mathtt{v}\rangle^\alpha = \mathsf{W}^\alpha\langle(\lambda x.\,P^\alpha)\,\mathtt{v}^\alpha\rangle \xrightarrow{\mathtt{beta}} \mathsf{W}^\alpha\langle P^\alpha\{x := \mathtt{v}^\alpha\}\rangle = \mathsf{W}\langle P\{x := \mathtt{v}\}\rangle^\alpha$$

This concludes this case. The fact that $\mathtt{v}^\alpha$ is indeed a value (required to be able to apply the `beta` rule), and the last equality are justified by Lem. A.1.

10. $\mathtt{Guard}_1$: Similar to the $\mathtt{App}_1$ case.

11. $\mathtt{Guard}_2$: Let $\mathtt{v}; t \overset{\mathsf{G}}{\Rightarrow} P$ be derived from $t \overset{\mathsf{G}}{\Rightarrow} P$. Let us write $P = \bigoplus_{i=1}^n t_i$. We consider two cases, depending on whether $\mathsf{mgu}(\mathsf{G}^\alpha)$ exists:

11.1 If $\sigma = \mathsf{mgu}(\mathsf{G}^\alpha)$ exists, then applying the *i.h.* on the term t under the context $\mathsf{W}\langle\mathtt{v};\Box\rangle$ we have that $\mathsf{W}\langle\mathtt{v};t\rangle^\alpha \twoheadrightarrow\equiv \mathsf{W}\langle\mathtt{v};P\rangle^{\alpha\cdot\sigma}$. Moreover, by Lem. A.1, $\mathtt{v}^{\alpha\cdot\sigma}$ is a value so we may apply the `guard` rule:

$$\begin{array}{rll} \mathsf{W}\langle\mathtt{v};t\rangle^\alpha & \twoheadrightarrow\equiv \mathsf{W}\langle\mathtt{v};P\rangle^{\alpha\cdot\sigma} & \text{by } \textit{i.h.} \text{ on } t \\ & = \mathsf{W}^{\alpha\cdot\sigma}\langle\mathtt{v}^{\alpha\cdot\sigma};P^{\alpha\cdot\sigma}\rangle & \\ & = \bigoplus_{i=1}^n \mathsf{W}^{\alpha\cdot\sigma}\langle\mathtt{v}^{\alpha\cdot\sigma};{t_i}^{\alpha\cdot\sigma}\rangle & \\ & \xrightarrow{\mathtt{guard}}\!\!\!\!\!\rightarrow \bigoplus_{i=1}^n \mathsf{W}^{\alpha\cdot\sigma}\langle{t_i}^{\alpha\cdot\sigma}\rangle & \\ & = \bigoplus_{i=1}^n \mathsf{W}\langle t_i\rangle^{\alpha\cdot\sigma} & \\ & = \mathsf{W}\langle P\rangle^{\alpha\cdot\sigma} & \end{array}$$

so since $\equiv$ is a strong bisimulation (Lem. 3.3), we have that $\mathsf{W}\langle \mathtt{v}; t\rangle^{\alpha} \twoheadrightarrow\equiv \mathsf{W}\langle P\rangle^{\alpha\cdot\sigma}$ as required.

11.2 If $\mathsf{mgu}(\mathsf{G}^{\alpha})$ fails, then applying the *i.h.* on the term t under the context $\mathsf{W}\langle \mathtt{v}; \square\rangle$ we have that $\mathsf{W}\langle \mathtt{v}; t\rangle^{\alpha} \twoheadrightarrow\equiv \mathtt{fail}$, as required.

12. $\mathtt{Unif}_1$: Similar to the $\mathtt{App}_1$ case.
13. $\mathtt{Unif}_2$: Let $\mathtt{v} \stackrel{\bullet}{=} \mathtt{w} \xRightarrow{\{\mathtt{v} \stackrel{\bullet}{=} \mathtt{w}\}} \mathbf{ok}$. We consider two cases, depending on whether $\mathsf{mgu}(\{\mathtt{v}^{\alpha} \stackrel{\bullet}{=} \mathtt{w}^{\alpha}\})$ exists:

13.1 If $\sigma = \mathsf{mgu}(\{\mathtt{v}^{\alpha} \stackrel{\bullet}{=} \mathtt{w}^{\alpha}\})$ exists, note that by Lem. A.1, $\mathtt{v}^{\alpha\cdot\sigma}$ and $\mathtt{w}^{\alpha\cdot\sigma}$ are values and we may apply the $\mathtt{unif}$ rule:

$$\begin{aligned}\mathsf{W}\langle \mathtt{v} \stackrel{\bullet}{=} \mathtt{w}\rangle^{\alpha} &= \mathsf{W}^{\alpha}\langle \mathtt{v}^{\alpha} \stackrel{\bullet}{=} \mathtt{w}^{\alpha}\rangle \\ &\xrightarrow{\mathtt{unif}} \mathsf{W}^{\alpha}\langle \mathbf{ok}\rangle^{\sigma} \\ &= \mathsf{W}\langle \mathbf{ok}\rangle^{\alpha\cdot\sigma}\end{aligned}$$

so $\mathsf{W}\langle \mathtt{v} \stackrel{\bullet}{=} \mathtt{w}\rangle^{\alpha} \twoheadrightarrow\equiv \mathsf{W}\langle \mathbf{ok}\rangle^{\alpha\cdot\sigma}$ as required.

13.2 If $\mathsf{mgu}(\{\mathtt{v}^{\alpha} \stackrel{\bullet}{=} \mathtt{w}^{\alpha}\})$ fails, note that by Lem. A.1, $\mathtt{v}^{\alpha\cdot\sigma}$ and $\mathtt{w}^{\alpha\cdot\sigma}$ are values and we may apply the $\mathtt{fail}$ rule:

$$\begin{aligned}\mathsf{W}\langle \mathtt{v} \stackrel{\bullet}{=} \mathtt{w}\rangle^{\alpha} &= \mathsf{W}^{\alpha}\langle \mathtt{v}^{\alpha} \stackrel{\bullet}{=} \mathtt{w}^{\alpha}\rangle \\ &\xrightarrow{\mathtt{fail}} \mathtt{fail}\end{aligned}$$

so $\mathsf{W}\langle \mathtt{v} \stackrel{\bullet}{=} \mathtt{w}\rangle^{\alpha} \twoheadrightarrow\equiv \mathtt{fail}$ as required.

Lemma A.3 (Values are irreducible). *Let* $\mathtt{v} \xRightarrow{\mathsf{G}} P$ *with* $\mathtt{v}$ *a value. Then* $\mathsf{G} = \varnothing$ *and* $P = \mathtt{v}$.

Proof. Straightforward by induction on $\mathtt{v}$. Note that the only rules that may be applied are $\mathtt{Var}$, $\mathtt{Cons}$, $\mathtt{Abs}^{\mathtt{A}}$, and $\mathtt{App}_1$.

Lemma A.4 (Diamond property). *Let* $t \xRightarrow{\mathsf{G}_1} \bigoplus_{i=1}^{n} t_i$ *and* $t \xRightarrow{\mathsf{G}_2} \bigoplus_{j=1}^{m} t_j^{\star}$. *Then there exist two sets of goals* G_1' *and* G_2', *and programs* $P_1, \dots, P_n$ *and* $P_1^{\star}, \dots, P_m^{\star}$ *such that:*

1. $t_i \xRightarrow{\mathsf{G}_2'}\equiv P_i$ *for all* $1 \le i \le n$;
2. $t_j^{\star} \xRightarrow{\mathsf{G}_1'}\equiv P_j^{\star}$ *for all* $1 \le j \le m$;
3. $\oplus_{i=1}^{n} P_i \sim \oplus_{j=1}^{m} P_j^{\star}$ *where "$\sim$" denotes the least equivalence generated by the* $\equiv$-$\mathtt{swap}$ *axiom,* i.e. *structural equivalence allowing only permutation of threads;*
4. $\mathsf{G}_1 \cup \mathsf{G}_2' = \mathsf{G}_2 \cup \mathsf{G}_1'$.

Proof. By induction on t:

1. *Variable,* $t = x$. The only rule that applies is $\mathtt{Var}$, *i.e.* $x \xRightarrow{\varnothing} x$, so this case is trivial. More precisely, we have that $n = m = 1$ and $t_1 = t_1^{\star} = x$, with $\mathsf{G}_1 = \mathsf{G}_2 = \varnothing$, so taking $\mathsf{G}_1' = \mathsf{G}_2' = \varnothing$ and $P_1 = P_1^{\star} = x$ it is straightforward to check that all the properties hold.

2. *Constructor,* $t = \mathbf{c}$. Immediate, similar to the variable case.
3. *Fresh variable declaration,* $t = \nu x.\, s$. There are four cases, depending on whether each of the simultaneous steps is deduced by $\mathtt{Fresh}_1$ or $\mathtt{Fresh}_2$:
   3.1 $\mathtt{Fresh}_1/\mathtt{Fresh}_1$: Immediate, similar to the variable case.
   3.2 $\mathtt{Fresh}_1/\mathtt{Fresh}_2$: Let $\nu x.\, s \stackrel{\varnothing}{\Rightarrow} \nu x.\, s$ be derived by rule $\mathtt{Fresh}_1$ (so that $n = 1$, $t_1 = \nu x.\, s$, and $\mathsf{G}_1 = \varnothing$), and let $\nu x.\, s \stackrel{\mathsf{G}_2}{\Longrightarrow} \bigoplus_{j=1}^{m} t_j^\star$ be derived by rule $\mathtt{Fresh}_2$ from $s \stackrel{\mathsf{G}_2}{\Longrightarrow} t_j^\star$. Then taking $\mathsf{G}_1' := \varnothing$, $\mathsf{G}_2' := \mathsf{G}_2$, $P_1 := \bigoplus_{j=1}^{m} t_j^\star$ and $P_j^\star := t_j^\star$ for each $1 \leq j \leq m$, using reflexivity for terms (Lem. 4.2) we have:

$$\frac{}{t_1 = \nu x.\, s \stackrel{\mathsf{G}_2}{\Longrightarrow} \bigoplus_{j=1}^{m} t_j^\star}\,\mathtt{Fresh}_2 \qquad \frac{\text{(Lem. 4.2)}}{t_j^\star \stackrel{\varnothing}{\Rightarrow} t_j^\star}$$

   3.3 $\mathtt{Fresh}_2/\mathtt{Fresh}_1$: Symmetric to the previous case ($\mathtt{Fresh}_1/\mathtt{Fresh}_2$).
   3.4 $\mathtt{Fresh}_2/\mathtt{Fresh}_2$: Let $\nu x.\, s \stackrel{\mathsf{G}_1}{\Longrightarrow} \bigoplus_{i=1}^{n} t_i$ be derived by rule $\mathtt{Fresh}_2$ from $s \stackrel{\mathsf{G}_1}{\Longrightarrow} \bigoplus_{i=1}^{n} t_i$, and let $\nu x.\, s \stackrel{\mathsf{G}_1}{\Longrightarrow} \bigoplus_{j=1}^{m} t_j$ be derived by rule $\mathtt{Fresh}_2$ from $s \stackrel{\mathsf{G}_2}{\Longrightarrow} \bigoplus_{j=1}^{n} t_j^\star$. Then by *i.h.* on s there exist sets of goals $\mathsf{G}_1', \mathsf{G}_2'$ and programs $P_1, \dots, P_n, P_1^\star, \dots, P_m^\star$ such that:

$$t_i \stackrel{\mathsf{G}_2'}{\Longrightarrow}\equiv P_i \qquad t_i^\star \stackrel{\mathsf{G}_1'}{\Longrightarrow}\equiv P_j \qquad \bigoplus_{i=1}^{n} P_i \sim \bigoplus_{j=1}^{m} P_j \qquad \mathsf{G}_1 \cup \mathsf{G}_2' = \mathsf{G}_2 \cup \mathsf{G}_1'$$

   which concludes this subcase.
4. *Abstraction code,* $t = \lambda x.\, P$. There are four cases, depending on whether each of the simultaneous steps is deduced by $\mathtt{Abs}_1^{\mathtt{C}}$ or $\mathtt{Abs}_2^{\mathtt{C}}$:
   4.1 $\mathtt{Abs}_1^{\mathtt{C}}/\mathtt{Abs}_1^{\mathtt{C}}$: Immediate, similar to the variable case.
   4.2 $\mathtt{Abs}_1^{\mathtt{C}}/\mathtt{Abs}_2^{\mathtt{C}}$: Let $\lambda x.\, P \stackrel{\varnothing}{\Rightarrow} \lambda x.\, P$ be derived from rule $\mathtt{Abs}_1^{\mathtt{C}}$, and let $\lambda x.\, P \stackrel{\varnothing}{\Rightarrow} \lambda^\ell x.\, P$ be derived from rule $\mathtt{Abs}_2^{\mathtt{C}}$, where ℓ is a fresh location. Note that $n = m = 1$ and $\mathsf{G}_1 = \mathsf{G}_2 = \varnothing$. Taking $\mathsf{G}_1' = \mathsf{G}_2' = \varnothing$, for some fresh location ℓ', we have that:

$$\frac{}{\lambda x.\, P \stackrel{\varnothing}{\Rightarrow} \lambda^{\ell'} x.\, P \equiv \lambda^\ell x.\, P}\,\mathtt{Abs}_2^{\mathtt{C}} \qquad \frac{}{\lambda^\ell x.\, P \stackrel{\varnothing}{\Rightarrow} \lambda^\ell x.\, P}\,\mathtt{Abs}^{\mathtt{A}}$$

   which concludes this subcase.
   4.3 $\mathtt{Abs}_2^{\mathtt{C}}/\mathtt{Abs}_1^{\mathtt{C}}$: Symmetric to the previous case ($\mathtt{Abs}_1^{\mathtt{C}}/\mathtt{Abs}_2^{\mathtt{C}}$).
   4.4 $\mathtt{Abs}_2^{\mathtt{C}}/\mathtt{Abs}_2^{\mathtt{C}}$: Let $\lambda x.\, P \stackrel{\varnothing}{\Rightarrow} \lambda^{\ell_1} x.\, P$ and $\lambda x.\, P \stackrel{\varnothing}{\Rightarrow} \lambda^{\ell_2} x.\, P$ be derived from rule $\mathtt{Abs}_2^{\mathtt{C}}$, where ℓ_1 and ℓ_2 are fresh locations. Note that $n = m = 1$ and $\mathsf{G}_1 = \mathsf{G}_2 = \varnothing$. Taking $\mathsf{G}_1' = \mathsf{G}_2' = \varnothing$ we have that:

$$\frac{}{\lambda^{\ell_1} x.\, P \stackrel{\varnothing}{\Rightarrow} \lambda^{\ell_1} x.\, P \equiv \lambda^{\ell_2} x.\, P}\,\mathtt{Abs}^{\mathtt{A}} \qquad \frac{}{\lambda^{\ell_2} x.\, P \stackrel{\varnothing}{\Rightarrow} \lambda^{\ell_2} x.\, P}\,\mathtt{Abs}^{\mathtt{A}}$$

5. *Allocated abstraction,* $t = \lambda x.\, s$. Immediate, similar to the variable case.

