On Type-Cases, Union Elimination, and Occurrence Typing

GIUSEPPE CASTAGNA, CNRS, Université de Paris, France
MICKAËL LAURENT, Université de Paris, France
KIM NGUYỄN, Université Paris-Saclay, France
MATTHEW LUTZE, Université de Paris, France

We extend classic union and intersection type systems with a type-case construction and show that the combination of the union elimination rule of the former and the typing rules for type-cases of our extension encompasses *occurrence typing*. To apply this system in practice, we define a canonical form for the expressions of our extension, called MSC-form. We show that an expression of the extension is typable if and only if its MSC-form is, and reduce the problem of typing the latter to the one of reconstructing annotations for that term. We provide a sound algorithm that performs this reconstruction and a proof-of-concept implementation.

CCS Concepts: • **Theory of computation** → *Type structures*; *Program analysis*; • **Software and its engineering** → *Functional languages*.

Additional Key Words and Phrases: subtyping, union types, intersection types, type-case, dynamic languages, type systems.

ACM Reference Format:
Giuseppe Castagna, Mickaël Laurent, Kim Nguyễn, and Matthew Lutze. 2022. On Type-Cases, Union Elimination, and Occurrence Typing. *Proc. ACM Program. Lang.* 6, POPL, Article 13 (January 2022), 75 pages. https://doi.org/10.1145/3498674

1 INTRODUCTION

TypeScript [Microsoft] and Flow [Facebook] are extensions of JavaScript that allow the programmer to specify in the code type annotations used to statically type-check the program. For instance, the following function definition is valid in both languages

```
function foo(x : number | string) {
  return (typeof(x) === "number")? x+1 : x.trim();
}
```
(1)

Apart from the type annotation (in red) of the function parameter, the above is standard JavaScript code defining a function that checks whether its argument is an integer; if it is so, then it returns the argument's successor (`x+1`), otherwise it calls the method `trim()` of the argument. The annotation specifies that the parameter is either a number or a string (the vertical bar denotes a union type). If this annotation is respected and the function is applied to either an integer or a string, then the application cannot fail because of a type error (`trim()` is a standard string method) and both TypeScript and Flow rightly accept this function and deduce that it will return either a number or a string, that is, a result of type `number|string`. This is possible because both type-checkers

Authors' addresses: Giuseppe Castagna, Mickaël Laurent, Matthew Lutze, Institut de Recherche en Informatique Fondamentale (IRIF), Université de Paris, CNRS, 8 place Aurélie Nemours, 75013 Paris, France; Kim Nguyễn, Laboratoire Méthodes Formelles (LMF), Université Paris-Saclay, CNRS, ENS Paris-Saclay, 91190, Gif-sur-Yvette, France.

2475-1421/2022/1-ART13
https://doi.org/10.1145/3498674

implement a specific type discipline called *occurrence typing* or *flow typing*:[1] as a matter of fact, standard type disciplines would reject this function. The reason for that is that standard type disciplines would try to type every part of the body of the function under the assumption that `x` has type `number | string` and they would fail, since the successor is not defined for strings and the method `trim()` is not defined for numbers. This is so because standard disciplines do not take into account the type test performed on `x`. Occurrence typing is the typing technique that uses the information provided by the type test to specialize—precisely, to *refine*—the type of the occurrences of `x` in the branches of the conditional: since the program tested that `x` is of type `number`, then we can safely assume that `x` is of type `number` in the "then" branch, and that it is *not* of type `number` (and thus deduce from the type annotation that it must be of type `string`) in the "else" branch.

Occurrence typing was first defined and formally studied by Tobin-Hochstadt and Felleisen [2008] to statically type-check untyped Scheme programs, and later extended by Tobin-Hochstadt and Felleisen [2010] yielding the development of Typed Racket. To that end the authors define a system to deduce propositions, that express relations between variables and types, and these are attached to functional types (*à la* effect system) to describe facts about the result of applying the corresponding functions. In this work we argue that to capture occurrence typing—and, as we detail later on, much, much more—it is not necessary to resort to effect-like systems, perform flow analysis, or invent new expressive types. It just suffices to add to the language at issue a type-case expression and combine (a tailored definition of) its typing rules with the classic union elimination rule as it was first introduced by MacQueen et al. [1986]. More precisely, let t be a type and $(e{\in}t)\,?\,e_1 : e_2$ be the type-case expression that first evaluates e to a value v and continues as e_1 if v is of type t, and as e_2 otherwise. Then we claim that all the situations in which occurrence typing is used are covered by these three typing rules.

$$\frac{\Gamma \vdash e' : t_1 \vee t_2 \qquad \Gamma, x{:}t_1 \vdash e : t \quad \Gamma, x{:}t_2 \vdash e : t}{\Gamma \vdash e\{e'/x\} : t} \qquad \frac{\Gamma \vdash e : t \quad \Gamma \vdash e_1 : t_1}{\Gamma \vdash (e{\in}t)\,?\,e_1 : e_2 : t_1} \qquad \frac{\Gamma \vdash e : \neg t \quad \Gamma \vdash e_2 : t_2}{\Gamma \vdash (e{\in}t)\,?\,e_1 : e_2 : t_2}$$

The first is the classic union elimination rule by MacQueen et al. [1986] where $e\{e'/x\}$ is the expression obtained from e by substituting e' for x and $t_1 \vee t_2$ is a *union type* (for union and intersection we respectively use `|` and `&` in code snippets and $\vee$ and $\wedge$ in formal types). If we interpret a type set-theoretically as the set of all values that have that type, then $t_1 \vee t_2$ is the type that contains all values of type t_1 and all values of type t_2. In a sound system an expression e is given a type t only if it can only produce a result in t; this implies that an expression of type $t_1 \vee t_2$ can produce a result either of type t_1 or of type t_2 . The union elimination rule states that given some expression (here, $e\{e'/x\}$) with a subexpression e' of type $t_1 \vee t_2$, if we can give to this expression the type t both under the hypothesis that e' produces a result of type t_1 and under the hypothesis the e' produces a result in t_2, then we can safely give this expression type t.

The two other rules are new and provide a natural and nifty way to type type-case expressions. The first rule states that if e can only produce a result in t, then the type of $(e{\in}t)\,?\,e_1 : e_2$ is the type of e_1. The second rule states that if e can only produce a result in $\neg t$, then the type of $(e{\in}t)\,?\,e_1 : e_2$ is the type of e_2: since the *negation type* $\neg t$ is interpreted set-theoretically as the set of all values that are *not* of type t, this means that, in that case, e can only produce a result *not* of type t.

The reader may wonder how we type a type-case expression $(e{\in}t)\,?\,e_1 : e_2$ when the tested expression e is neither of type t nor of type $\neg t$. As a matter of fact, a type-case is interesting only if we cannot statically determine whether it will succeed or fail. For instance, the type-case in (1) tests whether `x` is of type `number`, but since `x` is of type `number|string`, then it is neither of type `number` nor of type `¬number`. Here, the combination of set-theoretic types and the union rule plays its

[1] TypeScript calls it "type guard recognition" while Flow uses the terminology "type refinements".

magic. Union and negation types, give intersection types for free: just define $t_1 \wedge t_2$ as $\neg(\neg t_1 \vee \neg t_2)$. Thus, even though the tested expression e has some type s that is neither contained in (i.e., subtype of) t nor in $\neg t$, we can use intersection and negation to split s into the union of two types that have this property, since $s \simeq (s \wedge t) \vee (s \wedge \neg t)$. We can thus apply the union rule and check the type-case under the hypothesis that the tested expression has type $(s \wedge t)$ and under the hypothesis that it has type $(s \wedge \neg t)$. For instance, for (1) we check the type-case under the hypothesis that `x` has type `number` (i.e., `(number∨string)∧number`) and deduce the type `number`, and under the hypothesis that `x` has type `string` (i.e., `(number∨string)∧¬number`) and deduce the type `string`, which by subsumption gives for the whole expression the expected type `number∨string`.

We see that our treatment of occurrence typing heavily depends on the properties of *set-theoretic types*: unions, intersections, and negations of types. This does not come as a surprise since from its inception occurrence typing was intimately tied to type systems with set-theoretic types. Union was the first type connective to appear, since it was already used in [Tobin-Hochstadt and Felleisen 2008] to characterize the different control flows of a type test, as our `foo` example shows: one flow for integer arguments and another for strings. Intersection types appear (in limited forms) combined with occurrence typing both in TypeScript and in Flow and serve to give, among other things, more precise types to functions such as `foo`. For instance, since `x + 1` evaluates to an integer and `x.trim()` to a string, then our function `foo` has type `(number|string)→(number|string)`. But it is clear that a more precise type would be one that states that `foo` returns a number when it is applied to a number and returns a string when it is applied to a string, so that the type deduced for, say, `foo(42)` would be `number` rather than the less precise `number|string`. This is exactly what the *intersection type*

$$\texttt{(number→number) \& (string→string)} \tag{2}$$

states (intuitively, an expression has an intersection of types, noted `&`, if and only if it has all the types of the intersection) and corresponds in Flow to declaring `foo` as follows:

```
var foo : (number => number) & (string => string) =  x => {
   return (typeof(x) === "number")? x+1 : x.trim();
}
```
(3)

For what concerns negation types, they are pervasive in the occurrence typing approach, even though they are used only at meta-theoretic level, in particular to determine the type environment when the type-case fails. We already saw negation types at work when we informally typed the "else" branch in `foo`, for which we assumed that x did *not* have type `number`—i.e., it had the (negation) type `¬number`—and deduced from it that x then had type `string`—i.e., `(number|string)&¬number` which is equivalent to the set-theoretic difference `(number|string)\number` and, thus, to `string`.

Since set-theoretic types play such a pivotal role in our treatment the system we study in this work is a conservative extension of the standard type assignment system for union and intersection types, which was defined by Barbanera et al. [1995, Definition 3.5]. To cope with occurrence typing we extend, in a nutshell, the system of [Barbanera et al. 1995] with three simple ingredients:

(1) we add to its expressions the type-case expression $(e \in t)\,?\,e_1 : e_2$;
(2) we add to its types the negation connective and the empty type;
(3) we add to its deduction rules the typing rules for type-cases we showed before.

The resulting system, presented in Section 2, is a type-assignment system for an untyped λ-calculus with constants, pairs, and type-cases.

We said earlier that the combination of the union rule and set-theoretic types gives us much more than what current formalizations of occurrence typing can capture. The approaches cited above essentially focus on refining the type of variables that occur in an expression whose type is being tested. They do it when the variable occurs at top-level in the test (i.e., the variable is the

expression being tested) or under some specific positions such as in nested pairs or at the end of a path of selectors. The union elimination rule of MacQueen et al. [1986] does not have such limitations: it can refine the type of *any* expression e' occurring in *any* position of the current expression e, by splitting the type of e' into a union of types that are tested separately for e. The separation of these tests combines with our new rules for type-cases to yield a system in which different branches of the same type-case are typed under different typing hypotheses, which is the essence of occurrence typing. In this work we aim at exploiting this power of the union rule and refine the type of any expression that occurs in a tested expression (or elsewhere). Of particular interest will be the expressions occurring in applications since the refinement of their types is pivotal in deducing and exploiting intersection types for functions. For example, let x_1 be a variable of type $(\mathsf{Int}\to\mathsf{Int}) \wedge (\mathsf{String}\to\mathsf{String})$ (e.g., x_1 binds the function `foo` defined in (3)) and x_2 be of type $\mathsf{Int} \vee \mathsf{String}$. If `@` denotes string concatenation, then we can use the three typing rules above to deduce that the following expression has type $\mathsf{Int} \vee \mathsf{String}$.

$$(x_1 x_2 \in \mathsf{Int})\,?\,(x_2 + 1) : ((x_1 x_2)\,@\,x_2) \tag{4}$$

This is done by splitting the type of x_2: if x_2 is of type Int, then $x_1 x_2$ is also of type Int, thus the first branch is selected and the addition in it is well typed with type Int; if x_2 is of type String, then $x_1 x_2$ is also of type String, thus the second branch is selected and the concatenation in it is well typed with type String. This is an example of typing that is out of reach for all the previously cited approaches. This is possible because our approach does not perform occurrence typing using only the information given by type-cases: it also uses all type information provided by applications, even more when functions are overloaded (i.e., typed by an intersection of arrows, as x_1 in (4)).

One of the most important consequences of such a thorough analysis is that we can use its results to infer intersection types for functions, even in the absence of precise annotations such as the one given in the definition of `foo` in (3): we split the type of the function parameter (initially supposed to be the top type `Any`) and deduce a distinct arrow for each split of the input type, discarding from the domain the split types for which the inference fails. To put it simply, we can infer the type (2) for the unannotated pure JavaScript code of `foo` (i.e., no type annotation at all), while in TypeScript and Flow (and any other formalism we are aware of) this requires an explicit and full type annotation as the one given in (3). This creates a virtuous circle since, as the program in (4) shows, determining intersection types for functions is crucial to refine the type of expressions in applications, which allows to deduce more precise types for functions and so forth. Thanks to this virtuous circle our system can type a whole class of functions that other systems fail to type (even when given explicit full type annotations) and must then hard-code to retain sufficient expressiveness. And for well-typed programs our approach needs, in general, fewer annotations. For instance, we can type all the 14 paradigmatic examples of Tobin-Hochstadt and Felleisen [2010] without any annotation, whereas they need to specify annotations for 5 of them (see Section 6).

Having three typing rules that allow us to type all the examples of occurrence typing (and even more) is still a far cry from a practical system that can decide whether a program of our source language (the untyped λ-calculus with constants, pairs, and type-cases) is well-typed or not. The culprit is, of course, the powerful union rule: to use this rule to type some expression e one has to guess a subexpression e' of e to single out, the occurrences of e' to be tested, and how to split the type of this e' in a union of types to be tested separately. This is no simple feat: according to Mariangiola Dezani, arguably the best expert in union and intersection type systems, determining an inversion (a.k.a., generation) lemma for this union rule is the most important open problem in this field of research [Dezani-Ciancaglini 2020]. And an inversion lemma is an important aid to define a type-inference algorithm, since it tells us when and how to apply the rule.

```
bind x1 = a1 in
bind x2 = a2 in
bind x3 = x1x2 in
bind x4 = x2 + 1 in
bind x5 = x3@x2 in
bind x6 = (x3∈Int) ? x4 : x5 in x6
```

Fig. 1. Pure MSC-form

```
bind x1 : {t1} = a1 in
bind x2 : {Int, String} = a2 in
bind x3 : {x2:Int▹Int, x2:String▹String} = x1x2 in
bind x4 : {Int} = x2 + 1 in
bind x5 : {String} = x3@x2 in
bind x6 : {t2} = (x3∈Int) ? x4 : x5 in x6
```

Fig. 2. Annotated MSC-form

In order to tackle this last problem of deciding whether an expression is well typed or not, we transform it into an equivalent problem in which the range of possible choices is much more restricted. To that end we introduce a canonical form for the expressions of our source language that we call *maximal-sharing canonical form* (MSC-form). A MSC-form is essentially a list of bindings from variables to *atoms*. An atom is either an expression of our source language in which all subexpressions are variables, or it is a λ-abstraction whose body is a MSC-form. We call these forms *maximal-sharing* forms because they must satisfy the property that there cannot be two distinct bindings for the same atom. This is a crucial property because it ensures that every expression of the source language (i) is equivalent to a unique (modulo some trivial syntactic conversions) MSC-form and (ii) is well-typed if and only if its MSC-form is. For instance, consider the expression in (4) where x_1 and x_2 rather than being variables are generic atoms of type $t_1 = (\mathsf{Int}\to\mathsf{Int}) \wedge (\mathsf{String}\to\mathsf{String})$ and $t_2 = \mathsf{Int} \vee \mathsf{String}$, that is $(a_1a_2 \in \mathsf{Int})?(a_2 + 1) : ((a_1a_2)\,@\,a_2)$. Its MSC-form will look like the term in Figure 1. Notice that this term satisfies the maximal sharing property because the two occurrences of the application a_1a_2 in the source language expression are bound by the same variable x_3. The other crucial property that we prove is that an MSC-form is well-typed if and only if it is possible to explicitly annotate all the bindings of variables so that the MSC-form type-checks. These annotations essentially define how the type of the variables must be split and the annotated MSC-form type-checks if the rest of the expression type-checks for each of the splits specified in its annotations. Figure 2 gives the annotations for the previous MSC-form. The important annotations are those of the variables x_2 and x_3. The first states that to type the expression, the type $\mathsf{Int}\vee\mathsf{String}$ of a_2 must be split and the expression must be checked separately for $x_2 : \mathsf{Int}$ and $x_2 : \mathsf{String}$. The annotation of x_3 states that when x_2 has type Int then x_3 must be assumed to be of type Int and when x_2 has type String so must have x_3 (see Section 4 for details).

Since we can effectively transform a source language expression into its MSC-form, then we have a method to check the well-typedness of an expression of the source language: transform it into its MSC-form and infer all the annotations of its variables, if possible. Inferring the annotations of a MSC-form boils down to deciding how to split the types of its atoms. This is done by an algorithm we present in Section 5 which starts from a MSC-form in which all variables are annotated with the top type Any and performs several passes to refine these annotations. Each pass has three possible outcomes: either (i) the MSC-form type-checks with its current annotations and the algorithm stops with a success, or (ii) the MSC-form does not type-check, the pass proposes a new version of the same MSC-form but with refined annotations, and a new pass is started, or (iii) the MSC-form does not check and it is not possible to further refine the annotations so that the form may become typable, then the algorithm stops with a failure. The algorithm refines the annotations differently for variables that are bound by lambdas and by binds. For the variables in binds the algorithms produces a set of disjoint types so that their union is the type of the atom in the bind; for lambdas the algorithm splits the type of the parameter into a set of disjoint types and rejects the types in this set for which the function does not type-check, thus determining the domain of the function. The very last point that remains to explain is how to determine the split of a type: as a matter of fact, in general there are infinitely many different ways to split a type. The split of the types is driven by the types tested in type-cases and the operations applied to their components. For instance, the

split of the type of a_2 for the variable x_2 in Figures 1 and 2 is determined by the test $x_3 \in \mathsf{Int}$: the algorithm will propose to split the type t_3 of x_3 into $t_3 \wedge \mathsf{Int}$ and $t_3 \wedge \neg\mathsf{Int}$. Since t_3 is $\mathsf{Int} \vee \mathsf{String}$, the split proposed for x_3 is actually Int or String. This split triggers in the subsequent pass the split for the type of x_2 since x_3 is defined as $x_1 x_2$ and x_3 can be of type Int only if x_2 is of type Int and it can be of type String only if x_2 is of type String. We just got the expected annotation.

Contributions. This work provides four main technical contributions. (*i*) We show how to extend the system of Barbanera et al. [1995] with negation types and type-cases and prove its soundness (§2); (*ii*) we define MSC-forms and prove that the problem of typing a term of the previous system is equivalent to the one of typing its MSC-form (§3); (*iii*) we prove that the latter problem is equivalent to adding type annotations in a MSC-form so that it becomes a well-typed term and that checking well-typedness of an annotated MSC-form is decidable (§4); (*iv*) we define a sound reconstruction algorithm for the annotations of a MSC-form (§5) and provide an implementation (§6).

More generally, this work provides a novel formal lens for viewing the conceptual core of occurrence typing, whose essence it reveals. It reframes occurrence typing in the more standard and general setting of classic union and intersection type systems and, in doing so, it removes several current limitations of existing approaches. The removal of these limitations makes it possible for our system not only to type several examples that are out of reach of existing approaches but also to deduce precise intersection types for completely unannotated functions, something that, in our ken, no other system is currently capable of. By the definition of MSC-forms, it circumscribes the use of union elimination to a very specific setting, thus advancing in the quest for the characterization of inversion of union rules. More importantly, it shows that well-typing in such systems is equivalent to the problem of reconstructing annotations for MSC-forms, thus providing a formal yard-stick to compare different approaches. We exploited this new setting to define a sound reconstruction algorithm that we rendered in a proof-of-concept implementation. This implementation demonstrates the potential practical implications of our work, even though the gap with mature implementations such as those of Flow, Typed Racket, or TypeScript is still huge. Last but not least, we obtained a system that is arguably more robust to extensions such as the addition of side-effects and of polymorphic types, as we are eager to verify in the near future.

For space reasons several definitions and rules, the extensions with records and let-constructs, and all the proofs are moved to the appendix, available on line as supplemental material.

2 SOURCE LANGUAGE AND DECLARATIVE TYPE SYSTEM

2.1 Types

Types are exactly those of the semantic subtyping framework by Frisch et al. [2002, 2008].

Definition 2.1 (Types). *The set of types* **Types** *is formed by the terms t coinductively produced by the grammar:*

$$\textbf{Types} \quad t \quad ::= \quad b \mid t \to t \mid t \times t \mid t \vee t \mid \neg t \mid \mathbb{0}$$

and that satisfy the following conditions

- *(regularity) every term has a finite number of different sub-terms;*
- *(contractivity) every infinite branch of a term contains an infinite number of occurrences of the arrow or product type constructors.*

We introduce the abbreviations $t_1 \wedge t_2 \stackrel{\text{def}}{=} \neg(\neg t_1 \vee \neg t_2)$, $t_1 \setminus t_2 \stackrel{\text{def}}{=} t_1 \wedge (\neg t_2)$, and $\mathbb{1} \stackrel{\text{def}}{=} \neg\mathbb{0}$. b ranges over basic types (e.g., Int, Bool), $\mathbb{0}$ and $\mathbb{1}$ respectively denote the empty (that types no value) and top (that types all values) types. Coinduction accounts for recursive types and the condition on infinite branches bars out ill-formed types such as $t = t \vee t$ (which does not carry any information about the set denoted by the type) or $t = \neg t$ (which cannot represent any set). Regularity is needed

for the decidability of the subtyping relation. We refer to b, $\times$, and $\to$ as *type constructors*, and to $\vee$, $\neg$, $\wedge$, and $\setminus$ as *type connectives*. As customary, connectives have priority over constructors and negation has the highest priority—e.g., $\neg s \vee t \to u \wedge v$ denotes $((\neg s) \vee t) \to (u \wedge v)$.

The subtyping relation for these types, noted $\leq$, is the one defined by Frisch et al. [2008] to which the reader may refer for the formal definition (we recall it in Appendix A.1 for the reader's convenience). A detailed description of the algorithm to decide this relation can be found in [Castagna 2020]. For this presentation it suffices to consider that types are interpreted as sets of *values* (i.e., either constants, λ-abstractions, or pairs of values: see Section 2.2 right below) that have that type, and that subtyping is set containment (i.e., a type s is a subtype of a type t if and only if t contains all the values of type s). In particular, $s \to t$ contains all λ-abstractions that when applied to a value of type s, if their computation terminates, then they return a result of type t (e.g., $\mathbb{0} \to \mathbb{1}$ is the set of all functions and $\mathbb{1} \to \mathbb{0}$ is the set of functions that diverge on every argument). Type connectives (i.e., union, intersection, negation) are interpreted as the corresponding set-theoretic operators (e.g., $s \vee t$ is the union of the values of the two types). We use $\simeq$ to denote the symmetric closure of $\leq$: thus $s \simeq t$ (read, s is equivalent to t) means that s and t denote the same set of values and, as such, they are semantically the same type.

2.2 Terms

The expressions of our *source language*, that is the language the programmer uses, are defined as:

$$\begin{array}{lcll} \textbf{Test Types} & \tau & ::= & b \mid \mathbb{0} \to \mathbb{1} \mid \tau \times \tau \mid \tau \vee \tau \mid \neg\tau \mid \mathbb{0} \\ \textbf{Expressions} & e & ::= & c \mid x \mid \lambda x.e \mid ee \mid (e,e) \mid \pi_i e \mid (e{\in}\tau)\,?\,e:e \\ \textbf{Values} & v & ::= & c \mid \lambda x.e \mid (v,v) \end{array} \tag{5}$$

Expressions are an untyped λ-calculus with constants c, pairs (e,e), pair projections $\pi_i e$, and type-cases. A typecase $(e_0{\in}\tau)\,?\,e_1 : e_2$ is a dynamic type test that first evaluates e_0 and, then, if e_0 reduces to a value v evaluates e_1 if v has type τ or e_2 otherwise. Type-cases cannot test arbitrary types but just types of the form τ where the only arrow type that can occur in them is $\mathbb{0} \to \mathbb{1}$, the type of all functions. This means that type-cases can distinguish functions from other values but they cannot distinguish, say, functions that have type $\mathsf{Int}\to\mathsf{Int}$ from those that do not. In previous work on semantic subtyping, there is no such restriction, but this is possible only because λ-abstractions are explicitly annotated with their types. If in the presence of non-annotated λ-abstractions we allowed tests on function types, then in a practical implementation the semantics would depend on the implementation of the type checking or type inference algorithms. Thanks to this restriction, instead, the semantics does not depend on the type system: it can be implemented without keeping track of compile-time types at runtime. Moreover, the interest of the typecase construct in this work is mostly to encode a pattern matching construct. Standard pattern matching cannot check function types, so the restriction is not a problem for this. Typecases of this form also have the same expressiveness as the type-testing primitives of dynamic languages like JavaScript and Racket.

Since every test type τ is also a type, then in what follows we may sometimes use the metavariable t to denote test types when this is clear from the context.

2.3 Reduction Semantics

The reduction semantics is the one of call-by-value pure λ-calculus with products and with a type-case expression. The reduction is given by the following notions of reductions

$$\begin{array}{rcl} (\lambda x.e)v & \rightsquigarrow & e\{v/x\} \\ \pi_1(v_1,v_2) & \rightsquigarrow & v_1 \\ \pi_2(v_1,v_2) & \rightsquigarrow & v_2 \end{array} \qquad \begin{array}{rcll} (v{\in}\tau)\,?\,e_1:e_2 & \rightsquigarrow & e_1 & \text{if } v \in \tau \\ (v{\in}\tau)\,?\,e_1:e_2 & \rightsquigarrow & e_2 & \text{if } v \in \neg\tau \end{array}$$

together with the context rules that implement a leftmost outermost reduction strategy.

The definition uses the standard substitution operation $e\{e'/x\}$ that denotes the capture avoiding substitution of e' for x in e, and the relation $v \in \tau$ that determines whether a value is of a given type or not and holds true if and only if $\mathsf{typeof}(v) \leq \tau$, where $\mathsf{typeof}(\lambda x.e) = \mathbb{0}\to\mathbb{1}$, $\mathsf{typeof}(c) = \boldsymbol{b}_c$, $\mathsf{typeof}((v_1, v_2)) = \mathsf{typeof}(v_1)\times\mathsf{typeof}(v_2)$, and $\boldsymbol{b}_c$ is the unique basic type of the constant c (e.g., $\boldsymbol{b}_{42} = \mathsf{Int}$). Note that $\mathsf{typeof}()$ maps every λ-abstraction to $\mathbb{0} \to \mathbb{1}$, so it does not depend on static types. This approximation is allowed by the restriction on arrow types in typecases.

The language we just defined is the same as the functional core of CDuce defined by Frisch et al. [2002, 2008] bar two important differences. The first difference is that λ-abstractions in [Frisch et al. 2002, 2008] are explicitly annotated with their types while here no annotation is needed. The absence of annotations not only relieves the programmer of an important burden but also, in the case of curried functions, makes it possible to type some expressions that could not be typed with the annotations used in CDuce (see Section 4). The price to pay for this choice is twofold: the burden of finding the annotations for λ-abstractions is passed on the type system and, as explained before, we no longer allow type-cases to test for arbitrary types. The second difference is that the type-case expressions in [Frisch et al. 2002, 2008] introduce a binding since they are of the form $(x{:=}e_\circ{\in}\tau)\ ?\ e_1 : e_2$, that is, the expression binds the result of the tested expression $e_\circ$ to the variable x so that it is possible to specialize the type of x differently for typing e_1 and e_2 and thus implement a limited form of occurrence typing (if $e_\circ : t$, then we assume $x : t \wedge \tau$ when typing e_1 and $x : t \wedge \neg\tau$ when typing e_2). Here we do not ask the programmer to write such a binding: in our system such a binding is deduced by the type system (and this deduction is not limited to type-case expressions). The deduction of this binding is the core of our approach and constitutes the key idea of our generalization of occurrence typing.

2.4 Type System

While the terms, types, and operational semantics of the language are essentially the same as the language by Frisch et al. [2002, 2008], the type inference system is completely different, in particular in what concerns the typing of the type-cases. *Per se* the typing system we detail below is far from being new: it is composed exactly by the rules of the classic system of union and intersection types defined by Barbanera et al. [1995] to which we add standard introduction and elimination rules for products ([×I], [×E$_1$], [×E$_2$]) and the three rules for the type-cases ([𝕆], [∈$_1$], [∈$_2$]). The typing rules are given in Figure 3 and use the following definition of type environments.

Definition 2.2 (Type environment). *Type environments, ranged over by* Γ *are finite sets of mappings from pairwise distinct variables to types. We denote by* $dom(\Gamma)$ *the set of variables mapped by* Γ*. We write* $\Gamma, x : t$ *for the type environment* $\Gamma \cup \{x \mapsto t\}$*, when* Γ *is a type environment such that* $x \notin dom(\Gamma)$*. We write* $\varnothing$ *for the type environment formed by an empty set of mappings.*

If we remove from Figure 3 the three rules for type-cases ([𝕆], [∈$_1$], [∈$_2$]) the resulting system is the same as the one in Definition 3.5 of Barbanera et al. [1995, Definition 3.5] (extended with standard rules for products and constants). The rules for abstractions and applications are those of the simply typed λ-calculus while those for pairs and projections extend it to products. Union and intersection types are handled by the rule [∧] that introduces intersections, the rule [∨] that eliminates unions, and the subsumption rule [≤] that introduces unions and eliminate intersections.