6. *Application,* $t = s\,u$. There are four cases, depending on whether each of the simultaneous steps is deduced by $\mathtt{App}_1^{\mathsf{C}}$ or $\mathtt{App}_2^{\mathsf{C}}$:
   6.1 $\mathtt{App}_1/\mathtt{App}_1$: This subcase is heavy to write—we give a detailed proof—but actually it follows directly by resorting to the inductive hypothesis. Let $s\,u \xRightarrow{\mathsf{G}_1 \cup \mathsf{H}_1} \bigoplus_{i=1}^{n} \bigoplus_{i'=1}^{n'} s_i\, u_{i'}$ be derived by rule $\mathtt{App}_1$ from $s \xRightarrow{\mathsf{G}_1} \bigoplus_{i=1}^{n} s_i$ and $u \xRightarrow{\mathsf{H}_1} \bigoplus_{i'=1}^{n'} u_{i'}$. Similarly, let $s\,u \xRightarrow{\mathsf{G}_2 \cup \mathsf{H}_2} \bigoplus_{j=1}^{m} \bigoplus_{j'=1}^{m'} s_j^\star\, u_{j'}^\star$ be derived by rule $\mathtt{App}_1$ from $s \xRightarrow{\mathsf{G}_2} \bigoplus_{j=1}^{m} s_j^\star$ and $u \xRightarrow{\mathsf{H}_2} \bigoplus_{j'=1}^{m'} u_{j'}^\star$.
   By *i.h.* on s, we have that there are sets of goals $\mathsf{G}_1', \mathsf{G}_2'$ and programs $P_1, \dots, P_n, P_1^\star, \dots, P_m^\star$ such that for each $1 \le i \le n$ and each $1 \le j \le m$:
$$s_i \xRightarrow{\mathsf{G}_2'}\equiv P_i \qquad s_j^\star \xRightarrow{\mathsf{G}_1'}\equiv P_j^\star \qquad \bigoplus_{i=1}^{n} P_i \sim \bigoplus_{j=1}^{m} P_j^\star \qquad \mathsf{G}_1 \cup \mathsf{G}_2' = \mathsf{G}_2 \cup \mathsf{G}_1'$$
   Similarly, by *i.h.* on u, we have that there are sets of goals $\mathsf{H}_1', \mathsf{H}_2'$ and programs $Q_1, \dots, Q_{n'}, Q_1^\star, \dots, Q_{m'}^\star$ such that for each $1 \le i' \le n'$ and each $1 \le j' \le m'$:
$$u_{i'} \xRightarrow{\mathsf{H}_2'}\equiv Q_{i'} \qquad u_{j'}^\star \xRightarrow{\mathsf{H}_1'}\equiv Q_{j'}^\star \qquad \bigoplus_{i'=1}^{n'} Q_{i'} \sim \bigoplus_{j'=1}^{m'} Q_{j'}^\star \qquad \mathsf{H}_1 \cup \mathsf{H}_2' = \mathsf{H}_2 \cup \mathsf{H}_1'$$
   This implies that, for each $1 \le i \le n$, $1 \le j \le m$, $1 \le i' \le n'$, and $1 \le j' \le m'$:
$$\dfrac{}{s_i\, u_{i'} \xRightarrow{\mathsf{G}_2' \cup \mathsf{H}_2'}\equiv P_i\, Q_{i'}}\ \mathtt{App}_1 \qquad \dfrac{}{s_j^\star\, u_{j'}^\star \xRightarrow{\mathsf{G}_1' \cup \mathsf{H}_1'}\equiv P_j^\star\, Q_{j'}^\star}\ \mathtt{App}_1$$
   Moreover, note that $\bigoplus_{i=1}^{n} \bigoplus_{i'=1}^{n'} P_i\, Q_{i'} \sim \bigoplus_{j=1}^{m} \bigoplus_{j'=1}^{m'} P_j^\star\, Q_{j'}^\star$, and that $\mathsf{G}_1 \cup \mathsf{H}_1 \cup \mathsf{G}_2' \cup \mathsf{H}_2' = \mathsf{G}_2 \cup \mathsf{H}_2 \cup \mathsf{G}_1' \cup \mathsf{H}_1'$. This concludes this subcase.
   6.2 $\mathtt{App}_1/\mathtt{App}_2$: Note that $s = \lambda^\ell x.\ \bigoplus_{i=1}^{n} r_i$ and $u = \mathtt{v}$, which are both values. Using the fact that a value only reduces to itself with an empty set of goals (Lem. A.3), let $(\lambda^\ell x.\ \bigoplus_{i=1}^{n} r_i)\,\mathtt{v} \xRightarrow{\varnothing} (\lambda^\ell x.\ \bigoplus_{i=1}^{n} r_i)\,\mathtt{v}$ be derived by $\mathtt{App}_1$ from $\lambda^\ell x.\ \bigoplus_{i=1}^{n} r_i \xRightarrow{\varnothing} \lambda^\ell x.\ \bigoplus_{i=1}^{n} r_i$ and $\mathtt{v} \xRightarrow{\varnothing} \mathtt{v}$. Moreover, let $(\lambda^\ell x.\ \bigoplus_{i=1}^{n} r_i)\,\mathtt{v} \xRightarrow{\varnothing} \bigoplus_{i=1}^{n} r_i\{x := \mathtt{v}\}$ be derived by $\mathtt{App}_2$. It is then easy to conclude this subcase noting that, for each $1 \le i \le n$, using reflexivity for terms (Lem. 4.2), we have:
$$\dfrac{}{\left(\lambda^\ell x.\ \bigoplus_{i=1}^{n} r_i\right)\,\mathtt{v} \xRightarrow{\varnothing} \bigoplus_{i=1}^{n} r_i\{x := \mathtt{v}\}}\ \mathtt{App}_2 \qquad \dfrac{\text{(Lem. 4.2)}}{r_i\{x := \mathtt{v}\} \xRightarrow{\varnothing} r_i\{x := \mathtt{v}\}}$$
   6.3 $\mathtt{App}_2/\mathtt{App}_1$: Symmetric to the previous case ($\mathtt{App}_1/\mathtt{App}_2$).
   6.4 $\mathtt{App}_2/\mathtt{App}_2$: There is only one way to derive a reduction using rule $\mathtt{App}_2$, namely $(\lambda x.\ \bigoplus_{i=1}^{n} s_i)\,\mathtt{v} \xRightarrow{\varnothing} \bigoplus_{i=1}^{n} s_i\{x := \mathtt{v}\}$. It is then easy to conclude

this subcase noting that, for each $1 \leq i \leq n$, using reflexivity for terms (Lem. 4.2), we have:

$$\frac{\text{(Lem. 4.2)}}{s_i\{x := \mathtt{v}\} \overset{\varnothing}{\Rightarrow} s_i\{x := \mathtt{v}\}}$$

7. *Guarded expression,* $t = (s; u)$. There are four cases, depending on whether each of the simultaneous steps is deduced by $\mathtt{Guard}_1$ or $\mathtt{Guard}_2$:
   7.1 $\mathtt{Guard}_1/\mathtt{Guard}_1$: This subcase follows directly by resorting to the inductive hypothesis, similar to the $\mathtt{App}_1/\mathtt{App}_1$ case.
   7.2 $\mathtt{Guard}_1/\mathtt{Guard}_2$: Note that s must be a value $s = \mathtt{v}$. Using the fact that a value only reduces to itself with an empty set of goals (Lem. A.3), let $\mathtt{v}; u \overset{\mathsf{G}_1}{\Longrightarrow} \bigoplus_{i=1}^{n} \mathtt{v}; u_i$ be derived by $\mathtt{Guard}_1$ from $u \overset{\mathsf{G}_1}{\Longrightarrow} \bigoplus_{i=1}^{n} u_i$. Moreover, let $s; u = \mathtt{v}; u \overset{\mathsf{G}_2}{\Longrightarrow} \bigoplus_{j=1}^{m} u_j^\star$ be derived from $u \overset{\mathsf{G}_2}{\Longrightarrow} \bigoplus_{j=1}^{m} u_j^\star$. By *i.h.* on u, there are sets of goals $\mathsf{G}_1', \mathsf{G}_2'$ and programs $P_1, \dots, P_n, P_1^\star, \dots, P_m^\star$ such that for each $1 \leq i \leq n$ and $1 \leq j \leq m$:

$$u_i \overset{\mathsf{G}_2'}{\Longrightarrow}\equiv P_i \qquad u_j^\star \overset{\mathsf{G}_1'}{\Longrightarrow}\equiv P_i^\star \qquad \bigoplus_{i=1}^{n} P_i \sim \bigoplus_{j=1}^{m} P_j^\star \qquad \mathsf{G}_1 \cup \mathsf{G}_2' = \mathsf{G}_2 \cup \mathsf{G}_1'$$

   To conclude this subcase, note that moreover:

$$\frac{u_i \overset{\mathsf{G}_2'}{\Longrightarrow}\equiv P_i}{\mathtt{v}; u_i \overset{\mathsf{G}_2'}{\Longrightarrow}\equiv P_i}\ \mathtt{Guard}_2$$

   7.3 $\mathtt{Guard}_2/\mathtt{Guard}_1$: Symmetric to the previous case ($\mathtt{Guard}_1/\mathtt{Guard}_2$).
   7.4 $\mathtt{Guard}_2/\mathtt{Guard}_2$: Straightforward by *i.h.*. More precisely, let $\mathtt{v}; u \overset{\mathsf{G}_1}{\Longrightarrow} \bigoplus_{i=1}^{n} u_i$ be derived from $u \overset{\mathsf{G}_1}{\Longrightarrow} \bigoplus_{i=1}^{n} u_i$ and, similarly, let $\mathtt{v}; u \overset{\mathsf{G}_2}{\Longrightarrow} \bigoplus_{j=1}^{m} u_j^\star$ be derived from $u \overset{\mathsf{G}_2}{\Longrightarrow} \bigoplus_{j=1}^{m} u_j^\star$. By *i.h.* on u, there are sets of goals $\mathsf{G}_1', \mathsf{G}_2'$ and programs $P_1, \dots, P_n, P_1^\star, \dots, P_m^\star$ such that for each $1 \leq i \leq n$ and $1 \leq j \leq m$:

$$u_i \overset{\mathsf{G}_2'}{\Longrightarrow}\equiv P_i \qquad u_j^\star \overset{\mathsf{G}_1'}{\Longrightarrow}\equiv P_i^\star \qquad \bigoplus_{i=1}^{n} P_i \sim \bigoplus_{j=1}^{m} P_j^\star \qquad \mathsf{G}_1 \cup \mathsf{G}_2' = \mathsf{G}_2 \cup \mathsf{G}_1'$$

   which concludes this subcase.
8. *Unification,* $t = (s \overset{\bullet}{=} u)$. There are four cases, depending on whether each of the simultaneous steps is deduced by $\mathtt{Unif}_1$ or $\mathtt{Unif}_2$:
   8.1 $\mathtt{Unif}_1/\mathtt{Unif}_1$: This subcase follows directly by resorting to the inductive hypothesis, similar to the $\mathtt{App}_1/\mathtt{App}_1$ case.
   8.2 $\mathtt{Unif}_1/\mathtt{Unif}_2$: Note that s and u must both be values, *i.e.* $s = \mathtt{v}$ and $u = \mathtt{w}$. Using the fact that a value only reduces to itself with an empty set of goals (Lem. A.3), let $\mathtt{v} \overset{\bullet}{=} \mathtt{w} \overset{\varnothing}{\Rightarrow} \mathtt{v} \overset{\bullet}{=} \mathtt{w}$ be derived by $\mathtt{Unif}_1$ from

$\mathtt{v} \xRightarrow{\varnothing} \mathtt{v}$ and $\mathtt{w} \xRightarrow{\varnothing} \mathtt{w}$, and let $\mathtt{v} \overset{\bullet}{=} \mathtt{w} \xRightarrow{\{\mathtt{v} \overset{\bullet}{=} \mathtt{w}\}} \mathbf{ok}$ be derived by $\mathtt{Unif}_2$. To conclude this subcase, note that:

$$\dfrac{}{\mathtt{v} \overset{\bullet}{=} \mathtt{w} \xRightarrow{\{\mathtt{v} \overset{\bullet}{=} \mathtt{w}\}} \mathbf{ok}}\ \mathtt{Unif}_2 \qquad \dfrac{}{\mathbf{ok} \xRightarrow{\varnothing} \mathbf{ok}}\ \mathtt{Cons}$$

8.3 $\mathtt{Unif}_2/\mathtt{Unif}_1$: Symmetric to the previous case ($\mathtt{Unif}_1/\mathtt{Unif}_2$).