Notice that, by the definition of type-environments, it is not possible to type two nested λ-abstractions abstracting the same variable and that in the rule [∨] we have that $x \notin \mathrm{dom}(\Gamma)$. It is instead possible to have two distinct (not nested) λ-abstractions with the same abstracted variable, even though from a type-perspective point of view this is not relevant since, as it is

$$[\textsc{Const}]\ \frac{}{\Gamma \vdash c : \boldsymbol{b}_c} \qquad [\textsc{Ax}]\ \frac{}{\Gamma \vdash x : \Gamma(x)}\ x \in \mathrm{dom}(\Gamma)$$

$$[\to\mathrm{I}]\ \frac{\Gamma, x : t_1 \vdash e : t_2}{\Gamma \vdash \lambda x.e : t_1 \to t_2} \qquad [\to\mathrm{E}]\ \frac{\Gamma \vdash e_1 : t_1 \to t_2 \quad \Gamma \vdash e_2 : t_1}{\Gamma \vdash e_1 e_2 : t_2}$$

$$[\times\mathrm{I}]\ \frac{\Gamma \vdash e_1 : t_1 \qquad \Gamma \vdash e_2 : t_2}{\Gamma \vdash (e_1, e_2) : t_1 \times t_2} \qquad [\times\mathrm{E}_1]\ \frac{\Gamma \vdash e : t_1 \times t_2}{\Gamma \vdash \pi_1 e : t_1} \qquad [\times\mathrm{E}_2]\ \frac{\Gamma \vdash e : t_1 \times t_2}{\Gamma \vdash \pi_2 e : t_2}$$

$$[\wedge]\ \frac{\Gamma \vdash e : t_1 \quad \Gamma \vdash e : t_2}{\Gamma \vdash e : t_1 \wedge t_2} \qquad [\vee]\ \frac{\Gamma \vdash e' : t_1 \vee t_2 \quad \Gamma, x : t_1 \vdash e : t \quad \Gamma, x : t_2 \vdash e : t}{\Gamma \vdash e\{e'/x\} : t} \qquad [\leq]\ \frac{\Gamma \vdash e : t \quad t \leq t'}{\Gamma \vdash e : t'}$$

$$[\mathbb{0}]\ \frac{\Gamma \vdash e : \mathbb{0}}{\Gamma \vdash (e \in t)\,?\,e_1 : e_2 : \mathbb{0}} \qquad [\in_1]\ \frac{\Gamma \vdash e : t \qquad \Gamma \vdash e_1 : t_1}{\Gamma \vdash (e \in t)\,?\,e_1 : e_2 : t_1} \qquad [\in_2]\ \frac{\Gamma \vdash e : \neg t \qquad \Gamma \vdash e_2 : t_2}{\Gamma \vdash (e \in t)\,?\,e_1 : e_2 : t_2}$$

Fig. 3. Declarative type system

standard in such systems, the deduction is defined modulo α-conversion. In other terms, we suppose the existence of the implicit rule given below on the right (where $\equiv_\alpha$ denotes α-conversion). Working modulo α-conversion is crucial in systems with union types since rule [$\vee$] breaks the α-invariance property (see Hindley and Seldin [2008, Discussion 12.5]). For instance, the following judgement $y : \mathbb{1}\to\mathsf{Bool} \vdash (y(\lambda x.x), y(\lambda x.x)) : (\mathsf{True}\times\mathsf{True}) \vee (\mathsf{False}\times\mathsf{False})$ can be derived in the system above by using [$\vee$] together with the rules for application and pairs (where $\mathsf{Bool} = \mathsf{True}\vee\mathsf{False}$, with True being the singleton type containing the value true,[2] and likewise for False). However, to derive the same type for the α-equivalent term $(y(\lambda x.x), y(\lambda z.z))$ the rule [$\equiv_\alpha$] must be used. In what follows, we will use a variant of the system above where the rules [$\vee$] and [$\wedge$] are replaced by the following rules that produce more compact derivations and are closer to the syntax-directed system given in the next section:

$$[\equiv_\alpha]\ \frac{\Gamma \vdash e : t \qquad e \equiv_\alpha e'}{\Gamma \vdash e' : t}$$

$$[\wedge+]\ \frac{(\forall i \in I) \quad \Gamma \vdash e : t_i}{\Gamma \vdash e : \bigwedge_{i\in I} t_i}\ I \neq \varnothing \qquad [\vee+]\ \frac{\Gamma \vdash e' : \bigvee_{i\in I} t_i \qquad (\forall i \in I) \quad \Gamma, x : t_i \vdash e : t}{\Gamma \vdash e\{e'/x\} : t}\ I \neq \varnothing$$

Although the rules in our system are textually the same as those in [Barbanera et al. 1995, Definition 3.5] there is an important difference, namely, that our types are an extension of those of Barbanera et al. [1995] since they include recursive types, negation types, and the empty type. As a consequence our subsumption rule uses a type-theory that is more general than the one of Barbanera et al. [1995], the theory of semantic subtyping $\mathfrak{C}$ rather than the type theory $\mathfrak{I}$ of Barbanera et al. [1995] of which semantic subtyping is a conservative extension (cf. Dezani-Ciancaglini et al. [2003]). The subsumption rule handles directly the addition of recursive types; negation and empty types are explicitly handled by the rules to type type-case expressions that we comment next.

The combination of the union rule [$\vee$] with the three new rules [$\mathbb{0}$], [$\in_1$], [$\in_2$] is the key novelty of our type-system and, we claim, it captures the essence of occurrence typing. For one thing, thanks to this combination it is possible to type all the examples of [Tobin-Hochstadt and Felleisen 2010], all examples of [Castagna et al. 2021], and several more examples that are captured by neither of these systems. Of course, to paraphrase a famous quotation [see Wikipedia 2021], with great power comes great algorithmic complexity, and thus to determine when an expression is well typed is more challenging with [$\vee$] than in the cited systems. To see how this combination works it may

[2]Henceforth, for every constant of the language we suppose the existence of a singleton type containing that constant.

be useful to see how type-case expressions are typed in the system by Frisch et al. [2002, 2008]. These, we remind, require an explicit binding to perform occurrence typing, and are typed by the following rule:

$$\frac{\Gamma \vdash e' : s \qquad (s\wedge\tau \simeq \mathbb{0} \text{ or } \Gamma, x : s\wedge\tau \vdash e_1 : t) \qquad (s\wedge\neg\tau \simeq \mathbb{0} \text{ or } \Gamma, x : s\wedge\neg\tau \vdash e_2 : t)}{\Gamma \vdash (x{:=}e'{\in}\tau)\ ?\ e_1 : e_2\ :\ t}$$

In a nutshell, we know that e' can yield only a result in s and that this result will be bound to x; so we type e_1 only if e' can yield a result in τ (i.e., $s\wedge\tau \not\simeq \mathbb{0}$) and in that case we can assume that the obtained value (bound to x) is of type $s\wedge\tau$; likewise for e_2. We can type exactly the same type-case by using [$\vee$] combined with [$\mathbb{0}$], [$\in_1$], and/or [$\in_2$] and for that we do not need an explicit binding, since this is taken care of by [$\vee$]: our rules can directly type the expression in which we removed the binding, that is $e = (e'{\in}\tau)\ ?\ (e_1\{e'/x\}) : (e_2\{e'/x\})$, simply by noticing that this expression is equivalent to $((x{\in}\tau)\ ?\ e_1 : e_2)\{e'/x\}$, that $s \simeq (s\wedge\tau) \vee (s\wedge\neg\tau)$, and then applying [$\vee$]. For instance, when both $s\wedge\tau$ and $s\wedge\neg\tau$ are different from $\mathbb{0}$ we have:

$$[\vee]\ \frac{\Gamma \vdash e' : s \qquad \dfrac{[\leq]\ \dfrac{[\text{Ax}]\ \dfrac{}{\Gamma, x{:}s\wedge\tau \vdash x : s\wedge\tau}}{\Gamma, x{:}s\wedge\tau \vdash x : \tau} \qquad \Gamma, x{:}s\wedge\tau \vdash e_1 : t}{[\in_1]\ \Gamma, x : s\wedge\tau \vdash (x{\in}\tau)\ ?\ e_1 : e_2\ :\ t} \qquad \dfrac{[\leq]\ \dfrac{[\text{Ax}]\ \dfrac{}{\Gamma, x{:}s\wedge\neg\tau \vdash x : s\wedge\neg\tau}}{\Gamma, x{:}s\wedge\neg\tau \vdash x : \neg\tau} \qquad \Gamma, x{:}s\wedge\neg\tau \vdash e_2 : t}{[\in_2]\ \Gamma, x : s\wedge\neg\tau \vdash (x{\in}\tau)\ ?\ e_1 : e_2\ :\ t}}{\Gamma \vdash ((x{\in}\tau)\ ?\ e_1 : e_2)\{e'/x\}\ :\ t}$$

and if either $s\wedge\tau$ or $s\wedge\neg\tau$ is empty, then we replace the corresponding [$\in_i$] rule by [$\mathbb{0}$]. In summary, the combination of [$\vee$] with the three type-cases rule [$\mathbb{0}$], [$\in_1$], and [$\in_2$] encodes and simplifies the system by Frisch et al. [2002, 2008] moving the burden of the binding from the programmer to the type-system. But it also generalizes the approaches for occurrence typing defined by Tobin-Hochstadt and Felleisen [2010] and Castagna et al. [2021] since the binding in [$\vee$] is unconstrained, that is, it is not limited to the occurrences of an expression e' that appear in some particular positions (e.g., in the tests of type-cases [Castagna et al. 2021] or at the root of path expressions [Tobin-Hochstadt and Felleisen 2010]).

2.5 Type Soundness

It is well-known that subject-reduction (i.e., type preservation) does not hold in systems that, like ours, include the rule [$\vee$]. For instance, consider the expression $(f3, f3)$ where $f : \mathbb{1}{\to}\mathsf{Bool}$. Using the rule [$\vee$], it can be typed by $(\mathsf{True}\times\mathsf{True}) \vee (\mathsf{False}\times\mathsf{False})$. However, after a step of reduction, we might get for instance the expression $(\mathsf{true}, f3)$, which cannot be typed by $(\mathsf{True}\times\mathsf{True}) \vee (\mathsf{False}\times\mathsf{False})$ anymore (the smallest type we can deduce for it is $(\mathsf{True}\times\mathsf{Bool})$). Nevertheless, our type system is sound in the sense of Wright and Felleisen [1994]:

Theorem 2.3 (Type Soundness). *If $\varnothing \vdash e : t$, then either e diverges or $e \rightsquigarrow^* v$ with $\varnothing \vdash v : t$.*

For instance, with the earlier example, even if $(\mathsf{true}, f3)$ cannot be typed by $(\mathsf{True}\times\mathsf{True}) \vee (\mathsf{False}\times\mathsf{False})$, it will finally reduce to $(\mathsf{true}, \mathsf{true})$ which is of type $(\mathsf{True}\times\mathsf{True}) \vee (\mathsf{False}\times\mathsf{False})$.

In order to prove this theorem, we introduce an alternative semantics which performs parallel reductions and that satisfies both subject reduction and progress (a typable expression is either a value or can be reduced). These two properties yield soundness for the parallel semantics. Finally, we prove that the parallel semantics is equivalent to the semantics introduced in Section 2.3, in the sense that for any expression e, if e diverges with one semantics then it also diverges with the other, and if e reduces to a value v with one semantics then it also reduces to the value v with the other. From this we deduce the soundness of our system. All the details are given in the appendix.

3 INTERMEDIATE SYSTEM: SYNTAX-DIRECTED RULES AND CANONICAL FORMS

We have seen that the previous system is sound, that is, that every well-typed term can only diverge or yield a result of the same type. Now the problem is to decide whether a given term is well typed or not. For that the rules of Figure 3 are not very useful since they allow too many different possibilities to type a given term. As customary, there are essentially two problems:

(1) the rules are not *syntax directed*: given a term, to type it we can try to apply some elimination/introduction rule, but also to apply the intersection rule [∧], or the subsumption rule [≤], or the union rule [∨].
(2) some rules are *non-analytic*:[3] if we use the [→I] rule to type some λ-abstraction we do not know how to determine the type t_1 in the premise; if we use the [∨] rule we know neither how to determine e' nor how to determine the types t_1 and t_2 that split the type of e'.

Notice that [∨] cumulates both problems. We tackle each problem in the order.

In the rest of this section we deal with rules that are not syntax directed. These are the intersection rule [∧], the subsumption rule [≤], and the union rule [∨] insofar as the expression in their conclusion can have any form. We adopt different solutions for the rules [∧] and [≤] and for the rule [∨]. For [∧] and [≤] we simply eliminate them and embed the use of intersections and subtyping in the remaining rules. This essentially amounts to resorting to canonical derivations: we prove that it is possible to derive a type for a term if and only if there exists a derivation for that typing judgment in which intersection [∧] and subsumption [≤] rules are used only at determined specific places.[4] For the union rule [∨] we add to the language a *binding* expression whose typing rule will replace the current [∨] rule. Since the binding expressions will explicitly determine both the subterm e' and the variable x to be used in a [∨] instance, then the introduction of bindings also addresses part the non-analyticity of the union rule.

In Section 4 we tackle the non-analyticity problem, or what it remains of it, namely, how to determine the type(s) to assign to a function parameter in a [→I] instance and the split types t_1, t_2 in a [∨] instance. We solve this problem by adding explicit type annotations for the variables bound in bind-expressions and λ-abstractions: these annotations will provide the information that is missing when applying the [→I] and [∨] rules. The rest of this section proceeds as follows:

(1) In Section 3.1 we introduce an intermediate language obtained by adding bind-expressions to the source language of Section 2.2.
(2) In Section 3.2 we define a syntax-directed type system for this intermediate language (with a small caveat for the union rule). We prove that this system is sound and complete with respect to the source language type system, in the sense that every well-typed term of the intermediate language encodes a valid derivation in the source language (soundness) and that every term of the source language is well typed only if there exists a term of the intermediate language that encodes one of its type derivations (completeness).
(3) In Section 3.3 we show that soundness and completeness hold also for a strict sub-language of the intermediate language. We call the terms of this sub-language the *MSC-forms* (maximal sharing canonical forms). The advantage of this sub-language is that there is a one-to-one correspondence between MSC-forms and the expressions of the source language and such a correspondence is effective since it is easy to transform every source language expression into "its" MSC-form.

[3] We consider *non-analytic* (or *synthetic*) a rule in which the input (i.e., Γ and e) of the judgement at the conclusion is not sufficient to determine the inputs of the judgments at the premises (cf. [Martin-Löf 1994; Types 2019]).

[4] Intuitively, a deduction is canonical if (i) subsumption is only used on the premises of application, type-case, union, and projection rules and (ii) intersection is only used for expressions that are λ-abstractions, that is, all the premises of an intersection rule are the consequence of a [→I]. See the deduction system in Appendix A.3 and Lemmas D.5 and D.6.

In this way, we reduced the problem of typing a source language expression to the one of typing "its" MSC-form, for which a syntax-directed type system exists. In Section 4 we show this to be equivalent to searching for a way to annotate this MSC-form to make it typable. The search for these annotations is performed by the algorithm described in Section 5.

3.1 Expressions with Bindings

Formally, we consider the following grammar of *intermediate expressions* (or *expressions with bindings*) ranged over by the meta-variable $\boldsymbol{e}$ so as to distinguish them from expressions of the source language (*declarative expressions*) for which we continue to use the non-bold symbol e.

$$\textbf{Intermediate exprs} \quad \boldsymbol{e} \ ::= \ c \mid x \mid \lambda x.\boldsymbol{e} \mid \boldsymbol{e}\boldsymbol{e} \mid (\boldsymbol{e},\boldsymbol{e}) \mid \pi_i \boldsymbol{e} \mid (\boldsymbol{e} \in \tau)\,?\,\boldsymbol{e}:\boldsymbol{e} \mid \mathtt{bind}\, x = \boldsymbol{e}\, \mathtt{in}\, \boldsymbol{e} \tag{6}$$

Intermediate expressions extend the syntax of declarative expressions by adding a new construction $\mathtt{bind}\, x = \boldsymbol{e}\, \mathtt{in}\, \boldsymbol{e}$. Given an expression $\mathtt{bind}\, x = \boldsymbol{e}'\, \mathtt{in}\, \boldsymbol{e}$ we call $\boldsymbol{e}'$ the *argument* of the expression and $\boldsymbol{e}$ the *body* of the expression. Such an expression is used to bind a variable to a definition. A bind-expression is different from a let-expression $\mathtt{let}\, x = e'\, \mathtt{in}\, e$ (cf. Appendix C.1) as it is not associated with a call-by-value semantics: $\mathtt{bind}\, x = \boldsymbol{e}'\, \mathtt{in}\, \boldsymbol{e}$ is just a way to indicate that a specific instance of the [∨] rule must be used to type the expression, but it does not force the evaluation of the argument of the bind expression (call-by-need would be appropriate: cf. Appendix A.6).