8.4 $\mathtt{Unif}_2/\mathtt{Unif}_2$: There is a unique way that the reduction may be derived from rule $\mathtt{Unif}_2$, namely $\mathtt{v} \overset{\bullet}{=} \mathtt{w} \xRightarrow{\{\mathtt{v} \overset{\bullet}{=} \mathtt{w}\}} \mathbf{ok}$. To conclude this case, note that:

$$\dfrac{}{\mathbf{ok} \xRightarrow{\varnothing} \mathbf{ok}}\ \mathtt{Cons}$$

We now turn to the proof of Prop. 4.3 itself:

1. Item 1. of the proposition is precisely Lem. A.1.
2. For item 2. of the proposition, let $P \Rrightarrow Q$, and proceed by induction on P. If $P = \mathtt{fail}$, then $Q = \mathtt{fail}$, and indeed $P \twoheadrightarrow Q$ with the empty reduction sequence. If $P = t \oplus P'$, then $Q = R \oplus Q'$ where $t \Rrightarrow R$ and $P' \Rrightarrow Q'$. This in turn means that $t \xRightarrow{\mathsf{G}} R'$ in such a way that:

$$R \overset{\text{def}}{=} \begin{cases} R'^{\sigma} & \text{if } \sigma = \mathsf{mgu}(\mathsf{G}) \\ \mathtt{fail} & \text{if } \mathsf{mgu}(\mathsf{G}) \text{ fails.} \end{cases}$$

   Then:

$$\begin{aligned} t \oplus P' &\twoheadrightarrow\equiv R \oplus P' \text{ by Lem. A.2} \\ &\twoheadrightarrow\equiv R \oplus Q' \text{ by } \textit{i.h.} \end{aligned}$$

   Using the fact that $\equiv$ is a strong bisimulation (Lem. 3.3), this implies that $P = t \oplus P' \twoheadrightarrow\equiv R \oplus Q' = Q$, as required.
3. For item 3. of the proposition let $P \Rrightarrow P_1$ and $P \Rrightarrow P_2$, and proceed by induction on P. If $P = \mathtt{fail}$ then $P_1 = P_2 = \mathtt{fail}$ and the diamond may be closed with $\mathtt{fail} \Rrightarrow \mathtt{fail}$ on each side. If $P = t \oplus P'$ then $P_1 = Q_1 \oplus P'_1$ where $t \Rrightarrow Q_1$ and $P' \Rrightarrow P'_1$, and similarly $P_2 = Q_2 \oplus P'_2$ where $t \Rrightarrow Q_2$ and $P' \Rrightarrow P'_2$. By *i.h.* there are programs P'_3, P''_3 such that $P'_1 \Rrightarrow P'_3$ and $P'_2 \Rrightarrow P''_3 \equiv P'_3$. Moreover $t \xRightarrow{\mathsf{G}_1} \bigoplus_{i=1}^{n} t_i$ and $t \xRightarrow{\mathsf{G}_2} \bigoplus_{j=1}^{m} t^{\star}_j$ in such a way that:

$$Q_1 = \begin{cases} \bigoplus_{i=1}^{n} t_i{}^{\sigma_1} & \text{if } \sigma_1 = \mathsf{mgu}(\mathsf{G}_1) \\ \mathtt{fail} & \text{if } \mathsf{mgu}(\mathsf{G}_1) \text{ fails} \end{cases} \qquad Q_2 = \begin{cases} \bigoplus_{j=1}^{m} t^{\star}_j{}^{\sigma_2} & \text{if } \sigma_2 = \mathsf{mgu}(\mathsf{G}_2) \\ \mathtt{fail} & \text{if } \mathsf{mgu}(\mathsf{G}_2) \text{ fails} \end{cases}$$

   By Lem. A.4, there exist sets of goals $\mathsf{G}'_1, \mathsf{G}'_2$ and programs $R_1, \dots, R_n, R^{\star}_1, \dots, R^{\star}_m$ such that, for each $1 \le i \le n$ and $1 \le j \le m$:

$$t_i \xRightarrow{\mathsf{G}'_2} R_i \qquad t^{\star}_j \xRightarrow{\mathsf{G}'_1} R^{\star}_j \qquad \bigoplus_{i=1}^{n} R_i \sim \bigoplus_{j=1}^{m} R^{\star}_j \qquad \mathsf{G}_1 \cup \mathsf{G}'_2 = \mathsf{G}_2 \cup \mathsf{G}'_1$$

   We consider two subcases, depending on whether $\mathsf{mgu}(\mathsf{G}_1)$ exists:

3.1 If $\sigma_1 = \mathsf{mgu}(\mathsf{G}_1)$ exists, then by Lem. 4.2 we have that $t_i{}^{\sigma_1} \xRightarrow{\mathsf{G}_2'{}^{\sigma_1}} R_i{}^{\sigma_1}$ for each $1 \leq i \leq n$. We consider two further subcases, depending on whether $\mathsf{mgu}(\mathsf{G}_2'{}^{\sigma_1})$ exists:

3.1.1 If $\rho_1 = \mathsf{mgu}(\mathsf{G}_2'{}^{\sigma_1})$ exists, then by the compositionality property (Lem. A.2) we have that $\mathsf{mgu}(\mathsf{G}_1 \cup \mathsf{G}_2') = \mathsf{mgu}(\mathsf{G}_2 \cup \mathsf{G}_1')$ also exists, and it is a renaming of $\sigma_1 \cdot \rho_1$. Again, by the compositionality property (Lem. A.2), this in turn implies that $\sigma_2 = \mathsf{mgu}(\mathsf{G}_2)$ and $\rho_2 = \mathsf{mgu}(\mathsf{G}_1'{}^{\sigma_2})$ both exist, and $\sigma_2 \cdot \rho_2$ is a renaming of $\sigma_1 \cdot \rho_1$, *i.e.* $\sigma_2 \cdot \rho_2 = \sigma_1 \cdot \rho_1 \cdot \tau$ for some renaming τ. So by Lem. 4.2 we have that $t_j^{\star\sigma_2} \xRightarrow{\mathsf{G}_1'{}^{\sigma_2}} R_i^{\star\sigma_2}$ for each $1 \leq j \leq m$, and the situation is:

$$\begin{tikzcd}
t \oplus P' \arrow[rr, Rightarrow] \arrow[d, Rightarrow] & & \bigoplus_{i=1}^{n} t_i{}^{\sigma_1} \oplus P_1' \arrow[d, Rightarrow] \\
\bigoplus_{j=1}^{m} t_j^{\star\sigma_2} \oplus P_2' \arrow[r, Rightarrow] & \bigoplus_{j=1}^{m} R_j^{\star\sigma_2\cdot\rho_2} \oplus P_3'' \quad \equiv & \bigoplus_{i=1}^{n} R_i{}^{\sigma_1\cdot\rho_1} \oplus P_3'
\end{tikzcd}$$

The structural equivalence at the bottom of the diagram is justified as follows:

$$\begin{aligned}
\bigoplus_{j=1}^{m} R_j^{\star\sigma_2\cdot\rho_2} \oplus P_3'' &\sim \bigoplus_{i=1}^{n} R_i{}^{\sigma_2\cdot\rho_2} \oplus P_3'' \text{ since } \bigoplus_{j=1}^{m} R_j^{\star} \sim \bigoplus_{i=1}^{n} R_i \\
&\equiv \bigoplus_{i=1}^{n} R_i{}^{\sigma_1\cdot\rho_1} \oplus P_3'' \text{ since } \sigma_2 \cdot \rho_2 = \sigma_1 \cdot \rho_2 \cdot \tau \\
&\equiv \bigoplus_{i=1}^{n} R_i{}^{\sigma_1\cdot\rho_1} \oplus P_3' \text{ since } P_3'' \equiv P_3'
\end{aligned}$$

3.1.2 If $\mathsf{mgu}(\mathsf{G}_2'{}^{\sigma_1})$ fails, then by the compositionality property (Lem. A.2) we have that $\mathsf{mgu}(\mathsf{G}_1 \cup \mathsf{G}_2') = \mathsf{mgu}(\mathsf{G}_2 \cup \mathsf{G}_1')$ also fails. Again, by the compositionality property (Lem. A.2), this in turn implies that either $\sigma_2 = \mathsf{mgu}(\mathsf{G}_2)$ fails or $\mathsf{mgu}(\mathsf{G}_1'{}^{\sigma_2})$ fails. On one hand, if $\mathsf{mgu}(\mathsf{G}_2)$ fails, the situation is:

$$\begin{tikzcd}
t \oplus P' \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \bigoplus_{i=1}^{n} t_i{}^{\sigma_1} \oplus P_1' \arrow[d, Rightarrow] \\
P_2' \arrow[r, Rightarrow] & P_3'' \equiv P_3'
\end{tikzcd}$$

On the other hand, if $\sigma_2 = \mathsf{mgu}(\mathsf{G}_2)$ exists and $\mathsf{mgu}(\mathsf{G}_1'{}^{\sigma_2})$, the situation is:

$$\begin{tikzcd}
t \oplus P' \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \bigoplus_{i=1}^{n} t_i{}^{\sigma_1} \oplus P_1' \arrow[d, Rightarrow] \\
\bigoplus_{j=1}^{m} t_j^{\star\sigma_2} \oplus P_2' \arrow[r, Rightarrow] & P_3'' \equiv P_3'
\end{tikzcd}$$

3.2 If $\sigma_1 = \mathsf{mgu}(\mathsf{G}_1)$ fails, then by the compositionality property (Lem. A.2) we have that $\mathsf{mgu}(\mathsf{G}_1 \cup \mathsf{G}_2') = \mathsf{mgu}(\mathsf{G}_2 \cup \mathsf{G}_1')$ also fails. Again by the compositionality property (Lem. A.2) this implies that either $\sigma_2 = \mathsf{mgu}(\mathsf{G}_2)$

fails or $\rho_2 = \mathsf{mgu}(\mathsf{G}_1'^{\sigma_2})$ fails. On one hand, if $\mathsf{mgu}(\mathsf{G}_2)$ fails, the situation is:

$$\begin{array}{ccc} t \oplus P' & \Longrightarrow & P_1' \\ \Downarrow & & \Downarrow \\ P_2' & \Longrightarrow & P_3'' \equiv P_3' \end{array}$$

On the other hand, if $\sigma_2 = \mathsf{mgu}(\mathsf{G}_2)$ exists and $\mathsf{mgu}(\mathsf{G}_1'^{\sigma_2})$, the situation is:

$$\begin{array}{ccc} t \oplus P' & \Longrightarrow & P_1' \\ \Downarrow & & \Downarrow \\ \bigoplus_{j=1}^{m} t_j^{\star\sigma_2} \oplus P_2' & \Longrightarrow & P_3'' \equiv P_3' \end{array}$$

A.8 Proof of Prop. 5.2 — Subject Reduction

Definition A.1 (Typing unification problems). *We define the judgment* $\Gamma \vdash \mathsf{G}$ *for each unification problem* G *as follows:*

$$\frac{\Gamma \vdash \mathtt{v}_i \overset{\bullet}{=} \mathtt{w}_i : \mathcal{T}_{\mathbf{ok}} \quad \text{for all } i = 1..n}{\Gamma \vdash \{\mathtt{v}_1 \overset{\bullet}{=} \mathtt{w}_1, \dots, \mathtt{v}_n \overset{\bullet}{=} \mathtt{w}_n\}}$$

Lemma A.2 (Subject reduction for the unification algorithm). *Let* $\Gamma \vdash \mathsf{G}$ *and suppose that* $\mathsf{G} \rightsquigarrow \mathsf{H}$ *is a step that does not fail. Then* $\Gamma \vdash \mathsf{H}$*.*

Proof. Routine by case analysis on the transition $\mathsf{G} \rightsquigarrow \mathsf{H}$, using Lem. 5.1.

We turn to the proof of Prop. 5.2 itself. The proof proceeds by case analysis, depending on the rule applied to conclude that $P \to Q$. Most cases are straightforward using using Lem. 5.1. The only interesting case is when applying the `unif` rule. Then we have that:

$$P_1 \oplus \mathsf{W}\langle \mathtt{v} \overset{\bullet}{=} \mathtt{w} \rangle \oplus P_2 \xrightarrow{\mathtt{unif}} P_1 \oplus \mathsf{W}\langle \mathbf{ok} \rangle^{\sigma} \oplus P_2$$

where $\sigma = \mathsf{mgu}(\{\mathtt{v} \overset{\bullet}{=} \mathtt{w}\})$. Moreover, by hypothesis the program is typable, *i.e.*

$$\Gamma \vdash P_1 \oplus \mathsf{W}\langle \mathtt{v} \overset{\bullet}{=} \mathtt{w} \rangle \oplus P_2 : A$$

By Lem. 5.1 the following holds for some type B:

$$\Gamma \vdash P_1 : A \qquad \Gamma, \Box : B \vdash \mathsf{W} : A \qquad \Gamma \vdash \mathtt{v} \overset{\bullet}{=} \mathtt{w} : B \qquad \Gamma \vdash P_2 : A$$

The third judgment can only be derived using the `t-unif` rule, so necessarily $B = \mathcal{T}_{\mathbf{ok}}$, and in particular $\Gamma \vdash \mathsf{W}\langle \mathbf{ok} \rangle : A$ by contextual substitution (Lem. 5.1). Note that $\Gamma \vdash \{\mathtt{v} \overset{\bullet}{=} \mathtt{w}\}$. Moreover the most general unifier exists by hypothesis, so the unification algorithm terminates, *i.e.* there is a finite sequence of $n \geq 0$ steps:

$$\{\mathtt{v} \stackrel{\bullet}{=} \mathtt{w}\} = \mathsf{G}_0 \rightsquigarrow \mathsf{G}_1 \rightsquigarrow \ldots \rightsquigarrow \mathsf{G}_n = \{x_1 \stackrel{\bullet}{=} \mathtt{v}'_1, \ldots, x_n \stackrel{\bullet}{=} \mathtt{v}'_n\}$$

such that for all i, j we have that $x_i \neq x_j$ and $x_i \notin \mathsf{fv}(\mathtt{v}'_j)$. Moreover $\sigma = \mathsf{mgu}(\{\mathtt{v} \stackrel{\bullet}{=} \mathtt{w}\}) = \{x_1 \mapsto \mathtt{v}'_1, \ldots, x_n \mapsto \mathtt{v}'_n\}$. Recall that the unification algorithm preserves typing (Lem. A.2) so for each $i = 1..n$ there is a type C_i such that $\Gamma \vdash x_i : C_i$ and $\Gamma \vdash \mathtt{v}'_i : C_i$ hold. This means that Γ is of the form $\Delta, x_1 : C_1, \ldots, x_n : C_n$. By repeatedly applying the substitution property (Lem. 5.1), we conclude that $\Delta \vdash \mathsf{W}\langle\mathbf{ok}\rangle\{x_1 := \mathtt{v}'_1\} \ldots \{x_n := \mathtt{v}'_n\} : A$, that is $\Delta \vdash \mathsf{W}\langle\mathbf{ok}\rangle^\sigma : A$. Finally, applying Lem. 5.1 we obtain that the following judgment holds, as required:

$$\Gamma \vdash P_1 \oplus \mathsf{W}\langle\mathbf{ok}\rangle^\sigma \oplus P_2 : A$$

A.9 Proof of Prop. 6.1 — Properties of the denotational semantics

Let us introduce some auxiliary notation. We write Φ, Φ', etc. for sequences of variables ($\Phi = x_1^{A_1}, \ldots, x_n^{A_n}$) without repetition. If $\boldsymbol{A} = (A_1, \ldots, A_n)$ is a sequence of types, we write $[\![\boldsymbol{A}]\!]$ for $[\![A_1]\!] \times \ldots \times [\![A_n]\!]$. If $\boldsymbol{x} = (x_1, \ldots, x_n)$ is a sequence of variable names, we write $\boldsymbol{x}^{\boldsymbol{A}}$ for the sequence $(x_1^{A_1}, \ldots, x_n^{A_n})$. Moreover, if $\boldsymbol{a} = (a_1, \ldots, a_n) \in [\![\boldsymbol{A}]\!]$ then we write $\rho[\boldsymbol{x} \mapsto \boldsymbol{a}]$ for $\rho[x_1 \mapsto a_1] \ldots [x_n \mapsto a_n]$. Sometimes we treat sequences of variables as sets, when the order is not relevant. If X is a term or a program we define $[\![X]\!]_\rho^\Phi$ as follows, by induction on Φ:

$$\begin{aligned} [\![X]\!]_\rho^\varnothing &\stackrel{\text{def}}{=} [\![X]\!]_\rho \\ [\![X]\!]_\rho^{x^A, \Phi} &\stackrel{\text{def}}{=} \{b \mid a \in [\![A]\!], b \in [\![X]\!]_{\rho[x \mapsto a]}^\Phi\} \end{aligned}$$

The following lemma generalizes the **Irrelevance** property of Lem. 6.1. An easy corollary of this lemma is that $[\![P]\!] = [\![P]\!]_\rho^{\mathsf{fv}(P)}$, whatever be the environment ρ.

Lemma A.1 (Irrelevance — proof of Lem. 6.1, point 1). *Let $\vdash X : A$ be a typable term or program.*

1. *If ρ, ρ' are environments that agree on $\mathsf{fv}(X) \setminus \Phi$,* i.e. *for any variable $x^B \in \mathsf{fv}(X) \setminus \Phi$ one has that $\rho(x^B) = \rho'(x^B)$, then $[\![X]\!]_\rho^\Phi = [\![X]\!]_{\rho'}^\Phi$.*
2. *Let Φ, Φ' be sequences of variables such that $\mathsf{fv}(X) \setminus \Phi = \mathsf{fv}(X) \setminus \Phi'$. Then $[\![X]\!]_\rho^\Phi = [\![X]\!]_\rho^{\Phi'}$.*

Proof. 1. By induction on Φ.

1.1 **Empty, *i.e.* $\Phi = \varnothing$.** By induction on X, *i.e.* the term or program:

1.1.1 **Variable, $X = x^A$.** Immediate, as $[\![x^A]\!]_\rho = \rho(x^A) = \rho'(x^A) = [\![x^A]\!]_{\rho'}$.

1.1.2 **Constructor, $X = \mathbf{c}$.** Immediate, as $[\![\mathbf{c}]\!]_\rho = \{\underline{\mathbf{c}}\} = [\![\mathbf{c}]\!]_{\rho'}$.

1.1.3 **Abstraction, $X = \lambda x^A. P$.** Note that $[\![\lambda x^A. P]\!]_\rho = \{f\}$ where $f(a) = [\![P]\!]_{\rho[x^A \mapsto a]}$. Symmetrically, $[\![\lambda x^A. P]\!]_{\rho'} = \{g\}$ where $g(a) = [\![P]\!]_{\rho'[x^A \mapsto a]}$. Note that, for any fixed $a \in [\![A]\!]$, we have that $\rho[x^A \mapsto a]$ and $\rho'[x^A \mapsto a]$ agree on $\mathsf{fv}(\lambda x. P)$ and also on x so they agree on

$\mathsf{fv}(P)$. This allows us to apply the *i.h.* to conclude that $[\![P]\!]_{\rho[x^A \mapsto a]} = [\![P]\!]_{\rho'[x^A \mapsto a]}$, so $f = g$ as required.

1.1.4 **Allocated abstraction,** $X = \lambda^\ell x^A.\, P$**.** Similar to the previous case.

1.1.5 **Application,** $X = t\, s$**.** Straightforward by *i.h.*, as $[\![t\, s]\!]_\rho = \{b \mid f \in [\![t]\!]_\rho, a \in [\![s]\!]_\rho, b \in f(a)\} = \{b \mid f \in [\![t]\!]_{\rho'}, a \in [\![s]\!]_{\rho'}, b \in f(a)\} = [\![t\, s]\!]_{\rho'}$.

1.1.6 **Unification,** $X = (t \overset{\bullet}{=} s)$**.** Straightforward by *i.h.* as $[\![t \overset{\bullet}{=} s]\!]_\rho = \{\underline{\mathbf{ok}} \mid a \in [\![t]\!]_\rho, b \in [\![s]\!]_\rho, a = b\} = \{\underline{\mathbf{ok}} \mid a \in [\![t]\!]_{\rho'}, b \in [\![s]\!]_{\rho'}, a = b\} = [\![t \overset{\bullet}{=} s]\!]_{\rho'}$.

1.1.7 **Guarded expression,** $X = t; s$**.** Straightforward by *i.h.* as $[\![t; s]\!]_\rho = \{b \mid a \in [\![t]\!]_\rho, b \in [\![s]\!]_\rho\} = \{b \mid a \in [\![t]\!]_{\rho'}, b \in [\![s]\!]_{\rho'}\} = [\![t; s]\!]_{\rho'}$.

1.1.8 **Fresh,** $X = \nu x^A.\, t$**.** Note that $[\![\nu x^A.\, t]\!]_\rho = \{b \mid a \in [\![A]\!], b \in [\![t]\!]_{\rho[x^A \mapsto a]}\}$. Symetrically, $[\![\nu x^A.\, t]\!]_{\rho'} = \{b \mid a \in [\![A]\!], b \in [\![t]\!]_{\rho'[x^A \mapsto a]}\}$. Note that, for any fixed $a \in [\![A]\!]$ we have that $\rho[x^A \mapsto a]$ and $\rho'[x^A \mapsto a]$ agree on $\mathsf{fv}(\nu x^A.\, t)$ and also on x, so they agree on $\mathsf{fv}(t)$. This allows us to apply the *i.h.* to conclude that $[\![t]\!]_{\rho[x^A \mapsto a]} = [\![t]\!]_{\rho'[x^A \mapsto a]}$, so $[\![\nu x^A.\, t]\!]_\rho = [\![\nu x^A.\, t]\!]_{\rho'}$, as required.

1.1.9 **Fail,** $X = \mathtt{fail}^A$**.** Immediate, as $[\![\mathtt{fail}^A]\!]_\rho = \varnothing = [\![\mathtt{fail}^A]\!]_{\rho'}$.

1.1.10 **Alternative,** $X = t \oplus P$**.** Straightforward by *i.h.* as $[\![t \oplus P]\!]_\rho = [\![t]\!]_\rho \cup [\![P]\!]_\rho = [\![t]\!]_{\rho'} \cup [\![P]\!]_{\rho'} = [\![t \oplus P]\!]_\rho$.

1.2 **Non-empty, *i.e.*** $\Phi = x^A, \Psi$**.** Then note that $\rho[x \mapsto a]$ and $\rho[x \mapsto a]$ agree on $\mathsf{fv}(X) \setminus \Psi$ for any $a \in [\![A]\!]$. Then:

$$\begin{aligned}
[\![X]\!]_\rho^{x^A, \Psi} &= \{b \mid a \in [\![A]\!], [\![X]\!]_{\rho[x \mapsto a]}^{\Psi}\} \\
&= \{b \mid a \in [\![A]\!], [\![X]\!]_{\rho'[x \mapsto a]}^{\Psi}\} \text{ by } \textit{i.h.} \\
&= [\![X]\!]_{\rho'}^{x^A, \Psi}
\end{aligned}$$

2. Note that, seen as sets, $\mathsf{fv}(X) \cap \Phi = \mathsf{fv}(X) \cap \Phi'$ so the sequence Φ may be converted into the sequence Φ' by repeatedly removing *spurious* variables (not in $\mathsf{fv}(X)$), adding spurious variables, and swapping variables. Indeed, we first note that the two following properties hold:
   - **Add/remove spurious variable.** $[\![X]\!]_\rho^\Phi = [\![X]\!]_\rho^{x^A, \Phi}$ if $x^A \notin \mathsf{fv}(X)$.
     It suffices to show that $[\![X]\!]_\rho^\Phi = \{b \mid a \in [\![A]\!], b \in [\![X]\!]_{\rho[x \mapsto a]}^\Phi\}$, which is immediate since by item 1. of this lemma, $[\![X]\!]_\rho^\Phi = [\![X]\!]_{\rho[x \mapsto a]}^\Phi$ for all $a \in [\![A]\!]$. Note that here we crucially use the fact that $[\![A]\!]$ is a non-empty set.
   - **Swap.** $[\![X]\!]_\rho^{\Phi_1, x^A, \Phi_2} = [\![X]\!]_\rho^{x^A, \Phi_1, \Phi_2}$.
     Proceed by induction on Φ_1. If Φ_1 is empty, it is immediate. Otherwise, let $\Phi_1 = y^B, \Phi_1'$. Then:

$$\begin{aligned}
[\![X]\!]_\rho^{y^B, \Phi_1', x^A, \Phi_2} &= \{c \mid b \in [\![B]\!], c \in [\![X]\!]_{\rho[y \mapsto b]}^{\Phi_1', x^A, \Phi_2}\} \\
&= \{c \mid b \in [\![B]\!], c \in [\![X]\!]_{\rho[y \mapsto b]}^{x^A, \Phi_1', \Phi_2}\} && \text{by } \textit{i.h.} \\
&= \{c \mid b \in [\![B]\!], a \in [\![A]\!], c \in [\![X]\!]_{\rho[y \mapsto b][x \mapsto a]}^{\Phi_1', \Phi_2}\} \\
&= \{c \mid a \in [\![A]\!], b \in [\![B]\!], c \in [\![X]\!]_{\rho[x \mapsto a][y \mapsto b]}^{\Phi_1', \Phi_2}\} \; (\star) \\
&= [\![X]\!]_\rho^{x^A, y^B, \Phi_1', \Phi_2}
\end{aligned}$$

To justify the ($\star$) step, note that $\rho[y \mapsto b][x \mapsto a] = \rho[x \mapsto a][y \mapsto b]$ holds by definition.

Now we proceed by induction on Φ:

2.1 **Empty, *i.e.* $\Phi = \varnothing$.** Then $\mathsf{fv}(X) = \mathsf{fv}(X) \setminus \Phi'$ so $\Phi' \cap \mathsf{fv}(X) = \varnothing$. By iteratively adding spurious variables we have that $[\![X]\!]^{\Phi}_{\rho} = [\![X]\!]_{\rho} = [\![X]\!]^{\Phi'}_{\rho}$ as required.

2.2 **Non-empty, *i.e.* $\Phi = x^A, \Psi$.** We consider two subcases, depending on whether the variable x^A is spurious (*i.e.* $x^A \notin \mathsf{fv}(X)$) or not:

2.2.1 If $x^A \notin \mathsf{fv}(X)$ then note that $\mathsf{fv}(X) \setminus \Psi = \mathsf{fv}(X) \setminus \Phi = \mathsf{fv}(X) \setminus \Phi'$, so removing the spurious variable and appyling the *i.h.* we have that $[\![X]\!]^{x^A,\Psi}_{\rho} = [\![X]\!]^{\Psi}_{\rho} = [\![X]\!]^{\Phi'}_{\rho}$.

2.2.2 If $x^A \in \mathsf{fv}(X)$ then since $\mathsf{fv}(t) \setminus \Phi = \mathsf{fv}(t) \setminus \Phi'$ we have that $x^A \in \Phi'$. Hence Φ' must be of the form $\Phi' = \Phi'_1, x^A, \Phi'_2$. Then by applying the *i.h.* and swapping we have that $[\![X]\!]^{x^A,\Psi}_{\rho} = [\![X]\!]^{x^A,\Phi'_1,\Phi'_2}_{\rho} = [\![X]\!]^{\Phi'_1,x^A,\Phi'_2}_{\rho}$ as required.

The following lemma generalizes the **Compositionality** property of Lem. 6.1.

Lemma A.2 (Compositionality — proof of Lem. 6.1, point 2).