3.2 Intermediate Typing Rules

We want to define a syntax-directed type-system for the expressions above. The addition of a binding expression makes [∨] syntax-directed, but we still have to eliminate the intersection [∧] and subsumption [≤] rules. In order to define the typing of applications and projections in the absence of subsumption we need some operators on types. Consider the rule [→E] for applications of source language expressions (Figure 3). It essentially does three things: (*i*) it checks that the expression in the function position has a functional type; (*ii*) it checks that the argument is in the domain of the function, and (*iii*) it returns the type of the application. In systems without set-theoretic types these operations are straightforward: (*i*) corresponds to checking that that expression in the function position has an arrow type, (*ii*) corresponds to checking that the argument is in the domain of the arrow deduced for the function, and (*iii*) corresponds to returning the codomain of that arrow. With set-theoretic types things get more complicated, since in general the type of a function is not always a single arrow, but it can be a union of intersections of arrow types and their negations. Checking that the expression in the function position has a functional type is easy since it corresponds to checking that it has a type subtype of $\mathbb{0}\to\mathbb{1}$. Determining its domain and the type of the application is more complicated and needs the operators $\mathsf{dom}()$ and $\circ$ defined as $\mathsf{dom}(t) \stackrel{\text{def}}{=} \max\{u \mid t \leq u \to \mathbb{1}\}$ and $t \circ s \stackrel{\text{def}}{=} \min\{u \mid t \leq s \to u\}$. In short, $\mathsf{dom}(t)$ is the largest domain of any single arrow that subsumes t while $t \circ s$ is the smallest codomain of an arrow type that subsumes t and has domain s. We need similar operators for projections since the type t of e in $\pi_i e$ may not be a single product type but, say, a union of products: all we know is that t must be a subtype of $\mathbb{1}\times\mathbb{1}$. So let t be a type such that $t \leq \mathbb{1}\times\mathbb{1}$, we define $\boldsymbol{\pi_1}(t) \stackrel{\text{def}}{=} \min\{u \mid t \leq u \times \mathbb{1}\}$ and $\boldsymbol{\pi_2}(t) \stackrel{\text{def}}{=} \min\{u \mid t \leq \mathbb{1}\times u\}$. All these type operators can be effectively computed (cf. Appendix A.4). We have now all the notions we need to define the syntax-directed type system for the intermediate language whose rules are given in Figure 4. The rules for constants, variables, and pairs are omitted since they are the same as in the deduction system for the declarative expressions. Contrary to the previous system, there no longer are explicit rules for intersection and subtyping: we want to have canonical derivations for which the deductions performed by these rules are distributed over the rest of the system. In particular, the only rule that introduces intersections is now the rule [→I-Int] for λ-abstractions. The type subsumption rule [≤] is no longer needed since the

$$[\to\text{I-Int}]\ \frac{(\forall j \in J) \qquad \Gamma, x : t_j \vdash_{\mathcal{I}} \boldsymbol{e} : s_j}{\Gamma \vdash_{\mathcal{I}} \lambda x.\boldsymbol{e} : \bigwedge_{j\in J} t_j \to s_j}\ J \neq \varnothing \qquad [\to\text{E-Int}]\ \frac{\Gamma \vdash_{\mathcal{I}} \boldsymbol{e}_1 : t_1 \quad \Gamma \vdash_{\mathcal{I}} \boldsymbol{e}_2 : t_2}{\Gamma \vdash_{\mathcal{I}} \boldsymbol{e}_1\boldsymbol{e}_2 : t_1 \circ t_2}\ \begin{array}{l} t_1 \leq \mathbb{0} \to \mathbb{1} \\ t_2 \leq \mathrm{dom}(t_1) \end{array}$$

$$[\times\text{E}_1\text{-Int}]\ \frac{\Gamma \vdash_{\mathcal{I}} \boldsymbol{e} : t \leq (\mathbb{1} \times \mathbb{1})}{\Gamma \vdash_{\mathcal{I}} \pi_1\boldsymbol{e} : \pi_1(t)} \quad [\times\text{E}_2\text{-Int}]\ \frac{\Gamma \vdash_{\mathcal{I}} \boldsymbol{e} : t \leq (\mathbb{1} \times \mathbb{1})}{\Gamma \vdash_{\mathcal{I}} \pi_2\boldsymbol{e} : \pi_2(t)} \qquad [\mathbb{0}\text{-Int}]\ \frac{\Gamma \vdash_{\mathcal{I}} \boldsymbol{e} : \mathbb{0}}{\Gamma \vdash_{\mathcal{I}} (\boldsymbol{e}\in t)\,?\,\boldsymbol{e}_1 : \boldsymbol{e}_2 : \mathbb{0}}$$

$$[\in_1\text{-Int}]\ \frac{\Gamma \vdash \boldsymbol{e} : t_0 \leq t \qquad \Gamma \vdash \boldsymbol{e}_1 : t_1}{\Gamma \vdash (\boldsymbol{e}\in t)\,?\,\boldsymbol{e}_1 : \boldsymbol{e}_2 : t_1}\ t_0 \not\simeq \mathbb{0} \quad [\in_2\text{-Int}]\ \frac{\Gamma \vdash_{\mathcal{I}} \boldsymbol{e} : t_0 \leq \neg t \qquad \Gamma \vdash \boldsymbol{e}_2 : t_2}{\Gamma \vdash_{\mathcal{I}} (\boldsymbol{e}\in t)\,?\,\boldsymbol{e}_1 : \boldsymbol{e}_2 : t_2}\ t_0 \not\simeq \mathbb{0}$$

$$[\vee_1\text{-Int}]\ \frac{\Gamma \vdash_{\mathcal{I}} \boldsymbol{e}_2 : s}{\Gamma \vdash_{\mathcal{I}} \mathtt{bind}\, x = \boldsymbol{e}_1\, \mathtt{in}\, \boldsymbol{e}_2 : s}\ x \notin \mathrm{dom}(\Gamma) \quad [\vee_2\text{-Int}]\ \frac{\Gamma \vdash_{\mathcal{I}} \boldsymbol{e}_1 : \bigvee_{j\in J} t_j \quad {\scriptstyle(\forall j\in J)}\ \Gamma, x{:}t_j \vdash_{\mathcal{I}} \boldsymbol{e}_2 : s_j}{\Gamma \vdash_{\mathcal{I}} \mathtt{bind}\, x = \boldsymbol{e}_1\, \mathtt{in}\, \boldsymbol{e}_2 : \bigvee_{j\in J} s_j}\ J \neq \varnothing$$

Fig. 4. Intermediate typing rules

checks for the subtyping relation are performed in the elimination rules and in the two $[\in_i]$ rules. The [→E-Int] rule works as we explained above: (*i*) it checks that the type t_1 of the expression in the function position is functional (i.e., $t_1 \leq \mathbb{0}\to\mathbb{1}$); (*ii*) it checks that the type t_2 of the argument is contained the domain of the function (i.e, $t_2 \leq \mathrm{dom}(t_1)$), and (*iii*) it returns the type $t_1 \circ t_2$ of the application. The product elimination rules check whether the argument of the projection is a product (i.e., $t \leq \mathbb{1}\times\mathbb{1}$) and apply the corresponding type operator on this type.

The three rules for type-case expressions are essentially as before, bar two minor modifications. First, in the $[\in_i$-Int] rules the checked expression must be explicitly subsumed to either t or $\neg t$ since there no longer is a [≤] rule in our system to do that. Second, since we want our type-system to be syntax-directed, then we add the side condition $t_0 \not\simeq \mathbb{0}$ in the $[\in_i]$ rules so as to avoid any overlap with the [𝟘] rule and thus giving priority to the latter.

Finally, the [∨] rule (actually, [∨+]) is encoded by a binding expression. We split the [∨+] in two rules. One, [$\vee_1$-Int], is for the case when the variable x in $\boldsymbol{e}_2$ is not reachable (either because it is not free in $\boldsymbol{e}_2$ or because it is in a type-case branch that cannot be selected such as in $(42\in\mathsf{Int})\,?\,3 : x$). The other, [$\vee_2$-Int], is the normal case for [∨+] where the bind-expression determines the variable x and the expression $\boldsymbol{e}_1$ to be substituted for it, but does not specify how to split the type of $\boldsymbol{e}_1$ into a union of types. Notice that in [$\vee_1$-Int] we added the side condition $x \notin \mathrm{dom}(\Gamma)$: this condition is not necessary in [$\vee_2$-Int] since (as in [∨] and [∨+]) the environment Γ is extended and, by Definition 2.2, the extension $\Gamma, x : t_j$ is defined only if $x \notin \mathrm{dom}(\Gamma)$.

The system is syntax-directed: the form of the expression determines the rules to apply and the rules for a same form do not overlap (for bindings, [$\vee_1$-Int] must be used only if $\boldsymbol{e}_1$ is not typable: we will be more precise in Section 4).

Soundness and completeness. A well-typed expression of the intermediate language is typed by derivations in which every instance of the [∨] rule corresponds to a bind-expression. Any such derivation is also a canonical derivation for a particular expression of the source language. This expression can be obtained from the intermediate language expression by unfolding its bindings. Formally, this is obtained by the *unwinding* operation, noted $\lceil . \rceil$ and defined for the binding expressions as $\lceil \mathtt{bind}\, x = \boldsymbol{e}_1\, \mathtt{in}\, \boldsymbol{e}_2 \rceil \stackrel{\text{def}}{=} \lceil \boldsymbol{e}_2 \rceil\{\lceil \boldsymbol{e}_1 \rceil / x\}$, as the identity for constants and variables, and homomorphically for all the other expressions (cf. Appendix A.5).

We can now prove that the problem of typing a declarative expression is equivalent to the problem of finding a typable intermediate expression whose unwinding is that declarative expression. In other terms, a declarative expression is typable if and only if we can enrich it with bindings so that it becomes a typable intermediate expression. This is formally stated by the theorems of soundness and completeness of the intermediate system:

Theorem 3.1 (Soundness). *If* $\Gamma \vdash_{\mathcal{I}} \boldsymbol{e} : t$ *then* $\Gamma \vdash \lceil \boldsymbol{e} \rceil : t$

Theorem 3.2 (Completeness). *If* $\Gamma \vdash e : t$ *then* $\exists \boldsymbol{e}', t'$ *such that* $\lceil \boldsymbol{e}' \rceil \equiv_\alpha e$, $t' \leq t$, *and* $\Gamma \vdash_{\mathcal{I}} \boldsymbol{e}' : t'$

3.3 Maximal Sharing Canonical Forms

The definition of the intermediate expressions is a step forward in solving the problem of typing a declarative expression, but it also brings a new problem, since we now have to decide where to add the bindings in a declarative expression so as to make it typable in the intermediate system. We get rid of this problem by defining the *maximal sharing canonical forms* (*MSC-form* for short). The idea is pretty simple, and consists in adding a new binding for every *distinct* (modulo α-conversion) sub-expressions of a declarative expression. Formally, this transformation yields a MSC-form:

Definition 3.3 (MSC Forms). *An intermediate expression $\boldsymbol{e}$ is a* maximal sharing canonical form *if it is produced by the following grammar:*

$$\begin{array}{lrcl} \textbf{\textit{Atomic expressions}} & \boldsymbol{a} & ::= & c \mid \lambda x.\boldsymbol{\kappa} \mid (x,x) \mid xx \mid (x{\in}\tau)\,?\,x:x \mid \pi_i x \\ \textbf{\textit{MSC-forms}} & \boldsymbol{\kappa} & ::= & x \mid \mathtt{bind}\, x = \boldsymbol{a}\, \mathtt{in}\, \boldsymbol{\kappa} \end{array} \tag{7}$$

and is α-equivalent to an expression $\boldsymbol{\kappa}$ that satisfies the following properties:
(1) if $\mathtt{bind}\, x_1 = \boldsymbol{a}_1\, \mathtt{in}\, \boldsymbol{\kappa}_1$ *and* $\mathtt{bind}\, x_2 = \boldsymbol{a}_2\, \mathtt{in}\, \boldsymbol{\kappa}_2$ *are distinct sub-expressions of $\boldsymbol{\kappa}$, then $\lceil \boldsymbol{a}_1 \rceil \not\equiv_\alpha \lceil \boldsymbol{a}_2 \rceil$;*
(2) if $\lambda x.\boldsymbol{\kappa}_1$ is a sub-expression of $\boldsymbol{\kappa}$ and $\mathtt{bind}\, y = \boldsymbol{a}\, \mathtt{in}\, \boldsymbol{\kappa}_2$ *a sub-expression of $\boldsymbol{\kappa}_1$, then $fv(\boldsymbol{a}) \not\subseteq fv(\lambda x.\boldsymbol{\kappa}_1)$;*
(3) if $\mathtt{bind}\, x = \boldsymbol{a}\, \mathtt{in}\, \boldsymbol{\kappa}'$ *is a sub-expression of $\boldsymbol{\kappa}$, then $x \in fv(\boldsymbol{\kappa}')$.*

MSC-forms, ranged over by $\boldsymbol{\kappa}$, are variables possibly preceded by a list of bindings of variables to atoms. Atoms are either λ-abstractions whose body is a MSC-form or any other expression in which all proper sub-expressions are variables. Therefore, bindings can appear in a MSC-form either at top-level or at the beginning of the body of a function. MSC-forms are defined modulo α-conversion.[5] Since MSC-forms are also intermediate expressions, then the typing rules and the definition of unwinding for intermediate terms of Section 3.2 apply to MSC-forms, too.

The syntactic form of MSC-forms guarantees that if a source language expression e is the unwinding of an MSC-form $\boldsymbol{\kappa}$, then every distinct sub-expression of e is bound by a variable in $\boldsymbol{\kappa}$, while the first property of Definition 3.3 guarantees that distinct variables bind distinct (i.e., non α-convertible) sub-expressions (i.e., this first property enforces the *maximal sharing* of common sub-expressions). The second property requires that bind-expressions must extrude λ-abstractions whenever possible. The third property guarantees that in a MSC-form there is no useless binding.

The first two properties of Definition 3.3 are important since they ensure that an expression of the source language is typable *if and only if* it is the unwinding of a typable MSC-form. For the first property, this is because reducing the bindings in an intermediate expression—while preserving unwinding—increases the typeability of a term: if we can type an intermediate term in which two distinct variables bind the same sub-expression, then the same term in which this sub-expression is bound by a single variable can also be typed by assigning to the unique variable the intersection of the types of the distinct variables, but the converse does not hold. For the second property this is because outer bindings may produce better types. For instance, consider the expression $\mathtt{bind}\, x = \boldsymbol{a}\, \mathtt{in}\, \lambda y.\, x$, where $\boldsymbol{a}$ is an expression that can be either an integer or a Boolean. This expression can be typed with $(\mathbb{1} \to \mathsf{Int}) \vee (\mathbb{1} \to \mathsf{Bool})$. However, for the expression $\lambda y.\ (\mathtt{bind}\, x = \boldsymbol{a}\, \mathtt{in}\, x)$ which has the same unwinding as the previous one, the most precise type one can deduce is $\mathbb{1} \to (\mathsf{Int} \vee \mathsf{Bool})$, which is strictly larger than $(\mathbb{1} \to \mathsf{Int}) \vee (\mathbb{1} \to \mathsf{Bool})$.

The last property of Definition 3.3 is important because it ensures that given a source language expression e there exists a unique (modulo α-conversion and the order of bindings) MSC-form whose unwinding is e (cf. Proposition 3.5): we denote this MSC-form by $\mathsf{MSC}(e)$.

Given a source language expression e it is easy to produce its unique MSC-form $\mathsf{MSC}(e)$. For space constraints we give the formal definition of the transformation and all details in the Appendixes A.7

[5] For instance, both $\lambda x.\mathtt{bind}\, z = xy\, \mathtt{in}\, zy$ and $\lambda x.\mathtt{bind}\, z = xy\, \mathtt{in}\, z$ are two distinct atoms that can occur in the same MSC-form, even though the atom xy appears in both: an α-renaming of x makes the first MSC-property hold.

and A.8, but in practice what the transformation needs to do is to visit e bottom up and generate a distinct binding for each distinct sub-expression, taking special care for free-variables, when extruding abstractions, and for α-convertible expressions (see Section 6 for more details).

We just got rid of the problem of determining where to put the bindings in a source language expression e: generate $\mathsf{MSC}(e)$ and try to type it in the syntax-directed system of Section 3.2.

Formally, we define the following congruence on MSC-forms:

Definition 3.4 (Canonical equivalence). *We denote by $\equiv_\kappa$ the smallest congruence on MSC-forms that is closed by α-conversion and such that*

$$\mathtt{bind}\, x_1 = \boldsymbol{a}_1 \,\mathtt{in}\, \mathtt{bind}\, x_2 = \boldsymbol{a}_2 \,\mathtt{in}\, \boldsymbol{\kappa} \quad \equiv_\kappa \quad \mathtt{bind}\, x_2 = \boldsymbol{a}_2 \,\mathtt{in}\, \mathtt{bind}\, x_1 = \boldsymbol{a}_1 \,\mathtt{in}\, \boldsymbol{\kappa} \qquad x_1 \notin fv(\boldsymbol{a}_2), x_2 \notin fv(\boldsymbol{a}_1)$$

Then we prove that all the MSC forms of a source language expression are equivalent:

Proposition 3.5. *If $\boldsymbol{\kappa}_1$ and $\boldsymbol{\kappa}_2$ are two MSC-forms and $\lceil \boldsymbol{\kappa}_1 \rceil \equiv_\alpha \lceil \boldsymbol{\kappa}_2 \rceil$, then $\boldsymbol{\kappa}_1 \equiv_\kappa \boldsymbol{\kappa}_2$.*

(Proof hint). Given two MSC-forms with the same unwinding, conditions (1) *and* (3) *of Definition 3.3 ensure that there is a one-to-one correspondence between their bindings, and condition* (2) *that each binding is located in the outermost possible λ. So the two MSC-forms differ by the relative order between independent bindings that are in the same λ-abstraction or at top-level and, thus, are equivalent.* □

It is easy to observe that the canonical equivalence preserves typeability (this is a direct consequence that type environments are mappings in which order does not matter). Thus, the corollary of this proposition is that an expression e is typable if and only if its unique (modulo $\equiv_\kappa$) MSC-form is typable, too. Formally, let $\mathsf{MSC}(e)$ be any element of the set $\{\boldsymbol{\kappa} \mid e \equiv_\alpha \lceil \boldsymbol{\kappa} \rceil\}$, then

Corollary 3.6 (Soundness and Completeness). *For every closed term e of the source language*

$$\vdash e : t \quad \Rightarrow \quad \vdash_{\mathcal{I}} \mathsf{MSC}(e) : t' \leq t \qquad \textit{(completeness)}$$
$$\vdash e : t \quad \Leftarrow \quad \vdash_{\mathcal{I}} \mathsf{MSC}(e) : t \qquad \textit{(soundness)}$$

Corollary 3.6 states that given a source language expression e it is typable if and only if $\mathsf{MSC}(e)$ is: we reduced the problem of typing e to the one of typing $\mathsf{MSC}(e)$, a form that we can effectively produce from e and for which we have a syntax-directed type system.

4 ALGORITHMIC SYSTEM: ADDING TYPE ANNOTATIONS

The intermediate type system of Figure 4 is not algorithmic since it still contains non-analytic rules: we neither know which decomposition in t_i's to use when applying the [$\vee_2$-Int] rule, nor which t_j's to choose when applying the [$\to$I-Int] rule. To solve this problem, we enrich our intermediate language with *annotations* that determine the types to use when typing a bind expression or a λ-abstraction. It is then straightforward to define an algorithmic system (i.e., a syntax-directed system composed only of analytic rules) for these enriched expressions and prove it to be sound and complete with respect to the system of the intermediate language.

Annotations. In a nutshell, we consider expressions of the form $\lambda x{:}A.\boldsymbol{e}$ and $\mathtt{bind}\, x{:}A = \boldsymbol{e} \,\mathtt{in}\, \boldsymbol{e}$, where A ranges over annotations of the form $\{\Gamma \triangleright t, \ldots, \Gamma \triangleright t\}$. Our annotations are, thus, finite relations between type environments and types. An annotation of the form $x : \{\Gamma_i \triangleright t_i\}_{i \in I}$ indicates that under the hypothesis Γ_i the variable x is assumed to be of type t_i.

We write $\{t_1, \ldots, t_n\}$ for $\{\varnothing \triangleright t_1, \ldots, \varnothing \triangleright t_n\}$ and just t for $\{\varnothing \triangleright t\}$. So for instance we write $\lambda x{:}t.\boldsymbol{e}$ for $\lambda x{:}\{\varnothing \triangleright t\}.\boldsymbol{e}$ while, say, $\mathtt{bind}\, x{:}\{t_1, \ldots, t_n\} = \boldsymbol{e}_1 \,\mathtt{in}\, \boldsymbol{e}_2$ stands for $\mathtt{bind}\, x{:}\{\varnothing \triangleright t_1, \ldots, \varnothing \triangleright t_n\} = \boldsymbol{e}_1 \,\mathtt{in}\, \boldsymbol{e}_2$.

In this system terms encode derivations. Terms with simple annotations such as $\lambda x{:}t.\boldsymbol{e}$ represent derivations as they can be found in the simply-typed λ-calculus: in other terms, to type the function the system must look for a type s such that $\lambda x{:}t.\boldsymbol{e}$ is of type $t \to s$.

When annotations are sets of types, such as in $\lambda x{:}\{t_1, \ldots, t_n\}.\boldsymbol{e}$, then the term represents a derivation for an intersection type, such as the derivations that can be found in semantic subtyping

calculi: in other terms, to type the function the system look for a set of types $\{s_1, \ldots, s_n\}$ such that $\lambda x{:}\{t_1, \ldots, t_n\}.\boldsymbol{e}$ has type $\bigwedge_{i=1}^{n} t_i \to s_i$.

Finally, the reason why we need the more complex annotations of the form $\{\Gamma_1 \triangleright t_1, \ldots, \Gamma_1 \triangleright t_1\}$ can be shown by an example. Consider $\lambda x.((\lambda y.(x, y))x)$: in the declarative system we can deduce for it the type $(\mathsf{Int}\to\mathsf{Int}\times\mathsf{Int}) \wedge (\mathsf{Bool}\to\mathsf{Bool}\times\mathsf{Bool})$. We must find the annotations A_1 and A_2 such that $\lambda x{:}A_1.((\lambda y{:}A_2.(x, y))x)$ has type $(\mathsf{Int}\to\mathsf{Int}\times\mathsf{Int}) \wedge (\mathsf{Bool}\to\mathsf{Bool}\times\mathsf{Bool})$. Clearly $A_1 = \{\mathsf{Int}, \mathsf{Bool}\}$. However, the typing of the parameter y depends on the typing of x: when $x{:}\mathsf{Int}$ then y must have type Int (the type of y must be larger than the one of x—the argument it will be bound to—, but also smaller than Int so as to deduce that $\lambda y.(x, y)$ returns a pair in $\mathsf{Int}\times\mathsf{Int}$). Likewise when $x{:}\mathsf{Bool}$, then y must be of type Bool, too. Therefore, we use as A_2 the annotation $\{x{:}\mathsf{Int}\triangleright\mathsf{Int}, x{:}\mathsf{Bool}\triangleright\mathsf{Bool}\}$, which precisely states that when $x{:}\mathsf{Int}$, then we must suppose that y (the variable annotated by A_2) is of type Int, and likewise for Bool. Using the typing rules we describe in the next section we are then able to deduce that $\lambda x{:}\{\mathsf{Int}, \mathsf{Bool}\}.(\lambda y{:}\{x{:}\mathsf{Int}\triangleright\mathsf{Int}, x{:}\mathsf{Bool}\triangleright\mathsf{Bool}\}.(x, y))x$ has type $(\mathsf{Int}\to\mathsf{Int}\times\mathsf{Int}) \wedge (\mathsf{Bool}\to\mathsf{Bool}\times\mathsf{Bool})$. Because of this last form of annotations, these annotations are strictly more expressive than those of the functional core of CDuce presented in [Frisch et al. 2008]: even if CDuce is a calculus with explicit full annotations, it is not possible to decorate $\lambda x.((\lambda y.(x, y))x)$ with a (CDuce) annotation so that the resulting term has type $(\mathsf{Int}\to\mathsf{Int}\times\mathsf{Int}) \wedge (\mathsf{Bool}\to\mathsf{Bool}\times\mathsf{Bool})$: CDuce annotations are exactly as expressive as our $\{\varnothing\triangleright t_1, \ldots, \varnothing\triangleright t_n\}$ annotations.

In the preceding paragraphs we explained how our annotations work by using as examples expressions of the intermediate language. However, recall that our ultimate goal is to type the expressions of the *source language* we introduced in Section 2.2 and, as we saw in the previous section, for that one does not need to consider the whole intermediate language: the MSC-forms suffice. This is why in the rest of this section we add annotations *only to MSC-forms*: the definitions and results of this section can be easily extended to all expressions of the intermediate language.

4.1 Algorithmic Expressions and Typing Rules

Formally, we consider the following grammar of *explicitly annotated MSC-forms* (or *algorithmic expressions*)—i.e., MSC-forms as per Definition 3.3 enriched with annotations—ranged over by the meta-variable κ (to distinguish them from the unannotated MSC-forms ranged over by $\boldsymbol{\kappa}$).

$$\begin{array}{lrcl} \textbf{Annotations} & A & ::= & \{\Gamma\triangleright t, \ldots, \Gamma\triangleright t\} \\ \textbf{Algorithmic Atoms} & a & ::= & c \mid \lambda x{:}A.\kappa \mid (x, x) \mid xx \mid (x{\in}\tau)\,?\,x : x \mid \pi_i x \\ \textbf{Algorithmic Expressions} & \kappa & ::= & x \mid \mathtt{bind}\, x{:}A = a\, \mathtt{in}\, \kappa \end{array} \tag{8}$$

These enrich the syntax of MSC-forms by inserting an annotation wherever a variable is introduced by a binder (either a "λ" or a "bind"). We use φ to range over either atoms a or expressions κ.

For the algorithmic typing rules we need to define the following pre-order on type environments:

Definition 4.1 (Envinronment subsumption). *Given two type environments* Γ *and* Γ'*, we say that* Γ' subsumes Γ*, written,* $\Gamma \le \Gamma'$ *if and only if* $\forall x \in dom(\Gamma')$ *we have* $\Gamma(x) \le \Gamma'(x)$.

The algorithmic type system is then given by the rules for abstractions and binding in Figure 5 plus all the other rules of the intermediate type system (specialized for MSC-forms, i.e., where every subexpression is a variable: cf. Figure 4 and Appendix A.9). The introduction of intersections is driven by the annotation $\{\Gamma_i\triangleright t_i\}_{i\in I}$ of the λ-abstraction: for every t_j whose hypotheses Γ_j subsume the current environment Γ, the system checks whether the function has type $t_j \to s_j$, that is, under the hypothesis that $x : t_j$ it tries to infer a type s_j for the body κ of the function; the condition $J \neq \varnothing$ ensures that at least one Γ_i subsumes Γ. Bind expressions are still handled by the two rules [$\vee_1$-Int] and [$\vee_2$-Int]. The first one, [$\vee_1$-Int], is for the case when the variable x is not reachable in κ. It is used when the current environment Γ is not subsumed by any of the environments in

$$[\to\text{I-Alg}]\ \frac{(\forall j \in J) \qquad \Gamma, x : t_j \vdash_{\mathcal{A}} \kappa : s_j}{\Gamma \vdash_{\mathcal{A}} \lambda x{:}\{\Gamma_i \triangleright t_i\}_{i\in I}.\kappa : \bigwedge_{j\in J} t_j \to s_j}\ J = \{i \in I \mid \Gamma \le \Gamma_i\} \neq \varnothing$$

$$[\vee_1\text{-Alg}]\ \frac{\Gamma \vdash_{\mathcal{A}} \kappa : s}{\Gamma \vdash_{\mathcal{A}} \mathtt{bind}\, x{:}\{\Gamma_i \triangleright t_i\}_{i\in I} = a\ \mathtt{in}\ \kappa\ : s}\quad \begin{array}{c} x \notin \mathrm{dom}(\Gamma) \\ \{i \in I \mid \Gamma \le \Gamma_i\} = \varnothing \end{array}$$

$$[\vee_2\text{-Alg}]\ \frac{\Gamma \vdash_{\mathcal{A}} a : \bigvee_{j\in J} t_j \qquad (\forall j \in J) \qquad \Gamma, x : t_j \vdash_{\mathcal{A}} \kappa : s_j}{\Gamma \vdash_{\mathcal{A}} \mathtt{bind}\, x{:}\{\Gamma_i \triangleright t_i\}_{i\in I} = a\ \mathtt{in}\ \kappa\ : \bigvee_{j\in J} s_j}\ J = \{i \in I \mid \Gamma \le \Gamma_i\} \neq \varnothing$$

Fig. 5. Algorithmic typing rules

the annotation of x. The other, [$\vee_2$-Alg], is the normal case for [$\vee$+] where the bind-expression determines both the variable x and the atom a to be substituted for it, and where its annotation determines how to split the type of a into a union of types.

The first important property satisfied by the algorithmic type system is that it is syntax directed and composed only by analytic rules (a simple visual check of the rules in Appendix A.9 suffices to verify it). As such it describes a deterministic algorithm to infer the type of an algorithmic expression. Furthermore, it is also decidable (this can be proved by a simple induction on the structure of the term, by observing that the subtyping relation is decidable, and that the operators used in the rules can be effectively computed: cf. Frisch et al. [2008, Section 6] and Appendix A.4).