1. $[\![P \oplus Q]\!]^{\Phi}_{\rho} = [\![P]\!]^{\Phi}_{\rho} \cup [\![Q]\!]^{\Phi}_{\rho}$.
2. *If* W *is a context whose hole is of type* A*, then* $[\![\mathsf{W}\langle t\rangle]\!]_{\rho} = \{b \mid a \in [\![t]\!]_{\rho}, b \in [\![\mathsf{W}]\!]_{\rho[\Box^A \mapsto a]}\}$.

Proof.

1. By induction on the length of Φ.

1.1 **Empty, $\Phi = \varnothing$.** Then we proceed by induction on P:

1.1.1 If $P = \texttt{fail}$, then $[\![\texttt{fail} \oplus Q]\!]_{\rho} = [\![Q]\!]_{\rho} = [\![\texttt{fail}]\!]_{\rho} \cup [\![Q]\!]_{\rho}$.

1.1.2 If $P = t \oplus P'$, then:

$$\begin{aligned}
[\![(t \oplus P') \oplus Q]\!]_{\rho} &= [\![t \oplus (P' \oplus Q)]\!]_{\rho} \\
&= [\![t]\!]_{\rho} \cup [\![P' \oplus Q]\!]_{\rho} \\
&= [\![t]\!]_{\rho} \cup [\![P']\!]_{\rho} \cup [\![Q]\!]_{\rho} \text{ by } \textit{i.h.} \\
&= [\![t \oplus P']\!]_{\rho} \cup [\![Q]\!]_{\rho}
\end{aligned}$$

1.2 **Non-empty, $\Phi = x^A, \Phi'$.** Then:

$$\begin{aligned}
[\![P \oplus Q]\!]^{x^A,\Phi'}_{\rho} &= \{b \mid a \in [\![A]\!], b \in [\![P \oplus Q]\!]^{\Phi'}_{\rho[x \mapsto a]}\} \\
&= \{b \mid a \in [\![A]\!], b \in ([\![P]\!]^{\Phi'}_{\rho[x \mapsto a]} \cup [\![Q]\!]^{\Phi'}_{\rho[x \mapsto a]})\} && \text{by } \textit{i.h.} \\
&= \{b \mid a \in [\![A]\!], b \in [\![P]\!]^{\Phi'}_{\rho[x \mapsto a]}\} \cup \{b \mid a \in [\![A]\!], b \in [\![Q]\!]^{\Phi'}_{\rho[x \mapsto a]}\} \\
&= [\![P]\!]^{x^A,\Phi'}_{\rho} \cup [\![Q]\!]^{x^A,\Phi'}_{\rho}
\end{aligned}$$

2. By induction on the structure of the weak context W.
   - **Empty, $\mathsf{W} = \Box$.**

$$\begin{aligned}
[\![t]\!]_{\rho} &= \{b \mid a \in [\![t]\!]_{\rho}, b \in \{a\}\} \\
&= \{b \mid a \in [\![t]\!]_{\rho}, b \in [\![\Box]\!]_{\rho[\Box^A \mapsto a]}\}
\end{aligned}$$

– **Left of an application,** $\mathsf{W} = \mathsf{W}'\,s$**.**

$$\begin{aligned}
[\![\mathsf{W}'\langle t\rangle\, s]\!]_\rho &= \{b \mid f \in [\![\mathsf{W}'\langle t\rangle]\!]_\rho, c \in [\![s]\!]_\rho, b \in f(c)\} \\
&= \{b \mid a \in [\![t]\!]_\rho, f \in [\![\mathsf{W}']\!]_{\rho[\Box^A \mapsto a]}, c \in [\![s]\!]_\rho, b \in f(c)\} && \text{(By } \textit{i.h.}\text{)} \\
&= \{b \mid a \in [\![t]\!]_\rho, f \in [\![\mathsf{W}']\!]_{\rho[\Box^A \mapsto a]}, c \in [\![s]\!]_{\rho[\Box^A \mapsto a]}, b \in f(c)\} && \text{(By Lem. 6.1)} \\
&= \{b \mid a \in [\![t]\!]_\rho, b \in [\![\mathsf{W}'\, s]\!]_{\rho[\Box^A \mapsto a]}\}
\end{aligned}$$

– **Right of an application,** $\mathsf{W} = s\,\mathsf{W}'$**.**

$$\begin{aligned}
[\![s\,\mathsf{W}'\langle t\rangle]\!]_\rho &= \{b \mid f \in [\![s]\!]_\rho, c \in [\![\mathsf{W}'\langle t\rangle]\!]_\rho, b \in f(c)\} \\
&= \{b \mid f \in [\![s]\!]_\rho, a \in [\![t]\!]_\rho, c \in [\![\mathsf{W}']\!]_{\rho[\Box^A \mapsto a]}, b \in f(c)\} && \text{(By } \textit{i.h.}\text{)} \\
&= \{b \mid a \in [\![t]\!]_\rho, f \in [\![s]\!]_{\rho[\Box^A \mapsto a]}, c \in [\![\mathsf{W}']\!]_{\rho[\Box^A \mapsto a]}, b \in f(c)\} && \text{(By Lem. 6.1)} \\
&= \{b \mid a \in [\![t]\!]_\rho, b \in [\![s\,\mathsf{W}']\!]_{\rho[\Box^A \mapsto a]}\}
\end{aligned}$$

– **Left of a unification,** $\mathsf{W} = \mathsf{W}' \overset{\bullet}{=} s$**.**

$$\begin{aligned}
[\![\mathsf{W}'\langle t\rangle \overset{\bullet}{=} s]\!]_\rho &= \{\underline{\mathbf{ok}} \mid c \in [\![\mathsf{W}'\langle t\rangle]\!]_\rho, d \in [\![s]\!]_\rho, c = d\} \\
&= \{\underline{\mathbf{ok}} \mid a \in [\![t]\!]_\rho, c \in [\![\mathsf{W}']\!]_{\rho[\Box^A \mapsto a]}, d \in [\![s]\!]_\rho, c = d\} && \text{(By } \textit{i.h.}\text{)} \\
&= \{\underline{\mathbf{ok}} \mid a \in [\![t]\!]_\rho, c \in [\![\mathsf{W}']\!]_{\rho[\Box^A \mapsto a]}, d \in [\![s]\!]_{\rho[\Box^A \mapsto a]}, c = d\} && \text{(By Lem. 6.1)} \\
&= \{b \mid a \in [\![t]\!]_\rho, b \in [\![\mathsf{W}' \overset{\bullet}{=} s]\!]_{\rho[\Box^A \mapsto a]}\}
\end{aligned}$$

– **Right of a unification,** $\mathsf{W} = s \overset{\bullet}{=} \mathsf{W}'$**.**

$$\begin{aligned}
[\![s \overset{\bullet}{=} \mathsf{W}'\langle t\rangle]\!]_\rho &= \{\underline{\mathbf{ok}} \mid c \in [\![s]\!]_\rho, d \in [\![\mathsf{W}'\langle t\rangle]\!]_\rho, c = d\} \\
&= \{\underline{\mathbf{ok}} \mid a \in [\![t]\!]_\rho, c \in [\![s]\!]_\rho, d \in [\![\mathsf{W}']\!]_{\rho[\Box^A \mapsto a]}, c = d\} && \text{(By } \textit{i.h.}\text{)} \\
&= \{\underline{\mathbf{ok}} \mid a \in [\![t]\!]_\rho, c \in [\![s]\!]_{\rho[\Box^A \mapsto a]}, d \in [\![\mathsf{W}']\!]_{\rho[\Box^A \mapsto a]}, c = d\} && \text{(By Lem. 6.1)} \\
&= \{b \mid a \in [\![t]\!]_\rho, b \in [\![s \overset{\bullet}{=} \mathsf{W}']\!]_{\rho[\Box^A \mapsto a]}\}
\end{aligned}$$

– **Left of a guarded expression,** $\mathsf{W} = \mathsf{W}'; s$**.**

$$\begin{aligned}
[\![\mathsf{W}'\langle t\rangle; s]\!]_\rho &= \{b \mid c \in [\![\mathsf{W}'\langle t\rangle]\!]_\rho, b \in [\![s]\!]_\rho\} \\
&= \{b \mid a \in [\![t]\!]_\rho, c \in [\![\mathsf{W}']\!]_{\rho[\Box^A \mapsto a]}, b \in [\![s]\!]_\rho\} && \text{(By } \textit{i.h.}\text{)} \\
&= \{b \mid a \in [\![t]\!]_\rho, c \in [\![\mathsf{W}']\!]_{\rho[\Box^A \mapsto a]}, b \in [\![s]\!]_{\rho[\Box^A \mapsto a]}\} && \text{(By Lem. 6.1)} \\
&= \{b \mid a \in [\![t]\!]_\rho, b \in [\![\mathsf{W}'; s]\!]_{\rho[\Box^A \mapsto a]}\}
\end{aligned}$$

– **Right of a guarded expression,** $\mathsf{W} = s; \mathsf{W}'$**.**

$$\begin{aligned}
[\![s; \mathsf{W}'\langle t\rangle]\!]_\rho &= \{b \mid c \in [\![s]\!]_\rho, b \in [\![\mathsf{W}'\langle t\rangle]\!]_\rho\} \\
&= \{b \mid a \in [\![t]\!]_\rho, c \in [\![s]\!]_\rho, b \in [\![\mathsf{W}']\!]_{\rho[\Box^A \mapsto a]}\} && \text{(By } \textit{i.h.}\text{)} \\
&= \{b \mid a \in [\![t]\!]_\rho, c \in [\![s]\!]_{\rho[\Box^A \mapsto a]}, b \in [\![\mathsf{W}']\!]_{\rho[\Box^A \mapsto a]}\} && \text{(By Lem. 6.1)} \\
&= \{b \mid a \in [\![t]\!]_\rho, b \in [\![s; \mathsf{W}']\!]_{\rho[\Box^A \mapsto a]}\}
\end{aligned}$$

Lemma A.3 (Free variables). *The following hold:*

1. $\mathsf{fv}(P \oplus Q) = \mathsf{fv}(P) \cup \mathsf{fv}(Q)$
2. $\mathsf{fv}(\mathsf{W}\langle t\rangle) = \mathsf{fv}(\mathsf{W}) \cup \mathsf{fv}(t)$
3. $\mathsf{fv}(\mathsf{W}\langle P\rangle) = \mathsf{fv}(\mathsf{W}) \cup \mathsf{fv}(P)$
4. $\mathsf{fv}(t^\sigma) \subseteq (\mathsf{fv}(t) \setminus \operatorname{supp}\sigma) \cup \bigcup_{x \in \operatorname{supp}\sigma} \mathsf{fv}(\sigma(x))$

5. $\mathsf{fv}(P^\sigma) \subseteq (\mathsf{fv}(P) \setminus \operatorname{supp}\sigma) \cup \bigcup_{x \in \operatorname{supp}\sigma} \mathsf{fv}(\sigma(x))$

Proof. Routine by induction on P, W, or t, correspondingly.

Lemma A.4 (Interpretation of values — proof of Lem. A.4, point 3). *If* $\mathtt{v}$ *is a value then* $[\![\mathtt{v}]\!]_\rho$ *is a singleton.*

Proof. By induction on $\mathtt{v}$. If $\mathtt{v}$ is a variable or an allocated abstraction, it is immediate, so let $\mathtt{v} = \mathbf{c}\,\mathtt{v}_1 \ldots \mathtt{v}_n$. In that case, by induction on n we claim that $[\![\mathbf{c}\,\mathtt{v}_1 \ldots \mathtt{v}_n]\!]_\rho$ is a singleton of the form $\{a\}$ where moreover a is unitary:

1. **If** $n = 0$**.** Then $[\![\mathbf{c}]\!]_\rho = \{\underline{\mathbf{c}}\}$, which is a singleton. Moreover, recall that $\underline{\mathbf{c}}$ is always requested to be unitary.
2. **If** $n > 0$**.** Then by *i.h.* of the innermost induction $[\![\mathbf{c}\,\mathtt{v}_1 \ldots \mathtt{v}_{n-1}]\!]_\rho$ is a singleton of the form $\{f_0\}$, where f_0 is unitary, and by *i.h.* of the outermost induction $[\![\mathtt{v}_n]\!]_\rho$ is a singleton of the form $\{a_0\}$, so we have that:

$$\begin{aligned} [\![\mathbf{c}\,\mathtt{v}_1 \ldots \mathtt{v}_{n-1}\,\mathtt{v}_n]\!]_\rho &= \{b \mid f \in [\![\mathbf{c}\,\mathtt{v}_1 \ldots \mathtt{v}_{n-1}]\!]_\rho, a \in [\![\mathtt{v}_n]\!]_\rho, b \in f(a)\} \\ &= f_0(a_0) \end{aligned}$$

Since f_0 is unitary, $f_0(a_0)$ is a singleton of the form $\{b\}$, where b is unitary, as required.

Lemma A.5 (Interpretation of substitution — proof of Lem. 6.1, point 4). *Let* $\sigma = \{x_1^{A_1} \mapsto \mathtt{v}_1, \ldots, x_n^{A_n} \mapsto \mathtt{v}_n\}$ *be a substitution with support* $\{x_1^{A_1}, \ldots, x_n^{A}\}$ *and such that* $x_i \notin \mathsf{fv}(\mathtt{v}_j)$ *for any two* $1 \le i, j \le n$*. Recall that the interpretation of a value is always a singleton (Lem. 6.1), so let* $[\![\mathtt{v}_i]\!]_\rho = \{a_i\}$ *for each* $i = 1..n$*. Then:*

1. $[\![t^\sigma]\!]_\rho = [\![t]\!]_{\rho[x_1 \mapsto a_1]\ldots[x_n \mapsto a_n]}$
2. $[\![P^\sigma]\!]_\rho = [\![P]\!]_{\rho[x_1 \mapsto a_1]\ldots[x_n \mapsto a_n]}$

Proof. By simultaneous induction on the term t (resp. program P).