The main interest of the algorithmic system is that a well-typed algorithmic term univocally encodes a type derivation for a MSC-form and, in virtue of Corollary 3.6, it also encodes a particular canonical derivation for a source language expression. The source language expression at issue is the one obtained by erasing the annotations from our algorithmic term and then applying the unwinding operation defined in Section 3.2. The annotation erasing operation, noted $\langle . \rangle$, is defined as $\langle \mathtt{bind}\, x{:}A = a\ \mathtt{in}\ \kappa \rangle \stackrel{\text{def}}{=} \mathtt{bind}\, x = \langle a \rangle\ \mathtt{in}\ \langle \kappa \rangle$, $\langle \lambda x{:}A.\kappa \rangle \stackrel{\text{def}}{=} \lambda x.\langle \kappa \rangle$, and as the identity otherwise. We can now prove that the problem of typing an MSC-form is equivalent to the problem of decorating it with some annotations that make it typable with the algorithmic type system. This is formally stated by the theorems of soundness and completeness of the system for algorithmic expressions (ranged over by κ) *with respect to the unannotated MSC-forms* (ranged over by $\boldsymbol{\kappa}$):

Theorem 4.2 (Soundness). *If* $\Gamma \vdash_{\mathcal{A}} \kappa : t$ *then* $\Gamma \vdash_{\mathcal{I}} \langle \kappa \rangle : t$

Theorem 4.3 (Completeness). *If* $\Gamma \vdash_{\mathcal{I}} \boldsymbol{\kappa} : t$, *then* $\exists \kappa$ *such that* $\langle \kappa \rangle = \boldsymbol{\kappa}$ *and* $\Gamma \vdash_{\mathcal{A}} \kappa : t' \le t$

Soundness states that if an algorithmic expression is well-typed, then removing its annotations gives a well-typed MSC-form. Completeness states that every well-typed MSC-form can be decorated with annotations so that it becomes a well-typed algorithmic expression.

By combining these theorems with the previous results on the intermediate language, we obtain the soundness and completeness of the algorithmic system *with respect to the source language.*

Corollary 4.4 (Algorithmic soundness and completeness).

$$\vdash_{\mathcal{A}} \kappa : t \quad \Rightarrow \quad \vdash \lceil \langle \kappa \rangle \rceil : t \qquad \textit{(soundness)}$$

$$\vdash e : t \quad \Rightarrow \quad \exists \kappa\ .\ \vdash_{\mathcal{A}} \kappa : t' \le t \text{ and } \lceil \langle \kappa \rangle \rceil \equiv_\alpha e \qquad \textit{(completeness)}$$

Notice that in the statement of completeness $\lceil \langle \kappa \rangle \rceil \equiv_\alpha e$ is equivalent to writing $\langle \kappa \rangle = \mathsf{MSC}(e)$. Combining this with the soundness result yields that for every closed declarative expression e, if $\vdash_{\mathcal{A}} \kappa : t$ and $\langle \kappa \rangle = \mathsf{MSC}(e)$, then $\vdash e : t$. All this gives us a procedure to check whether an expression e of the source language is well typed or not: produce $\mathsf{MSC}(e)$ and look for a way to annotate it so that it becomes a well-typed algorithmic expression κ. If we find such annotations, then the soundness property tells us that e is well typed. If such annotations do not exist, then the completeness property tells us that e is not well-typed.

In the next section we describe a sound algorithm to search for such annotations.

5 ALGORITHM FOR RECONSTRUCTING ANNOTATIONS

We define an algorithm to reconstruct annotations for an MSC-form to make it become a well-typed algorithmic expression. It starts by annotating all the bindings of the MSC-form by $\mathbb{1}$ (the weakest possible annotation) and performs several passes to refine these annotations until it either obtains a well-typed algorithmic expression or it fails.

At each pass the algorithm takes as input a type environment Γ, an algorithmic expression κ, and a type t and checks whether κ can be given the type t under the hypothesis Γ. The check yields one of three possible results: either (i) success with an expression κ' obtained from κ by refining some annotations—meaning that it is possible to deduce from Γ the type t for κ'—, or (ii) a failure—meaning that the algorithm cannot propose any better refinement of the annotations to type the expression—, or (iii) a refined expression κ' and a set of type environments that refine Γ—meaning that it is not yet possible to deduce t for κ' under Γ and that the algorithm must try further passes using the new type environments returned by this pass.

Formally, passes are defined by a deduction system whose judgments are of the form $\Gamma \vdash_{\mathcal{R}} \varphi : t \Rightarrow (\varphi', \mathbb{\Gamma})$, where $\mathbb{\Gamma}$ denotes a possibly empty set of type environments, t is a type, and φ, φ' are either algorithmic atoms or algorithmic expressions as defined in (8). Γ, φ, and t form the input of the pass while φ' and $\mathbb{\Gamma}$ are the output and they refine φ and Γ, respectively. The reason why the output is a pair is because we want to refine the type of *all* the variables in the input expression φ: the types of the variables that are free in φ are refined by providing new environments that refine the input environment Γ, yielding $\mathbb{\Gamma}$; the types of the variables that are bound in φ are refined by refining their annotations in φ, yielding φ'.

Given a judgment $\Gamma \vdash_{\mathcal{R}} \varphi : t \Rightarrow (\varphi', \mathbb{\Gamma})$, an empty $\mathbb{\Gamma}$ means failure while if $\mathbb{\Gamma}$ is the singleton $\{\Gamma\}$, this means success. For instance, the rules for constants in the deduction system are:

$$[\textsc{Const}]\ \frac{\boldsymbol{b}_c \leq t}{\Gamma \vdash_{\mathcal{R}} c : t \Rightarrow (c, \{\Gamma\})} \qquad [\textsc{ConstUntypable}]\ \frac{\boldsymbol{b}_c \not\leq t}{\Gamma \vdash_{\mathcal{R}} c : t \Rightarrow (c, \{\})}$$

The system succeeds in checking that a constant c has a supertype of $\boldsymbol{b}_c$ and fails otherwise. Notice that the atom in the result is the same as in the input, since in a constant there is no annotation to refine (this is true for all the rules for atoms excluding λ-abstractions).

If a pass neither fails nor succeeds, then it proposes a refinement of the types of the variables in the expression, refinement that is to submit to a further pass. This corresponds to a judgment $\Gamma \vdash_{\mathcal{R}} \varphi : t \Rightarrow (\varphi', \{\Gamma_1, ..., \Gamma_n\})$: for the variables that are bound in φ it proposes a refinement by refining the annotations in φ yielding the new expression φ'; for the variables that are free in φ, it proposes a refinement of the environment Γ by proposing the refinements $\Gamma_1 \dots \Gamma_n$. The type of a variable is refined in two ways: either it can be restricted to match the usage of the variable or it can be split when it is the union of simpler types (to determine a unique split of unions, the rules use the disjunctive normal forms of [Frisch et al. 2008]: cf. Appendix B.1). For instance, if we try to type the atom $\pi_1 x$ and the current annotation/environment for x is a type t that does not contain only pairs, then the algorithm proposes to refine the type of x into $t \wedge (\mathbb{1}\times\mathbb{1})$; if the type t is a union of products such as $(s_1\times s_2) \vee (t_1\times t_2)$, then the algorithm suggests to split the type of x into two separate types $(s_1\times s_2)$ and $(t_1\times t_2)$. Both these refinements are done by the rules for projections:

$$[\textsc{Proj}_1]\ \frac{\Gamma(x) \wedge (t \times \mathbb{1}) \simeq \bigvee_{i\in I} t_i \times s_i}{\Gamma \vdash_{\mathcal{R}} \pi_1 x : t \Rightarrow (\pi_1 x, \{\Gamma[x :\hat{=} t_i\times s_i]\}_{i\in I})} \qquad [\textsc{Proj}_2]\ \frac{\Gamma(x) \wedge (\mathbb{1} \times t) \simeq \bigvee_{i\in I} t_i \times s_i}{\Gamma \vdash_{\mathcal{R}} \pi_2 x : t \Rightarrow (\pi_2 x, \{\Gamma[x :\hat{=} t_i\times s_i]\}_{i\in I})}$$

where $\Gamma[x :\hat{=} t]$ is the environment obtained by *refining* the binding of x in Γ by intersecting it with t, that is, $\Gamma[x :\hat{=} t] \stackrel{\text{def}}{=} (\Gamma \setminus \{x \mapsto \Gamma(x)\}) \cup \{x \mapsto \Gamma(x) \wedge t\}$ for $x \in \text{dom}(\Gamma)$. The rules force the projections to have the checked type t by intersecting the type of x with $(t\times\mathbb{1})$ or $(\mathbb{1}\times t)$, and split

the resulting type into the different summands by proposing different refinements of the current environment Γ. Again, the returned atom is the same as in the input, since there are no annotations to refine in it. The inference for occurrence typing is performed by the rule for type-cases:

$$[\textsc{Case}]\ \frac{}{\Gamma \vdash_{\mathcal{R}} (x{\in}s)\,?\,x_1 : x_2 : t \Rightarrow ((x{\in}s)\,?\,x_1 : x_2, \{\Gamma[x :\hat{=} s][x_1 :\hat{=} t], \Gamma[x :\hat{=} \neg s][x_2 :\hat{=} t]\})}$$

In order to analyze the test that x has type s, the rule [Case] splits the current type of x by intersecting it with s and $\neg s$, a split that it proposes in the two refinements $\Gamma[x :\hat{=} s]$ and $\Gamma[x :\hat{=} \neg s]$ given in the result of the conclusion. The first refinement corresponds to the selection of the "then" branch, that is of x_1. Since the rule requires the whole expression to be of type t, then the first type environment also refines the type of x_1 with t. Likewise for the second environment and x_2. An important though pretty hidden detail is that the notation for the refinement of type environments handles the cases in which two or more variables coincide: for instance if $x = x_1$, then the rule [Case] will refine $\Gamma(x)$ in the first refinement by intersecting it both with s and with t. In all the rules presented in this section we suppose that the intersections occurring in them are not empty: the cases for empty types are handled by other rules, omitted here (see Appendix B.3).

The reason why we may split the type of a variable x when its type is a union or when we test it dynamically can be understood by considering the typing rule [$\vee_2$-Alg] in Figure 5: we are trying to reconstruct the annotation for x in the conclusion of [$\vee_2$-Alg] and thus determine the environments compatible with the current one that should be used in this annotation. However, [$\vee_2$-Alg] is not the only rule that splits the derivation in sub-derivations with different environments: also [$\to$I-Alg] does it, with the difference that it does not split a union or a tested case, but it splits an intersection of arrows. We encounter this split of intersections in the rules for applications, in particular in [AppR]. These rules are defined as follows (we present a simplified version):

$$[\textsc{AppR}]\ \frac{\Gamma(x_1) \simeq \bigwedge_{i\in I}(s_i \to t_i)}{\Gamma \vdash_{\mathcal{R}} x_1x_2 : t \Rightarrow (x_1x_2, \{\Gamma[x_1 :\hat{=} ((s_i \wedge \Gamma(x_2)) \to t)][x_2 :\hat{=} s_i]\}_{i\in I})}$$

$$[\textsc{AppL}]\ \frac{\Gamma(x_1) \wedge (\mathbb{0} \to \mathbb{1}) \simeq \bigvee_{i\in I} s_i}{\Gamma \vdash_{\mathcal{R}} x_1x_2 : t \Rightarrow (x_1x_2, \{\Gamma[x_1 :\hat{=} s_i]\}_{i\in I})}$$

The type of a functional expression is in general a union of intersections of arrows (cf. Frisch et al. [2008]). When it is a union then, as for any other algorithmic atom, the system splits this union into distinct type environments, here in the rule [AppL]. Then each summand (which is an intersection of arrows) is separately checked by the rule [AppR] which deserves a detailed explanation. The hypothesis about x_1 is that it is bound to a function whose type is an intersection of arrows. For each arrow $s_i \to t_i$ in this intersection, the rule proposes a refined environment Γ_i in which both the type of x_1 and the type of x_2 are refined: the first by intersecting it with $(s_i \wedge \Gamma(x_2)) \to t$, to ensure that the application uses the right domain and will yield a result not only in t_i (since $\Gamma(x_1) \leq s_i \to t_i$), but also in t (and, thus, in $t_i \wedge t$); the second by intersecting it with s_i since the argument must be in the domain of x_1. The intuition is that these different Γ_i correspond to the different typing checks performed by the rule [$\to$I-Alg] to type the body of the function bound to x_1. It is important to stress that, as in previous cases, an environment Γ_i is added to the result only if $\Gamma(x_2) \wedge s_i$ is not empty since we want to discard from the type of x_1 the arrows whose domain is not compatible with the current typing of the argument. Likewise, if the intersection in [AppL] is empty, then this produces an empty set of refinements, meaning failure since we are applying to some argument an expression that is not a function.

All the rules we have seen so far are actually axioms (we only considered atoms in which the only subexpressions are variables) in which the returned expression is the same as in the input (there are no annotations to refine). The bulk of the inference work is done in the rules for binding expressions

$$[\textsc{BindArgSkip}]\ \frac{(\Gamma \triangleright A) = \{\} \qquad \Gamma \vdash_{\mathcal{R}} \kappa : t \Rightarrow (\kappa', \mathbb{\Gamma})}{\Gamma \vdash_{\mathcal{R}} \mathtt{bind}\, x{:}A = a\, \mathtt{in}\, \kappa\ : t \Rightarrow (\mathtt{bind}\, x{:}\{\} = a\, \mathtt{in}\, \kappa', \mathbb{\Gamma})}$$

$$[\textsc{BindArgUntyp}]\ \frac{\Gamma \vdash_{\mathcal{R}} a : \bigvee(\Gamma \triangleright A) \Rightarrow (a', \{\}) \qquad \Gamma \vdash_{\mathcal{R}} \kappa : t \Rightarrow (\kappa', \mathbb{\Gamma})}{\Gamma \vdash_{\mathcal{R}} \mathtt{bind}\, x{:}A = a\, \mathtt{in}\, \kappa\ : t \Rightarrow (\mathtt{bind}\, x{:}\{\} = a'\, \mathtt{in}\, \kappa', \mathbb{\Gamma})}$$

$$[\textsc{BindArgRefEnv}]\ \frac{\Gamma \vdash_{\mathcal{R}} a : \bigvee(\Gamma \triangleright A) \Rightarrow (a', \mathbb{\Gamma})}{\Gamma \vdash_{\mathcal{R}} \mathtt{bind}\, x{:}A = a\, \mathtt{in}\, \kappa\ : t \Rightarrow (\mathtt{bind}\, x{:}A = a'\, \mathtt{in}\, \kappa, \mathbb{\Gamma} \cup \{\Gamma\})}\ (\mathbb{\Gamma} \neq \{\Gamma\})$$

$$[\textsc{BindArgRefAnns}]\ \frac{\Gamma \vdash_{\mathcal{R}} a : \bigvee(\Gamma \triangleright A) \Rightarrow (a', \{\Gamma\}) \quad \Gamma \vdash_{\mathcal{R}} \mathtt{bind}\, x{:}A = a'\, \mathtt{in}\, \kappa\ : t \Rightarrow (\kappa', \mathbb{\Gamma})}{\Gamma \vdash_{\mathcal{R}} \mathtt{bind}\, x{:}A = a\, \mathtt{in}\, \kappa\ : t \Rightarrow (\kappa', \mathbb{\Gamma})}\ (a' \neq a)$$

$$[\textsc{Bind}]\ \frac{\begin{array}{c}\Gamma \vdash_{\mathcal{R}} a : \bigvee(\Gamma \triangleright A) \Rightarrow (a, \{\Gamma\}) \qquad \Gamma \vdash_{\mathcal{A}} a : s \qquad \{s_i\}_{i \in I} = \mathtt{partition}(\{s \wedge u \mid u \in (\Gamma \triangleright A)\}) \\ (\forall i \in I)\ \ \Gamma, (x : s_i) \vdash_{\mathcal{R}} \kappa : t \Rightarrow (\kappa_i, \mathbb{\Gamma}_i) \quad \mathbb{\Gamma}'_i = \mathtt{propagate}_{x,a,s_i}(\mathbb{\Gamma}_i) \quad (A_i, \mathbb{\Gamma}''_i) = \mathtt{extract}_x(\mathbb{\Gamma}'_i)\end{array}}{\Gamma \vdash_{\mathcal{R}} \mathtt{bind}\, x{:}A = a\, \mathtt{in}\, \kappa\ : t \Rightarrow (\mathtt{bind}\, x{:}\bigcup_{i \in I} A_i = a'\, \mathtt{in}\, \mathtt{merge}(\{\kappa_i\}_{i \in I}), \bigcup_{i \in I} \mathbb{\Gamma}''_i)}$$

Fig. 6. Reconstruction rules for bind-expressions

(and in those for λ-abstractions that are conceptually similar to those for bindings). The complete set of rules for bind-expressions are presented in Figure 6 in their priority order: a rule can be applied only if the previous rules cannot (we just did two slight simplifications in the first and third rule: cf. Appendix B.3). These rules use some auxiliary definitions. We note by $(\Gamma \triangleright A)$ the set of the types of the annotation A that are compatible with Γ, that is, $(\Gamma \triangleright A) \stackrel{\text{def}}{=} \{t \mid \Gamma' \triangleright t \in A \text{ and } \Gamma \leq \Gamma'\}$, and by $\bigvee(\Gamma \triangleright A)$ the union of these types, that is, $\bigvee(\Gamma \triangleright A) \stackrel{\text{def}}{=} \bigvee_{t \in (\Gamma \triangleright A)} t$.