1. **Variable,** $t = x^A$**.** There are two subcases, depending on whether $x \in \{x_1, \ldots, x_n\}$ or not.
   1.1 If $x = x_i$ for some $1 \le i \le n$, then:

$$[\![(x_i^A)^\sigma]\!]_\rho = [\![\mathtt{v}_i]\!]_\rho = \{a_i\} = [\![x_i^A]\!]_{\rho[x_1 \mapsto a_1]\ldots[x_n \mapsto a_n]}$$

   1.2 If $x \notin \{x_1, \ldots, x_n\}$, then:

$$[\![(x^A)^\sigma]\!]_\rho = \rho(x^A) = [\![x^A]\!]_{\rho[x_1 \mapsto a_1]\ldots[x_n \mapsto a_n]}$$

2. **Constructor,** $t = \mathbf{c}$**.** Immediate, as:

$$[\![\mathbf{c}^\sigma]\!]_\rho = [\![\mathbf{c}]\!]_\rho = \{\underline{\mathbf{c}}\} = [\![\mathbf{c}]\!]_{\rho[x_1 \mapsto a_1]\ldots[x_n \mapsto a_n]}$$

3. **Abstraction code,** $t = \lambda x^A.\, P$**.** Then:

$$\begin{aligned}
[\![(\lambda x^A.\, P)^\sigma]\!]_\rho &= [\![\lambda x^A.\, P^\sigma]\!]_\rho \\
&= \{f\} \quad \text{where } f(a) = [\![P^\sigma]\!]_{\rho[x \mapsto a]} \\
&= \{g\} \quad \text{where } g(a) = [\![P]\!]_{\rho[x \mapsto a][x_1 \mapsto a_1] \ldots [x_n \mapsto a_n]} \ \text{(By } i.h.\text{)} \\
&= [\![\lambda x^A.\, P]\!]_{\rho[x_1 \mapsto a_1] \ldots [x_n \mapsto a_n]}
\end{aligned}$$

4. **Allocated abstraction,** $t = \lambda^\ell x.\, P$**.** Similar to the previous case.
5. **Application,** $t = s\, u$**.** Then:

$$\begin{aligned}
[\![(s\, u)^\sigma]\!]_\rho &= [\![s^\sigma\, u^\sigma]\!]_\rho \\
&= \{b \mid f \in [\![s^\sigma]\!]_\rho, a \in [\![u^\sigma]\!]_\rho, b \in f(a)\} \\
&= \{b \mid f \in [\![s]\!]_{\rho[x_1 \mapsto a_1] \ldots [x_n \mapsto a_n]}, a \in [\![u]\!]_{\rho[x_1 \mapsto a_1] \ldots [x_n \mapsto a_n]}, b \in f(a)\} \ \text{(By } i.h.\text{)} \\
&= [\![s\, u]\!]_{\rho[x_1 \mapsto a_1] \ldots [x_n \mapsto a_n]}
\end{aligned}$$

6. **Unification,** $t = (s \overset{\bullet}{=} u)$**.** Then:

$$\begin{aligned}
[\![(s \overset{\bullet}{=} u)^\sigma]\!]_\rho &= [\![s^\sigma \overset{\bullet}{=} u^\sigma]\!]_\rho \\
&= \{\underline{\mathbf{ok}} \mid a \in [\![s^\sigma]\!]_\rho, b \in [\![u^\sigma]\!]_\rho, a = b\} \\
&= \{\underline{\mathbf{ok}} \mid a \in [\![s]\!]_{\rho[x_1 \mapsto a_1] \ldots [x_n \mapsto a_n]}, b \in [\![u]\!]_{\rho[x_1 \mapsto a_1] \ldots [x_n \mapsto a_n]}, a = b\} \ \text{(By } i.h.\text{)} \\
&= [\![s \overset{\bullet}{=} u]\!]_{\rho[x_1 \mapsto a_1] \ldots [x_n \mapsto a_n]}
\end{aligned}$$

7. **Guarded expression,** $t = s; u$**.** Then:

$$\begin{aligned}
[\![(s; u)^\sigma]\!]_\rho &= [\![s^\sigma; u^\sigma]\!]_\rho \\
&= \{a \mid b \in [\![s^\sigma]\!]_\rho, a \in [\![u^\sigma]\!]_\rho\} \\
&= \{a \mid b \in [\![s]\!]_{\rho[x_1 \mapsto a_1] \ldots [x_n \mapsto a_n]}, a \in [\![u]\!]_{\rho[x_1 \mapsto a_1] \ldots [x_n \mapsto a_n]}\} \ \text{(By } i.h.\text{)} \\
&= [\![s; u]\!]_{\rho[x_1 \mapsto a_1] \ldots [x_n \mapsto a_n]}
\end{aligned}$$

8. **Fresh,** $t = \nu x^A.\, s$**.** Then:

$$\begin{aligned}
[\![(\nu x^A.\, s)^\sigma]\!]_\rho &= [\![\nu x^A.\, s^\sigma]\!]_\rho \\
&= \{b \mid a \in [\![A]\!], b \in [\![s^\sigma]\!]_{\rho[x \mapsto a]}\} \\
&= \{b \mid a \in [\![A]\!], b \in [\![s]\!]_{\rho[x \mapsto a][x_1 \mapsto a_1] \ldots [x_n \mapsto a_n]}\} \ \text{(By } i.h.\text{)} \\
&= \{b \mid a \in [\![A]\!], b \in [\![s]\!]_{\rho[x_1 \mapsto a_1] \ldots [x_n \mapsto a_n][x \mapsto a]}\} \ \text{(Since } x \notin \{x_1, \ldots, x_n\}\text{)} \\
&= [\![\nu x^A.\, s]\!]_{\rho[x_1 \mapsto a_1] \ldots [x_n \mapsto a_n]}
\end{aligned}$$

9. **Fail,** $P = \texttt{fail}$**.** Immediate, as:

$$[\![\texttt{fail}^\sigma]\!]_\rho = [\![\texttt{fail}]\!]_\rho = \varnothing = [\![\texttt{fail}]\!]_{\rho[x_1 \mapsto a_1] \ldots [x_n \mapsto a_n]}$$

10. **Alternative,** $P = t \oplus P$**.** Then:

$$\begin{aligned}
[\![(t \oplus P)^\sigma]\!]_\rho &= [\![t^\sigma \oplus P^\sigma]\!]_\rho \\
&= [\![t^\sigma]\!]_\rho \cup [\![P^\sigma]\!]_\rho \\
&= [\![t]\!]_{\rho[x_1 \mapsto a_1] \ldots [x_n \mapsto a_n]} \cup [\![P]\!]_{\rho[x_1 \mapsto a_1] \ldots [x_n \mapsto a_n]} \ \text{(By } i.h.\text{)} \\
&= [\![t \oplus P]\!]_{\rho[x_1 \mapsto a_1] \ldots [x_n \mapsto a_n]}
\end{aligned}$$

A.10 Proof of Thm. 6.2 — Soundness

Definition A.1 (Goal satisfaction). *Let ρ be a fixed variable assignment, and let $\boldsymbol{x}^{\boldsymbol{A}}$ be a fixed sequence of variables. Moreover, let $\mathsf{G} = \{(\mathtt{v}_1 \stackrel{\bullet}{=} \mathtt{w}_1), \dots, (\mathtt{v}_n \stackrel{\bullet}{=} \mathtt{w}_n)\}$ be a unification problem. Given a sequence of elements $\boldsymbol{a} \in [\![\boldsymbol{A}]\!]$ we say that $\boldsymbol{a}$* satisfies G *(with respect to $\rho, \boldsymbol{x}$), written $\boldsymbol{a} \vDash_{\rho,\boldsymbol{x}} \mathsf{G}$, if and only if $[\![\mathtt{v}_i]\!]_{\rho[\boldsymbol{x}\mapsto\boldsymbol{a}]} = [\![\mathtt{w}_i]\!]_{\rho[\boldsymbol{x}\mapsto\boldsymbol{a}]}$ for all $i = 1..n$. We write $\boldsymbol{a} \vDash \mathsf{G}$ if ρ and $\boldsymbol{x}$ are clear from the context.*

Lemma A.2 (Unification preserves satisfaction). *Let $\mathsf{G} \rightsquigarrow \mathsf{H}$ be a step of the unification algorithm that does not fail. Then for any $\rho, \boldsymbol{x}^{\boldsymbol{A}}$ we have that:*

$$\{\boldsymbol{a} \mid \boldsymbol{a} \vDash_{\rho,\boldsymbol{x}} \mathsf{G}\} = \{\boldsymbol{a} \mid \boldsymbol{a} \vDash_{\rho,\boldsymbol{x}} \mathsf{H}\}$$

Proof. Note that the step does not fail so it cannot be the result of applying the `u-clash` or the `u-occurs-check` rules. We consider the five remaining cases:

1. `u-delete`: Our goal is to prove that:

   $$\{\boldsymbol{a} \mid \boldsymbol{a} \vDash_{\rho,\boldsymbol{x}} \{y \stackrel{\bullet}{=} y\} \uplus \mathsf{G}'\} = \{\boldsymbol{a} \mid \boldsymbol{a} \vDash_{\rho,\boldsymbol{x}} \mathsf{G}'\}$$

   This is immediate since $[\![y]\!]_{\rho[\boldsymbol{x}\mapsto\boldsymbol{a}]} = [\![y]\!]_{\rho[\boldsymbol{x}\mapsto\boldsymbol{a}]}$ always holds.
2. `u-orient`: Our goal is to prove that: $\{\boldsymbol{a} \mid \boldsymbol{a} \vDash_{\rho,\boldsymbol{x}} \{\mathtt{v} \stackrel{\bullet}{=} y\} \uplus \mathsf{G}'\} = \{\boldsymbol{a} \mid \boldsymbol{a} \vDash_{\rho,\boldsymbol{x}} \{y \stackrel{\bullet}{=} \mathtt{v}\} \uplus \mathsf{G}'\}$. Immediate by definition.
3. `u-match-lam`: Our goal is to prove that:

   $$\{\boldsymbol{a} \mid \boldsymbol{a} \vDash_{\rho,\boldsymbol{x}} \{\lambda^\ell y.\, P \stackrel{\bullet}{=} \lambda^\ell y.\, P\} \uplus \mathsf{G}'\} = \{\boldsymbol{a} \mid \boldsymbol{a} \vDash_{\rho,\boldsymbol{x}} \mathsf{G}'\}$$

   This is immediate since $[\![\lambda^\ell y.\, P]\!]_{\rho[\boldsymbol{x}\mapsto\boldsymbol{a}]} = [\![\lambda^\ell y.\, P]\!]_{\rho[\boldsymbol{x}\mapsto\boldsymbol{a}]}$ always holds.
4. `u-match-cons`: Our goal is to prove that:

   $$\{\boldsymbol{a} \mid \boldsymbol{a} \vDash_{\rho,\boldsymbol{x}} \{\mathbf{c}\,\mathtt{v}_1 \dots \mathtt{v}_n \stackrel{\bullet}{=} \mathbf{c}\,\mathtt{w}_1 \dots \mathtt{w}_n\} \uplus \mathsf{G}'\} = \{\boldsymbol{a} \mid \boldsymbol{a} \vDash_{\rho,\boldsymbol{x}} \{\mathtt{v}_1 \stackrel{\bullet}{=} \mathtt{w}_1, \dots, \mathtt{v}_n \stackrel{\bullet}{=} \mathtt{w}_n\} \uplus \mathsf{G}'\}$$

   Recall that $[\![\mathbf{c}]\!]_{\rho[\boldsymbol{x}\mapsto\boldsymbol{a}]} = \{\underline{\mathbf{c}}\}$ is $\mathcal{T}_{\mathbf{c}}$-unitary, and the interpretation of a value is always a singleton (Lem. 6.1), so let $[\![\mathtt{v}_i]\!]_{\rho[\boldsymbol{x}\mapsto\boldsymbol{a}]} = \{b_i\}$ and $[\![\mathtt{w}_i]\!]_{\rho[\boldsymbol{x}\mapsto\boldsymbol{a}]} = \{b'_i\}$. It suffices to note that:

   $$\begin{array}{ll} & \boldsymbol{a} \vDash_{\rho,\boldsymbol{x}} \{\mathbf{c}\,\mathtt{v}_1 \dots \mathtt{v}_n \stackrel{\bullet}{=} \mathbf{c}\,\mathtt{w}_1 \dots \mathtt{w}_n\} \\ \iff & [\![\mathbf{c}\,\mathtt{v}_1 \dots \mathtt{v}_n]\!]_{\rho[\boldsymbol{x}\mapsto\boldsymbol{a}]} = [\![\mathbf{c}\,\mathtt{w}_1 \dots \mathtt{w}_n]\!]_{\rho[\boldsymbol{x}\mapsto\boldsymbol{a}]} \\ \iff & \underline{\mathbf{c}}(b_1) \dots (b_n) = \underline{\mathbf{c}}(b'_1) \dots (b'_n) \\ \iff & b_i = b'_i \text{ for all } i = 1..n \qquad (\star) \\ \iff & [\![\mathtt{v}_i]\!]_{\rho[\boldsymbol{x}\mapsto\boldsymbol{a}]} = [\![\mathtt{w}_i]\!]_{\rho[\boldsymbol{x}\mapsto\boldsymbol{a}]}, \text{ for all } i = 1..n \\ \iff & \boldsymbol{a} \vDash_{\rho,\boldsymbol{x}} \{\mathtt{v}_1 \stackrel{\bullet}{=} \mathtt{w}_1, \dots, \mathtt{v}_n \stackrel{\bullet}{=} \mathtt{w}_n\} \end{array}$$

   The step $(\star)$ is justified by the fact that we assume that constructors are injective.
5. `u-eliminate`: Our goal is to prove that:

   $$\{\boldsymbol{a} \mid \boldsymbol{a} \vDash_{\rho,\boldsymbol{x}} \{y \stackrel{\bullet}{=} \mathtt{v}\} \uplus \mathsf{G}'\} = \{\boldsymbol{a} \mid \boldsymbol{a} \vDash_{\rho,\boldsymbol{x}} \{y \stackrel{\bullet}{=} \mathtt{v}\} \uplus \mathsf{G}'\{y := \mathtt{v}\}\}$$

if $y \in \mathsf{fv}(\mathsf{G}') \setminus \mathsf{fv}(\mathtt{v})$. Moreover, let $\mathsf{G}' = \{(\mathtt{v}_1 \doteq \mathtt{w}_1), \dots, (\mathtt{v}_n \doteq \mathtt{w}_n)\}$. Recall that the interpretation of a value is always a singleton (Lem. 6.1), so let $[\![\mathtt{v}]\!]_{\rho[\boldsymbol{x}\mapsto\boldsymbol{a}]} = \{b\}$. Let $\boldsymbol{a} \in [\![\boldsymbol{A}]\!]$. It suffices to show that whenever $\rho[\boldsymbol{x} \mapsto \boldsymbol{a}](y) = b$ then the following equivalence holds:

$$\boldsymbol{a} \vDash_{\rho,\boldsymbol{x}} \mathsf{G}' \iff \boldsymbol{a} \vDash_{\rho,\boldsymbol{x}} \mathsf{G}'\{y := \mathtt{v}\}$$

Note that, for each fixed $i = 1..n$:

$$\begin{aligned} [\![\mathtt{v}_i]\!]_{\rho[\boldsymbol{x}\mapsto\boldsymbol{a}]} &= [\![\mathtt{v}_i]\!]_{\rho[\boldsymbol{x}\mapsto\boldsymbol{a}][y\mapsto b]} && (\star) \\ &= [\![\mathtt{v}_i\{y := \mathtt{v}\}]\!]_{\rho[\boldsymbol{x}\mapsto\boldsymbol{a}]} && \text{(By Lem. 6.1)} \end{aligned}$$

The step $(\star)$ is trivial because, as we have already noted, $\rho[\boldsymbol{x} \mapsto \boldsymbol{a}](y) = b$ so $\rho[\boldsymbol{x} \mapsto \boldsymbol{a}]$ and $\rho[\boldsymbol{x} \mapsto \boldsymbol{a}][y \mapsto b]$ are the same variable assignment. And, similarly, $[\![\mathtt{w}_i]\!]_{\rho[\boldsymbol{x}\mapsto\boldsymbol{a}]} = [\![\mathtt{w}_i\{y := \mathtt{v}\}]\!]_{\rho[\boldsymbol{x}\mapsto\boldsymbol{a}]}$. Then:

$$\begin{aligned} & \boldsymbol{a} \vDash_{\rho,\boldsymbol{x}} \mathsf{G}' \\ \iff & [\![\mathtt{v}_i]\!]_{\rho[\boldsymbol{x}\mapsto\boldsymbol{a}]} = [\![\mathtt{w}_i]\!]_{\rho[\boldsymbol{x}\mapsto\boldsymbol{a}]} \text{ for all } i = 1..n \\ \iff & [\![\mathtt{v}_i\{y := \mathtt{v}\}]\!]_{\rho[\boldsymbol{x}\mapsto\boldsymbol{a}]} = [\![\mathtt{w}_i\{y := \mathtt{v}\}]\!]_{\rho[\boldsymbol{x}\mapsto\boldsymbol{a}]} \text{ for all } i = 1..n \text{ (Lem. 6.1)} \\ \iff & \boldsymbol{a} \vDash_{\rho,\boldsymbol{x}} \mathsf{G}'\{y := \mathtt{v}\} \end{aligned}$$

The following theorem generalizes Thm. 6.2:

Theorem A.10.3 (Soundness). *Let $\Gamma \vdash P : A$ and $P \to Q$. Let $\Phi = \mathsf{fv}(P)$ and $\Phi' = \mathsf{fv}(Q)$. Then for any variable assignment ρ:*

$$[\![P]\!]^{\Phi}_{\rho} \supseteq [\![Q]\!]^{\Phi'}_{\rho}$$

Moreover, the inclusion is an equality for all reduction rules other than the `fail` *rule.*

Proof. Let $P \to Q$. We consider six cases, depending on the rule applied to conclude that $P \to Q$:

1. `alloc`: Note that $\Phi = \Phi'$, and suppose that $\Phi = \boldsymbol{y}^{\boldsymbol{B}}$. Then:

$$\begin{aligned} [\![P_1 \oplus \mathsf{W}\langle \lambda x^A.\, Q\rangle \oplus P_2]\!]^{\Phi}_{\rho} &= \{a \mid \boldsymbol{b} \in [\![\boldsymbol{B}]\!], a \in [\![P_1 \oplus \mathsf{W}\langle \lambda x^A.\, Q\rangle \oplus P_2]\!]_{\rho[\boldsymbol{y}\mapsto\boldsymbol{b}]}\} \\ &= \{a \mid \boldsymbol{b} \in [\![\boldsymbol{B}]\!], a \in [\![P_1 \oplus \mathsf{W}\langle \lambda^{\ell} x^A.\, Q\rangle \oplus P_2]\!]_{\rho[\boldsymbol{y}\mapsto\boldsymbol{b}]}\} \ (\star) \\ &= [\![P_1 \oplus \mathsf{W}\langle \lambda^{\ell} x^A.\, Q\rangle \oplus P_2]\!]^{\Phi}_{\rho} \end{aligned}$$

   To justify $(\star)$, note that, by Compositionality (Lem. 6.1), it suffices to prove that $[\![\lambda x^A.\, Q]\!]_{\rho[\boldsymbol{y}\mapsto\boldsymbol{b}]} = [\![\lambda^{\ell} x^A.\, Q]\!]_{\rho[\boldsymbol{y}\mapsto\boldsymbol{b}]}$ for all $\boldsymbol{b} \in [\![B]\!]$. This holds by definition so we are done.
2. `beta`: Note that $\Phi = \Phi', \boldsymbol{z}^{\boldsymbol{C}}$ where

$$\boldsymbol{z} = \begin{cases} \varnothing & \text{if } x \notin \mathsf{fv}(Q) \\ \mathsf{fv}(\mathtt{v}) \setminus \mathsf{fv}(P_1 \oplus \mathsf{W}\langle(\lambda x.\, Q)\Box\rangle \oplus P_2) & \text{if } x \in \mathsf{fv}(Q) \end{cases}$$

Moreover, suppose that $\Phi' = \boldsymbol{y}^{\boldsymbol{B}}$. Then:

$$\begin{array}{ll} & [\![P_1 \oplus \mathsf{W}\langle(\lambda^\ell x^A.\, Q)\,\mathtt{v}\rangle \oplus P_2]\!]_\rho^{\boldsymbol{y}^{\boldsymbol{B}},\boldsymbol{z}^{\boldsymbol{C}}} \\ = & \{a \mid \boldsymbol{b} \in [\![\boldsymbol{B}]\!], \boldsymbol{c} \in [\![\boldsymbol{C}]\!], a \in [\![P_1 \oplus \mathsf{W}\langle(\lambda^\ell x^A.\, Q)\,\mathtt{v}\rangle \oplus P_2]\!]_{\rho[\boldsymbol{y}\mapsto\boldsymbol{b}][\boldsymbol{z}\mapsto\boldsymbol{c}]}\} \\ = & \{a \mid \boldsymbol{b} \in [\![\boldsymbol{B}]\!], a \in [\![P_1 \oplus \mathsf{W}\langle Q\{x^A := \mathtt{v}\}\rangle \oplus P_2]\!]_{\rho[\boldsymbol{y}\mapsto\boldsymbol{b}]}\} \qquad (\star) \\ = & [\![P_1 \oplus \mathsf{W}\langle Q\{x^A := \mathtt{v}\}\rangle \oplus P_2]\!]_\rho^{\boldsymbol{y}^{\boldsymbol{B}}} \end{array}$$

To justify $(\star)$ we proceed as follows. Let us write ρ' for $\rho[\boldsymbol{y} \mapsto \boldsymbol{b}]$. Recall that the interpretation of a value is always a singleton (Lem. 6.1), so let $[\![\mathtt{v}]\!]_{\rho'[\boldsymbol{z}\mapsto\boldsymbol{c}]} = \{a_0\}$. By Compositionality (Lem. 6.1) it suffices to note that:

$$\begin{array}{rll} [\![(\lambda^\ell x^A.\, Q)\,\mathtt{v}]\!]_{\rho'[\boldsymbol{z}\mapsto\boldsymbol{c}]} & = \{b \mid a \in [\![\mathtt{v}]\!]_{\rho'[\boldsymbol{z}\mapsto\boldsymbol{c}]}, b \in [\![Q]\!]_{\rho'[\boldsymbol{z}\mapsto\boldsymbol{c}][x^A\mapsto a]}\} & \\ & = [\![Q]\!]_{\rho'[\boldsymbol{z}\mapsto\boldsymbol{c}][x^A\mapsto a_0]} & \\ & = [\![Q]\!]_{\rho'[x^A\mapsto a_0]} & \text{(By Irrelevance (Lem. 6.1))} \\ & = [\![Q\{x^A := \mathtt{v}\}]\!]_{\rho'} & \text{(By Lem. 6.1)} \end{array}$$

3. $\mathtt{guard}$: Note that $\Phi = \Phi', \boldsymbol{z}^{\boldsymbol{C}}$, where $\boldsymbol{z}^{\boldsymbol{C}} = \mathsf{fv}(\mathtt{v}) \setminus \mathsf{fv}(P_1 \oplus \mathsf{W}\langle\Box; t\rangle \oplus P_2)$. Suppose that $\Phi' = \boldsymbol{y}^{\boldsymbol{B}}$. Then:

$$\begin{array}{rl} [\![P_1 \oplus \mathsf{W}\langle\mathtt{v}; t\rangle \oplus P_2]\!]_\rho^{\boldsymbol{y}^{\boldsymbol{B}},\boldsymbol{z}^{\boldsymbol{C}}} & = \{a \mid \boldsymbol{b} \in [\![\boldsymbol{B}]\!], \boldsymbol{c} \in [\![\boldsymbol{C}]\!], a \in [\![P_1 \oplus \mathsf{W}\langle\mathtt{v}; t\rangle \oplus P_2]\!]_{\rho[\boldsymbol{y}\mapsto\boldsymbol{b}][\boldsymbol{z}\mapsto\boldsymbol{c}]}\} \\ & = \{a \mid \boldsymbol{b} \in [\![\boldsymbol{B}]\!], a \in [\![P_1 \oplus \mathsf{W}\langle t\rangle \oplus P_2]\!]_{\rho[\boldsymbol{y}\mapsto\boldsymbol{b}]}\} \qquad (\star) \\ & = [\![P_1 \oplus \mathsf{W}\langle t\rangle \oplus P_2]\!]_\rho^{\boldsymbol{y}^{\boldsymbol{B}}} \end{array}$$

To justify $(\star)$ we proceed as follows. Let us write ρ' for $\rho[\boldsymbol{y} \mapsto \boldsymbol{b}]$. Recall that the interpretation of a value is always a singleton (Lem. 6.1), so let $[\![\mathtt{v}]\!]_{\rho'[\boldsymbol{z}\mapsto\boldsymbol{c}]} = \{b_0\}$. By Compositionality (Lem. 6.1) it suffices to note that:

$$\begin{array}{rl} [\![\mathtt{v}; t]\!]_{\rho'[\boldsymbol{z}\mapsto c]} & = \{a \mid b \in [\![\mathtt{v}]\!]_{\rho'[\boldsymbol{z}\mapsto\boldsymbol{c}]}, a \in [\![t]\!]_{\rho'[\boldsymbol{z}\mapsto\boldsymbol{c}]}\} \text{ (By Irrelevance Lem. 6.1)} \\ & = [\![t]\!]_{\rho'} \end{array}$$

4. $\mathtt{fresh}$: Note that $\Phi' = \Phi, y^A$ where y is a fresh variable. Suppose that $\Phi = \boldsymbol{z}^{\boldsymbol{B}}$. Then:

$$\begin{array}{rl} [\![P_1 \oplus \mathsf{W}\langle\nu x^A.\, t\rangle \oplus P_2]\!]_\rho^{\Phi} & = \{a \mid \boldsymbol{b} \in [\![\boldsymbol{B}]\!], a \in [\![P_1 \oplus \mathsf{W}\langle\nu x^A.\, t\rangle \oplus P_2]\!]_{\rho[\boldsymbol{z}\mapsto\boldsymbol{b}]}\} \\ & = \{a \mid \boldsymbol{b} \in [\![\boldsymbol{B}]\!], a \in [\![P_1 \oplus \mathsf{W}\langle t\{x^A := y^A\}\rangle \oplus P_2]\!]_{\rho[\boldsymbol{z}\mapsto\boldsymbol{b}]}^{y^A}\} \; (\star) \\ & = [\![P_1 \oplus \mathsf{W}\langle t\{x^A := y^A\}\rangle \oplus P_2]\!]_\rho^{\Phi, y^A} \end{array}$$