To check that the bind-expression $\mathtt{bind}\, x{:}A = a\, \mathtt{in}\, \kappa$ has type t under the hypotheses Γ, the system first focuses on the argument a of the bind-expression using the first four rules in Figure 6. If no type in A is compatible with the current environment Γ (i.e., $(\Gamma \triangleright A)$ is empty), then the bind is skipped and the system tries to type the body κ of the expression without using x: no type assumption for x is added to Γ and the annotation is emptied (rule [BindArgSkip]). If instead $(\Gamma \triangleright A)$ is not empty, then the argument a must have a type smaller than the union of all types in $(\Gamma \triangleright A)$. Thus the system tries to check under the current hypothesis Γ whether a can be given the type $\bigvee(\Gamma \triangleright A)$. The result of this check is a pair $(a', \mathbb{\Gamma})$ according to which we can distinguish four different outcomes, corresponding to the last four rules. (1) the check failed, that is, it returned an empty $\mathbb{\Gamma}$ (rule [BindArgUntyp]): then this binding must be skipped and we proceed as for rule [BindArgSkip]. (2) the check did not succeed but it proposed a set of refinements for Γ (and, possibly, for a), that is, $\mathbb{\Gamma} \neq \{\Gamma\}$ ([BindArgRefEnv]): then before attacking the body κ of the bind expression, the system proposes these refinements for the whole bind-expression updated with the refined argument a'; furthermore, since the first premise of the rules does not guarantee a to be well-typed, then the current environment Γ is also returned for the cases in which this should fail. (3) the test succeeded (i.e., $\mathbb{\Gamma} = \{\Gamma\}$) and proposed a refinement a' of a different from it (i.e., $a \neq a'$, rule [BindArgRefAnns]): since we do not know whether a' is the best possible refinement for the argument, yet, then before attacking the body κ the system retries to check the expression using the new refinement a' for argument. Finally, (4) the check for the argument succeeded (i.e., $\mathbb{\Gamma} = \{\Gamma\}$) and it proposed its best refinement for the argument (i.e., $a = a'$): then the system can attack the body κ of the bind-expression, which is done in the rule [Bind].

The [Bind] rule is, by far, the most complex rule of our system and needs several auxiliary definitions. First, [Bind] uses the algorithmic system to deduce the best type s for the argument a, since this can be a strict subtype of $\bigvee(\Gamma \triangleright A)$. Then it uses this type s to refine the types in the

annotation A that are compatible with the current Γ, yielding the set $\{s \wedge u \mid u \in (\Gamma \triangleright A)\}$. The function partition is applied to this set: this splits the types in the set so that they are pairwise disjoint (actually, two types with a non-empty intersection are split in three types: their intersection and their two differences).[6] This yields a set of types $\{s_i\}_{i\in I}$ which are the summands into which we want to split the type of the argument for the union rule: indeed we have $\Gamma \vdash_{\mathcal{A}} a : s = \bigvee_{i\in I} s_i$. Therefore the next step it to check that for each $i \in I$ the body κ of the bind-expression has type t under the hypothesis that x has type s_i. This gives a set of result pairs $\{(\kappa', \mathbb{\Gamma}_i)\}_{i\in I}$. We must extract from this set the appropriate information to elaborate the result for the whole bind-expression.

Using the various κ_i's is easy: all these are copies of κ with refined annotations, and we merge all of them simply by unioning the corresponding annotations: this is what the merge function occurring in the conclusion of the rule does. Using the various $\mathbb{\Gamma}_i$'s requires more work, since the type environments in $\mathbb{\Gamma}_i$ contain hypotheses about the variable x defined in the examined bind-expression. In particular, if the type for x has been refined, then we have to reflect this refinement to the free variable of a, since a is bound to x. Consider a Γ' in $\mathbb{\Gamma}_i$ for some i. If the type of x has been refined in Γ', that is, if $\Gamma'(x) \neq s_i$, then we have to refine in Γ' also the free variables of a. For instance imagine that a is (x_1, x_2), $s_i = \mathbb{1}\times\mathbb{1}$, and $\Gamma'(x) = (\mathsf{Int}\times\mathsf{Int}) \vee (\mathsf{Bool} \times \mathsf{String})$. Since $\Gamma'(x)$ is strictly smaller than s_i, then we have to refine the types of the variables in a by proposing two refinements for Γ', namely, $\Gamma'[x_1 :\hat{=} \mathsf{Int}][x_2 :\hat{=} \mathsf{Int}]$ and $\Gamma'[x_1 :\hat{=} \mathsf{Bool}][x_2 :\hat{=} \mathsf{String}]$. This is what $\mathtt{propagate}_{x,a,s_i}$ does: it propagates to the types of the free variables of a any refinement of s_i specified in the typing of x. This yields a new set $\mathbb{\Gamma}'_i$ whose environments refine those in $\mathbb{\Gamma}_i$. Once we obtained this new $\mathbb{\Gamma}'_i$ we can now extract the hypotheses about x to create a new annotation A_i for the binding and pass the rest of the environment as a refinement for the whole bind expression. This is done by the function $\mathtt{extract}_x$ defined as follows: $\mathtt{extract}_x(\mathbb{\Gamma}) \stackrel{\text{def}}{=} (\{(\Gamma\setminus x) \triangleright \Gamma(x) \mid \Gamma \in \mathbb{\Gamma}\}, \{\Gamma\setminus x \mid \Gamma \in \mathbb{\Gamma}\})$ where $\Gamma\setminus x \stackrel{\text{def}}{=} \Gamma \setminus \{x \mapsto \Gamma(x)\}$ for $x \in \mathsf{dom}(\Gamma)$. Finally, the result of the rule is formed by a pair obtained by unioning all the annotations A_i and all the refinements $\mathbb{\Gamma}''_i$ obtained for each $i \in I$.

We conclude the presentation of our system by explaining a simplified version of the main rule for checking λ-abstractions which is applied when the type t to check is an intersection of arrows:

$$[\textsc{Abs}]\ \frac{\begin{array}{c}\{s_i\}_{i\in I} = \mathtt{partition}((\Gamma\triangleright A) \cup \{s_j \mid j \in J\}) \\ (\forall i \in I) \quad \Gamma, (x : s_i) \vdash_{\mathcal{R}} \kappa : t \circ s_i \Rightarrow (\kappa_i, \mathbb{\Gamma}_i) \quad (A_i, \mathbb{\Gamma}'_i) = \mathtt{extract}_x(\mathbb{\Gamma}_i)\end{array}}{\Gamma \vdash_{\mathcal{R}} \lambda x{:}A.\kappa : t \Rightarrow (\lambda x{:}\bigcup_{i\in I} A_i.\, \mathtt{merge}(\{\kappa_i\}_{i\in I}), \bigcup_{i\in I} \mathbb{\Gamma}'_i)}\ t \simeq \bigwedge_{j\in J}(s_j \to t_j)$$

According to [→I-Alg], we must find how to split the domain of the function into some domain types, that we assign to the parameter of the function to check its body. This will yield the intersection type of the function. To determine this set of domains, we take those of the type t we are checking (i.e., $\{s_j \mid j \in J\}$, since $t \simeq \bigwedge_{j\in J}(s_j \to t_j)$) and we add them to those we already know, which are specified in the annotation A of the parameter (i.e., $(\Gamma\triangleright A)$). Then, as for [Bind], we partition this set yielding the set of domains $\{s_i\}_{i\in I}$. As customary for each i we check under the hypothesis $x : s_i$ that the body has the expected type, that is, the type of the function t applied to the type of the parameter s_i, namely, $t \circ s_i$. This yields a set of result pairs $\{(\kappa_i, \mathbb{\Gamma}_i)\}_{i\in I}$ that we use in the same way as we did in [Bind] to form the final result. The only difference is that we do not need any further refinements for the $\mathbb{\Gamma}_i$'s, since, contrary to [Bind], there is no argument whose variables need to be refined.

All the remaining rules (pairs, variables, and the rules for the special cases of unions and empty types) are mostly straightforward and can be found in Appendix B with a detailed explanation and the formal definition of all the auxiliary functions used therein. All that remains to do is to define

[6] Formally, $\mathtt{partition}(\{t_i\}_{i\in I})$ is the smallest (in term of cardinality) non-empty set of types $\{s_j\}_{j\in J}$ such that (i) $\bigvee_{j\in J} s_j \simeq \bigvee_{i\in I} t_i$, (ii) $\forall j \in J.\ \forall j' \in J.\ j \neq j' \Rightarrow s_j \wedge s'_j \simeq \mathbb{0}$, and (iii) $\forall j \in J.\ \forall i \in I.\ s_j \leq t_i$ or $s_j \wedge t_i \simeq \mathbb{0}$

$a : ((\mathsf{Int}\to(\mathsf{Int}\vee\mathsf{Bool}))\vee(\mathsf{Int}\times(\mathsf{Int}\vee\mathsf{Bool})))$
$n : \mathsf{Int}$

Fig. 7. Types of the atoms a and n.

```
1  (a ∈ (Int×Int))  ?  π1a == π2a
2    :(a ∈ (𝟙×𝟙))   ?  π2a
3    :((a  n) ∈ Int) ? (a  n) < 42
4    :(a  n)
```

Fig. 8. Expression $e_\circ$ of the source language.

```
0  bind x0 : A0 = a in
1  bind x1 : A1 = n in
2  bind x2 : A2 = π1x0 in
3  bind x3 : A3 = π2x0 in
4  bind x4 : A4 = x2 == x3 in
5  bind x5 : A5 = x0  x1 in
6  bind x6 : A6 = x5  < 42 in
7  bind x7 : A7 = (x5 ∈ Int) ? x6 : x5 in
8  bind x8 : A8 = (x0 ∈ 𝟙×𝟙) ? x3 : x7 in
9  bind x9 : A9 = (x0 ∈ Int×Int) ? x4 : x8 in x9
```

Fig. 9. MSC-form of the expression $e_\circ$.

the result of the inference algorithm as the fixpoint of the transformation defined by that system. Formally, let κ be a closed MSC-form, we define the annotation reconstruction algorithm $\mathcal{R}$ as:

$$\mathcal{R}(\kappa) = \begin{cases} \kappa & \text{if } \varnothing \vdash_{\mathcal{R}} \kappa : \mathbb{1} \Rightarrow (\kappa, \{\varnothing\}) \\ \mathcal{R}(\kappa') & \text{if } \varnothing \vdash_{\mathcal{R}} \kappa : \mathbb{1} \Rightarrow (\kappa', \{\varnothing\}) \text{ and } \kappa \neq \kappa' \\ \mathsf{Fail} & \text{if } \varnothing \vdash_{\mathcal{R}} \kappa : \mathbb{1} \Rightarrow (\kappa', \{\}) \end{cases}$$

The reconstruction algorithm is sound:

Theorem 5.1 (Soundness). *If κ is a closed MSC-form and $\mathcal{R}(\kappa) = \kappa'$, then $\varnothing \vdash_{\mathcal{A}} \kappa' : t$ for some t.*

Notice that if the algorithm does not fail, then $\lceil\langle\mathcal{R}(\kappa)\rangle\rceil = \lceil\langle\kappa\rangle\rceil$. This, together with Corollary 4.4, yields a sound procedure to type an expression e of the source language. Let κ be the algorithmic expression obtained by adding the annotation $\{\varnothing\triangleright\mathbb{1}\}$ everywhere in $\mathsf{MSC}(e)$. If $\mathcal{R}(\kappa)$ does not fail, then $\varnothing \vdash_{\mathcal{A}} \mathcal{R}(\kappa) : t$. Since $\lceil\langle\mathcal{R}(\kappa)\rangle\rceil = \lceil\langle\kappa\rangle\rceil = \lceil\mathsf{MSC}(e)\rceil \equiv_\alpha e$, then by the soundness part of Corollary 4.4 we can conclude $\varnothing \vdash e : t$. Notice also that the algorithm works for initial annotations different from $\mathbb{1}$, too. In particular, soundness holds also for intermediate terms whose λ-abstractions are explicitly annotated as in $\lambda x{:}A.\boldsymbol{e}$: if it succeeds, the algorithm will refine the term so that its domain is a subtype of $\bigvee(\Gamma\triangleright A)$. This means that we have for free a typing algorithm for the source language (5) of Section 2.2 extended with explicitly annotated functions of the form $\lambda x{:}A.e$. This is why in our prototype, presented in next section, function parameters may be optionally annotated.[7] Finally, we conjecture that the algorithm terminates, that is, that $\mathcal{R}(\kappa)$ is defined for every closed MSC-form κ, but this result is difficult to prove because the rule [AppR] creates new arrow types.

Example. We illustrate on a complete example the behaviour of our inference algorithm. We type the source language expression $e_\circ$ given in Figure 8 in which n and a are atomic expressions (whose definitions we omit) whose types are given in Figure 7. The MSC-form of $e_\circ$ is given in Figure 9. Notice that the various occurrences of $\pi_1 a$ and $a\,n$ are shared, using x_2 and x_5 respectively. We describe the iterations of Algorithm $\mathcal{R}$ which deduces for $e_\circ$ the type Bool. In what follows, we call t_a the original type of a given in Figure 8. We start with $A_0 = t_a$, $A_1 = \mathsf{Int}$, and $A_i = \mathbb{1}$ for $i = 2..9$.

First iteration.