To justify $(\star)$ we proceed as follows. Let ρ' stand for $\rho[\boldsymbol{z} \mapsto \boldsymbol{b}]$. By Irrelevance (Lem. 6.1), $[\![P_1]\!]_{\rho'} = [\![P_1]\!]_{\rho'}^{y^A}$. Similarly, $[\![P_2]\!]_{\rho'} = [\![P_2]\!]_{\rho'}^{y^A}$. By Compositionality (Lem. 6.1), it suffices to show that $[\![\mathsf{W}\langle\nu x^A.\, t\rangle]\!]_{\rho'} = [\![\mathsf{W}\langle t\{x^A := y^A\}\rangle]\!]_{\rho'}^{y^A}$. Indeed:

$$\begin{array}{lll} & [\![\mathsf{W}\langle\nu x^A.\, t\rangle]\!]_{\rho'} & \\ = & \{c \mid b \in [\![\nu x^A.\, t]\!]_{\rho'}, c \in [\![\mathsf{W}]\!]_{\rho'[\Box\mapsto b]}\} & \text{(By Lem. 6.1)} \\ = & \{c \mid a \in [\![A]\!], b \in [\![t]\!]_{\rho'[x^A\mapsto a]}, c \in [\![\mathsf{W}]\!]_{\rho'[\Box\mapsto b]}\} & \\ = & \{c \mid a \in [\![A]\!], b \in [\![t\{x^A := y^A\}]\!]_{\rho'[y^A\mapsto a]}, c \in [\![\mathsf{W}]\!]_{\rho'[\Box\mapsto b]}\} & \text{(By Lem. 6.1 and Lem. 6.1)} \\ = & \{c \mid a \in [\![A]\!], b \in [\![t\{x^A := y^A\}]\!]_{\rho'[y^A\mapsto a]}, c \in [\![\mathsf{W}]\!]_{\rho'[y^A\mapsto a][\Box\mapsto b]}\} & \text{(By Lem. 6.1)} \\ = & \{c \mid a \in [\![A]\!], c \in [\![\mathsf{W}\langle t\{x^A := y^A\}\rangle]\!]_{\rho'[y^A\mapsto a]}\} & \text{(By Lem. 6.1)} \\ = & [\![\mathsf{W}\langle t\{x^A := y^A\}\rangle]\!]_{\rho'}^{y^A} & \end{array}$$

5. $\mathtt{unif}$: Our goal is to prove that $[\![P_1 \oplus \mathsf{W}\langle \mathtt{v} \stackrel{\bullet}{=} \mathtt{w}\rangle \oplus P_2]\!]_\rho^{\Phi} = [\![P_1 \oplus \mathsf{W}\langle \mathbf{ok}\rangle^\sigma \oplus P_2]\!]_\rho^{\Phi'}$, where $\sigma = \mathsf{mgu}(\{\mathtt{v} \stackrel{\bullet}{=} \mathtt{w}\})$. Note that Φ' is a subset of Φ, so suppose that $\Phi = \Phi', \boldsymbol{y}^{\boldsymbol{B}}$ and $\Phi' = \boldsymbol{x}^{\boldsymbol{A}}$. Note also that $\sigma = \mathsf{mgu}(\mathtt{v} \stackrel{\bullet}{=} \mathtt{w})$ exists, so $\{\mathtt{v} \stackrel{\bullet}{=} \mathtt{w}\} \rightsquigarrow^* \{x_1 \stackrel{\bullet}{=} \mathtt{v}_1, \dots, x_n \stackrel{\bullet}{=} \mathtt{v}_n\}$ such that $x_i \notin \mathsf{fv}(\mathtt{v}_j)$ for all i, j, and the most general unifier is $\sigma = \{x_1 \mapsto \mathtt{v}_1, \dots, x_n \mapsto \mathtt{v}_n\}$. Moreover, recall that the interpretation of a value is always a singleton (Lem. 6.1), so for each fixed assignment ρ' let us write $b_i^{\rho'}$ for the only element in $[\![\mathtt{v}_i]\!]_{\rho'}$. Moreover, let $\boldsymbol{z}^{\boldsymbol{C}} = \boldsymbol{x}^{\boldsymbol{A}}, \boldsymbol{y}^{\boldsymbol{B}}$. By Compositionality (Lem. 6.1) and Irrelevance (Lem. 6.1), it suffices to note that:

$$
\begin{array}{ll}
[\![\mathsf{W}\langle \mathtt{v} \stackrel{\bullet}{=} \mathtt{w}\rangle]\!]_\rho^{\boldsymbol{z}^{\boldsymbol{C}}} & \\
= \{a \mid \boldsymbol{c} \in [\![\boldsymbol{C}]\!], a \in [\![\mathsf{W}\langle \mathtt{v} \stackrel{\bullet}{=} \mathtt{w}\rangle]\!]_{\rho[\boldsymbol{z}\mapsto\boldsymbol{c}]}\} & \\
= \{a \mid \boldsymbol{c} \in [\![\boldsymbol{C}]\!], b \in [\![\mathtt{v} \stackrel{\bullet}{=} \mathtt{w}]\!]_{\rho[\boldsymbol{z}\mapsto\boldsymbol{c}]}, a \in [\![\mathsf{W}]\!]_{\rho[\boldsymbol{z}\mapsto\boldsymbol{c}][\Box\mapsto b]}\} & \text{(By Lem. 6.1)} \\
= \{a \mid \boldsymbol{c} \in [\![\boldsymbol{C}]\!], b \in [\![\mathtt{v} \stackrel{\bullet}{=} \mathtt{w}]\!]_{\rho[\boldsymbol{z}\mapsto\boldsymbol{c}]}, a \in [\![\mathsf{W}]\!]_{\rho[\boldsymbol{z}\mapsto\boldsymbol{c}][\Box\mapsto\underline{\mathbf{ok}}]}\} & \\
= \{a \mid \boldsymbol{c} \in [\![\boldsymbol{C}]\!], \boldsymbol{c} \vDash_{\rho,\boldsymbol{z}} \{\mathtt{v} \stackrel{\bullet}{=} \mathtt{w}\}, a \in [\![\mathsf{W}]\!]_{\rho[\boldsymbol{z}\mapsto\boldsymbol{c}][\Box\mapsto\underline{\mathbf{ok}}]}\} & \\
= \{a \mid \boldsymbol{c} \in [\![\boldsymbol{C}]\!], \boldsymbol{c} \vDash_{\rho,\boldsymbol{z}} \{x_1 \stackrel{\bullet}{=} \mathtt{v}_1, \dots, x_n \stackrel{\bullet}{=} \mathtt{v}_n\}, a \in [\![\mathsf{W}]\!]_{\rho[\boldsymbol{z}\mapsto\boldsymbol{c}][\Box\mapsto\underline{\mathbf{ok}}]}\} & \text{(By Lem. A.2)} \\
= \{a \mid \boldsymbol{c} \in [\![\boldsymbol{C}]\!], \rho[\boldsymbol{z}\mapsto\boldsymbol{c}](x_i) = b_i^{\rho[\boldsymbol{z}\mapsto\boldsymbol{c}]} \text{ for all } i,\ a \in [\![\mathsf{W}\langle\mathbf{ok}\rangle]\!]_{\rho[\boldsymbol{z}\mapsto\boldsymbol{c}]}\} & \text{(By Lem. 6.1)} \\
= \{a \mid \boldsymbol{c} \in [\![\boldsymbol{C}]\!], a \in [\![\mathsf{W}\langle\mathbf{ok}\rangle]\!]_{\rho[\boldsymbol{z}\mapsto\boldsymbol{c}][x_1\mapsto b_1^{\rho[\boldsymbol{z}\mapsto\boldsymbol{c}]}]\dots[x_n\mapsto b_n^{\rho[\boldsymbol{z}\mapsto\boldsymbol{c}]}]}\} & (\star) \\
= \{a \mid \boldsymbol{c} \in [\![\boldsymbol{C}]\!], a \in [\![\mathsf{W}\langle\mathbf{ok}\rangle^\sigma]\!]_{\rho[\boldsymbol{z}\mapsto\boldsymbol{c}]}\} & \text{(By Lem. 6.1)} \\
= [\![\mathsf{W}\langle\mathbf{ok}\rangle^\sigma]\!]_\rho^{\boldsymbol{z}^{\boldsymbol{C}}} & \\
= [\![\mathsf{W}\langle\mathbf{ok}\rangle^\sigma]\!]_\rho^{\boldsymbol{x}^{\boldsymbol{A}}} & \text{(By Lem. 6.1)}
\end{array}
$$

To justify $(\star)$ note that $\rho[\boldsymbol{z}\mapsto\boldsymbol{c}](x_i) = \{b_i^{\rho[\boldsymbol{z}\mapsto\boldsymbol{c}]}\}$ for all $i = 1..n$. Therefore, we can write $\rho[\boldsymbol{z}\mapsto\boldsymbol{c}]$ as $\rho[\boldsymbol{z}\mapsto\boldsymbol{c}][x_1 \mapsto b_1^{\rho[\boldsymbol{z}\mapsto\boldsymbol{c}]}]\dots[x_n \mapsto b_n^{\rho[\boldsymbol{z}\mapsto\boldsymbol{c}]}]$.

6. $\mathtt{fail}$: Our goal is to prove that:

$$[\![P_1 \oplus \mathsf{W}\langle \mathtt{v} \stackrel{\bullet}{=} \mathtt{w}\rangle \oplus P_2]\!]_\rho^{\Phi} \supseteq [\![P_1 \oplus P_2]\!]_\rho^{\Phi'}$$

which is immediate by definition.

References

1. Albert, E., Hanus, M., Huch, F., Oliver, J., Vidal, G.: Operational semantics for functional logic languages. Electronic Notes in Theoretical Computer Science **76**, 1–19 (2002)
2. Arbiser, A., Miquel, A., Ríos, A.: A lambda-calculus with constructors. In: International Conference on Rewriting Techniques and Applications. pp. 181–196. Springer (2006)
3. Ayala-Rincón, M., Bonelli, E., Edi, J., Viso, A.: Typed path polymorphism. Theoretical Computer Science **781**, 111–130 (2019)
4. Baader, F., Nipkow, T.: Term Rewriting and All That. Cambridge University Press (1999)
5. Barendregt, H.: The Lambda Calculus: Its Syntax and Semantics, vol. 103. Elsevier (1984)

6. Barendregt, H., Dekkers, W., Statman, R.: Lambda calculus with types. Cambridge University Press (2013)
7. Byrd, W.E.: Relational programming in miniKanren: techniques, applications, and implementations. [Bloomington, Ind.]: Indiana University (2010)
8. Chakravarty, M.M., Guo, Y., Köhler, M., Lock, H.C.: Goffin: Higher-order functions meet concurrent constraints. Science of Computer Programming **30**(1-2), 157–199 (1998)
9. Faggian, C., Rocca, S.R.D.: Lambda calculus and probabilistic computation. In: 34th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2019, Vancouver, BC, Canada, June 24-27, 2019. pp. 1–13. IEEE (2019)
10. Friedman, D.P., Byrd, W.E., Kiselyov, O.: The Reasoned Schemer. The MIT Press (July 2005)
11. Gould, W.E.: A Matching Procedure for Omega-Order Logic. Ph.D. thesis, Princeton University (1966)
12. Hanus, M.: Functional logic programming: From theory to Curry. In: Programming Logics - Essays in Memory of Harald Ganzinger. pp. 123–168. Springer LNCS 7797 (2013)
13. Hanus, M.: A unified computation model for functional and logic programming. In: Lee, P., Henglein, F., Jones, N.D. (eds.) Conference Record of POPL'97: The 24th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, Papers Presented at the Symposium, Paris, France, 15-17 January 1997. pp. 80–93. ACM Press (1997)
14. Huet, G.P.: The undecidability of unification in third order logic. Information and control **22**(3), 257–267 (1973)
15. Huet, G.P.: A unification algorithm for typed λ-calculus. Theoretical Computer Science **1**(1), 27–57 (1975)
16. Jay, B., Kesner, D.: Pure pattern calculus. In: European Symposium on Programming. pp. 100–114. Springer (2006)
17. Klop, J.W., Van Oostrom, V., De Vrijer, R.: Lambda calculus with patterns. Theoretical Computer Science **398**(1-3), 16–31 (2008)
18. Levy, J., Veanes, M.: On the undecidability of second-order unification. Information and Computation **159**(1-2), 125–150 (2000)
19. Martelli, A., Montanari, U.: An efficient unification algorithm. ACM Transactions on Programming Languages and Systems (TOPLAS) **4**(2), 258–282 (1982)
20. Miller, D.: A logic programming language with lambda-abstraction, function variables, and simple unification. Journal of logic and computation **1**(4), 497–536 (1991)
21. Miller, D.: Unification of simply typed lambda-terms as logic programming. Tech. Rep. MS-CIS-91-24, University of Pennsylvania (1991)
22. Miller, D., Nadathur, G.: Programming with higher-order logic. Cambridge University Press (2012)
23. Milner, R.: A theory of type polymorphism in programming. Journal of computer and system sciences **17**(3), 348–375 (1978)
24. Nadathur, G., Miller, D.: Higher-order logic programming. Proceedings of the Third International Logic Programming Conference pp. 448–462 (1984)
25. Petit, B.: Semantics of typed lambda-calculus with constructors. Log. Methods Comput. Sci. **7**(1) (2011)
26. Ramsey, N., Pfeffer, A.: Stochastic lambda calculus and monads of probability distributions. In: Proceedings of the 29th ACM SIGPLAN-SIGACT symposium on Principles of programming languages. pp. 154–165 (2002)

27. Rozplokhas, D., Vyatkin, A., Boulytchev, D.: Certified semantics for minikanren. In: Proceedings of the 2019 miniKanren and Relational Programming Workshop. pp. 80–98 (2019)
28. Schmidt-Schauß, M., Huber, M.: A lambda-calculus with letrec, case, constructors and non-determinism. arXiv preprint cs/0011008 (2000)
29. Smolka, G.: A foundation for higher-order concurrent constraint programming. In: Mathematical Methods in Program Development, pp. 433–458. Springer (1997)
30. Somogyi, Z., Henderson, F., Conway, T.: The execution algorithm of mercury, an efficient purely declarative logic programming language. The Journal of Logic Programming **29**(1-3), 17–64 (1996)
31. The Coq Development Team: The Coq proof assistant reference manual. LogiCal Project (2004), http://coq.inria.fr, version 8.0
32. Urban, C., Pitts, A.M., Gabbay, M.J.: Nominal unification. Theoretical Computer Science **323**(1-3), 473–497 (2004)
33. Van Roy, P.: Multiparadigm Programming in Mozart/Oz: Second International Conference, MOZ 2004, Charleroi, Belgium, October 7-8, 2004, Revised Selected Papers, vol. 3389. Springer (2005)