→ `bind` $x_0 \ldots$, $\Gamma = \varnothing$, $A_0 = \{t_a\}$: Rule [Bind] on the only type in the annotation A_0 (we assume nothing is learned while typing a);

→ `bind` $x_1 \ldots$, $\Gamma = \{x_0 : t_a\}$, $A_1 = \{\mathsf{Int}\}$: Rule [Bind] on the only type in the annotation A_1;

→ `bind` $x_2 \ldots$, $\Gamma = \{x_0 : t_a\,,\ x_1 : \mathsf{Int}\}$, $A_2 = \{\mathbb{1}\}$: Rule [BindArgRefEnv] triggers recursively rule [Proj1] to type $\pi_1\, x_0$. It returns the singleton set of environments:

$$\mathbb{\Gamma} = \{\ \{x_0 : (\mathsf{Int}\times(\mathsf{Int}\vee\mathsf{Bool}))\,,\ x_1 : \mathsf{Int}\}\ \}.$$

[7] In the implementation we forbid the annotations written by the user to be refined, so that the domain of $\lambda x{:}A.e$ will be exactly $\bigvee(\Gamma\triangleright A)$. In this way the system deduces for $\lambda x.(x+1)$ the type $\mathsf{Int}\to\mathsf{Int}$ but rejects $\lambda x{:}\mathbb{1}.(x+1)$ as ill-typed.

← `bind` $x_2 \ldots$: Rule [BindArgRefEnv] returns the following set containing two environments
$$\mathbb{\Gamma}_0 = \{\ \{x_0 : (\mathsf{Int} \times (\mathsf{Int} \vee \mathsf{Bool})), x_1 : \mathsf{Int}\}\ ,\ \{x_0 : t_a, x_1 : \mathsf{Int}\}\ \}.$$
Notice that the rest of the program is ignored and $\mathbb{\Gamma}_0$ is propagated upward.

← `bind` $x_1 \ldots$: Rule [Bind] returns. Here since nothing new is learned about the type of x_1 (functions `propagate` and `extract` behave as identities), $\mathbb{\Gamma}_0$ is propagated upward.

← `bind` $x_0 \ldots$: Rule [Bind] returns. Here functions `propagate` and `extract` create the new annotation for x_0 that is $A_0' = \{t_a, (\mathsf{Int} \times (\mathsf{Int} \vee \mathsf{Bool}))\}$

At this point a new annotation has been inferred (i.e., A_0'), so Algorithm $\mathcal{R}$ restarts.

Second iteration.

→ `bind` $x_0 \ldots$, $\Gamma = \varnothing$, $A_0 = \{(\mathsf{Int} \times (\mathsf{Int} \vee \mathsf{Bool}))\ ,\ t_a\}$: Rule [Bind] on the two types in A_0. Here `partition` splits the annotation into $\mathsf{Int} \times (\mathsf{Int} \vee \mathsf{Bool})$ and $t_a \setminus (\mathsf{Int} \times (\mathsf{Int} \vee \mathsf{Bool})) \simeq \mathsf{Int} \to (\mathsf{Int} \vee \mathsf{Bool})$. The rule tries both types for x_0 in turn. We focus first on $\mathsf{Int} \times (\mathsf{Int} \vee \mathsf{Bool})$.

→ `bind` $x_1 \ldots$, $\Gamma = \{x_0 : \mathsf{Int} \times (\mathsf{Int} \vee \mathsf{Bool})\}, A_1 = \{\mathsf{Int}\}$: Rule [Bind] on the only type of the annotation A_1; (the following cases from `bind` x_2 to `bind` x_4 are similar and omitted);

→ `bind` x_5, $\Gamma = \{x_4 : \mathsf{Bool}, \ldots\}$: Rule [BindArgUntyp] since x_0 does not have a function type;

→ `bind` x_6 and `bind` x_7, $\Gamma = \{x_4 : \mathsf{Bool}, \ldots\}$: Rule [BindArgUntyp] since $x_5 \notin \mathrm{dom}(\Gamma)$

→ `bind` $x_8 \ldots$, $\Gamma = \{x_4 : \mathsf{Bool}, \ldots\}$: Rule [Bind] recursively calls [Case]. Here since, the type of x_0 is completely contained in $\mathbb{1} \times \mathbb{1}$, the case rule only returns the original Γ (cf. the definition of $[\_ :\hat{=} \_]$): no new information is learned; the rest of the MSC-form is examined.

→ `bind` $x_9 \ldots$, $\Gamma = \{x_8 : (\mathsf{Int} \vee \mathsf{Bool}), \ldots\}$: Rule [BindArgRefEnv] recursively calls [Case] rule. Here, however, the type of x_0 is not a subtype of the tested type, this rule therefore returns a singleton with a refined environment $\mathbb{\Gamma} = \{\Gamma\{[x_0 :\hat{=} \mathsf{Int}\times\mathsf{Int}]\}$

← `bind` $x_9 \ldots$: Rule [BindArgRefEnv] returns the original environment and a refined one for x_0. The typing does not continue further and returns upward.

← `bind` $x_0 \ldots$ like in the previous iteration the annotation for x_0 comes back to its binder, yielding a new annotation : $A_0'' = \{t_a, (\mathsf{Int} \times (\mathsf{Int} \vee \mathsf{Bool}))), \mathsf{Int}\times\mathsf{Int}\}$

At the third iteration, `partition`() used in [Bind] on the "`bind` x_0" expression splits A_0'' into three types : Int×Int, Int×Bool, and Int→(Int∨Bool). For both product types, the typing succeeds till the end (each time skipping the lines 5–7 where x_0 is used as a function). As for the functional annotation, it is almost straightforward. One caveat is in the typing of x_6: since $< : \mathsf{Int}\to\mathsf{Int}\to\mathsf{Bool}$, the application $x_5\ <\ 42$ introduces a new refinement for x_5 which, at this point, has type Int∨Bool (the return type of x_0). The algorithm propagates both types to A_5 and the rest of the program is typed twice, under both hypotheses. Notice that both succeed since, in the case where x_5 has type Bool, x_6 only occurs in an unreachable branch of a type case. The final MSC-form has annotations A_0={Int×Int, Int×Bool, Int→(Int∨Bool)}, A_1=A_2=Int, A_3={x_0:Int×Int▷Int, x_0:Int×Bool▷Bool}, A_5={x_0:Int→(Int∨Bool)▷Int, x_0:Int→(Int∨Bool)▷Bool}, Bool guarded by the active environments for the others. For this term $\vdash_{\mathcal{R}}$ infers the type Bool.

6 IMPLEMENTATION

We have implemented Algorithm $\mathcal{R}$ in OCaml, using CDuce [CDuce] as a library to provide set-theoretic types and semantic subtyping. The prototype amounts to 3500 lines of OCaml code and features several extensions such as let bindings and records (both formalised in Appendix C) and annotations of function parameters (see Footnote 7). The transformation of terms in their MSC-form is similar to the *locally nameless* approach ([Charguéraud 2012]). Expressions from the source language are transformed so that bound variables are represented using De Bruijn indices, while free variables are represented with symbolic names. While performing this transformation, hash-consing is used to identify structurally equal subterms. We give in Table 1 the code of

Table 1. Types inferred by the implementation (times are in ms)

	Code	Inferred type	MSC	Inf.
1	`let is_int = fun x -> if x is Int then true else false`	(Int → True) ∧ (¬Int → False)	0.02	0.22
	`let is_bool = fun x -> if x is Bool then true else false`	(Bool → True) ∧ (¬Bool → False)	0.02	0.21
2	`type Falsy = False | "" | 0` `type Truthy = ~Falsy`			
	`let not_ = fun x -> if x is Truthy then false else true`	(Truthy → False) ∧ (Falsy → True)	0.03	0.58
	`let to_Bool = fun x -> not_ (not_ x)`	(Truthy → True) ∧ (Falsy → False)	0.02	0.93
	`let and_ = fun x -> fun y -> if x is Truthy then to_Bool y else false`	(Falsy→𝟙→False) ∧ (Truthy→Truthy→True)∧ (Truthy→Falsy→False)	0.03	2.24
	`let or_ = fun x -> fun y -> not_ (and_ (not_ x) (not_ y))`	(Truthy→𝟙→True) ∧ (Falsy→Truthy→True)∧ (Falsy → Falsy → False)	0.03	3.34

3	`strlen : String -> Int`
	`let example14 =`
	`fun input -> fun extra ->`
	`if and_ (is_int input) (is_int(fst extra)) is True`
	`then input + (fst extra)`
	`else if is_int (fst extra) is True then (strlen input) + (fst extra)`
	`else 0`
		((Int ∨ String) → (¬Int×𝟙) → 0)∧ ((Int ∨ String) → (Int×𝟙) → Int)∧ (¬(Int ∨ String) → (¬Int×𝟙) → 0)	0.05	3.61

4	`let example6_wrong =`
	`fun (x : Int|String) -> fun (y : Any) ->`
	`if and_ (is_int x)(is_string y) is True then add x (strlen y) else strlen x`
		Ill typed	0.07	1.52

	`let example6_ok =`
	`fun x -> fun y ->`
	`if and_ (is_int x)(is_string y) is True then add x (strlen y) else strlen x`
		(String → 𝟙 → Int)∧ (Int → String → Int)	0.07	3.51

5	`let detailed_ex =`
	`fun (a : (Int -> (Int|Bool)) |(Int, (Int|Bool))) ->`
	`fun (n : Int) ->`
	`if a is (Int,Int) then (fst a)=(snd a)`
	`else if a is (Any,Any) then snd a`
	`else if (a n) is Int then (a n) < 42`
	`else a n`
		(Int → (Int ∨ Bool)) ∨ (Int×(Int ∨ Bool)) → Int → Bool	0.08	1.77

several functions, using a syntax similar to OCaml, where uppercase identifiers (e.g., True, String) denote types and lowercase identifiers denote variables or constants. For each function we report its inferred type, the time taken to put its body in MSC form, and the time taken to infer its type or typecheck it (for annotated functions). All runtimes are given in milliseconds, averaged over ten runs. The experiments were done on an Intel Core i7-8565U 1.8GHz CPU (with 16GB of RAM). The code was compiled natively using OCaml 4.12.0. All these examples (and more) can be tested online with the interactive prototype hosted at https://typecaseunion.github.io [Castagna et al. 2022].

Code 1 and 2 show that exact overloaded types can be inferred even in the absence of annotations. In Code 1 we encode type predicates as they can be found in Typed Racket. The inferred overloaded types exactly specify the semantics of these functions using the singleton types of the values `true` and `false`, while in Typed Racket this requires these predicates to be primitives of the language and are typed with specific rules. Code 2 implements Boolean operators by considering values as in JavaScript where eight specific "falsy" values (`false`, `""`, `0`, `-0`, `0n`, `undefined`, `null`, and `NaN`) are considered to be equivalent to false, and all the others—called "truthy" values—to be equivalent to true. We first define the type `Falsy` as the union of the singleton types of `false`, `""`, and `0` (the other values are absent in our prototype) and the type `Truthy` as the negation of `Falsy`. We said that our system decides how to split the types of variables in bindings by using the type-cases and the applications of overloaded functions that occur in the program. The function `not_` is an

example in which the decision is based on the type-cases: the exact inferred intersection type is obtained by splitting the type of `x` because `x` is tested in a type-case. The function `to_Bool` is an example in which the decision is based on an overloaded application: the type is inferred by splitting the type of `x` since `x` is the argument of the function `not_`. In `to_Bool` by a double application of `not_` we map truthy values into `true` and falsy ones into `false`, as the type inferred for `to_Bool` exactly specifies. The function `and_` mixes the two kinds of decision since it tests the type of the first argument and applies an overloaded function to the second argument. We could have defined `and_` as two nested tests checking whether both arguments are truthy and returning false otherwise: the system would have inferred the same type which, once more, exactly specifies the semantics of the function. If we wanted to implement for the "and" operator the same semantics as the one defined for the logical AND (`&&`) of JavaScript, then we should instead have used the following definition `fun x -> fun y -> if x is Falsy then x else y` whose inferred type `(Falsy→𝟙→Falsy)∧(Truthy→𝟙→𝟙)` does not specify the function's exact semantics because our system lacks polymorphism (with polymorphic types we would expect the inferred type to be $\forall\alpha.(\alpha\wedge\texttt{Falsy}\to\mathbb{1}\to\alpha\wedge\texttt{Falsy})\wedge(\texttt{Truthy}\to\alpha\to\alpha)$—where α is a type variable—which states that if the first argument is of type (subtype of) `Falsy`, then the result will be of the same type as the type of first argument—independently from the second one—, while if the first argument is of type `Truthy`, then the result will be of the same type as the type of second argument). Finally, the last example in Code 2 defines `or_` by combining the two previous functions according to De Morgan's laws: again the inferred type is exact. The degree of precision achieved by the type inference for the examples in Code 2 is out of reach of all existing approaches to occurrence typing.

Our implementation can type all the 14 paradigmatic examples listed by Tobin-Hochstadt and Felleisen [2010] (THF) whose results we improve in several ways: first, we infer types that are more precise than those inferred in THF; second, our system types all examples without needing any annotation, whereas THF must specify some annotations in 5 of the 14 examples; third, our analysis works also when in these example we employ user-defined connectives and type predicates, whereas in THF these must be hard-coded to be used inside a test. For space reasons, we did not detail all these examples here (but they can be tested in our online prototype by selecting the appropriate menu entry) and chose instead to show only two of them in Code 3 and 4.

Code 3 is Example 14 of THF, which is last and most complete of the 14 examples of THF and summarizes the features of all the others. This definition shows all the improvements brought by our system and listed above: first, we infer a more precise type which discriminates the cases in which the function returns a generic integer or `0` (i.e., `0` is returned whenever the second argument is of type $(\neg\mathsf{Int}\times\mathbb{1})$, independently from the first argument's type); second, our inference does not need any annotation, while in THF both parameters of the function must be explicitly annotated; third, the tested expression is a Boolean expression obtained by applying custom user-defined connectives (`and_`) and type predicates (`is_int`) whose use would make the analysis of THF fail.

Code 4 is Example 6 of THF which shows error detection: if `x` is assumed of type Int∨String (as in `example6_wrong`), then the function is ill-typed, and rightly so since if both arguments are not strings, then `strlen x` is selected and its execution fails. However, if as in `example6_ok`, we let our system determine the types of the parameters, then it rightly determines that the first argument must be either a string or an integer (any other type would select `strlen x` and then fail), but also that when the first is an integer, then the second must be a string, or the function would fail. Such a deduction is out of reach of the approach defined by THF.

Code 5 is the detailed example of the previous section and shows that the type of function parameters can easily be constrained if one wishes. Interestingly, if we remove the `Int` annotation from the second parameter `n`, the system computes a more precise type ((Int→(Bool∨Int)) →

$\mathsf{Int} \to \mathsf{Bool}) \wedge ((\mathsf{Int} \times (\mathsf{Bool} \vee \mathsf{Int})) \to \mathbb{1} \to \mathsf{Bool})$ which clearly states that the second argument of the function needs to be an integer only when the first one is a function.

7 RELATED WORK

As previously said, the present paper extends the system of [Barbanera et al. 1995] with three rules for type-cases and with the use of a particular subtyping relation. We then define, in several steps, a type inference algorithm for this calculus. The resulting calculus and type-inference appears to be particularly well suited for typing programs written in dynamic languages such as JavaScript.

While taking a radically different approach, we achieve a goal similar to occurrence typing, introduced in [Tobin-Hochstadt and Felleisen 2008] and further advanced in [Tobin-Hochstadt and Felleisen 2010], in the context of the Typed Racket language. In this and subsequent work, types are annotated by two logical propositions that record the type of the input depending on the (Boolean) value of the output. For instance, the type of the `number?` function states that when the output is `true`, then the argument has type `Number`, and when the output is `false`, the argument does not. These propositions are propagated and used in particular in type-cases to refine the type of variables and, more generally, expressions in the "then" and "else" branches of a conditional. Furthermore, this analysis focuses on a particular set of pure operations, so that the approach works also in the presence of side-effects. Contrary to these works, we try not to depend on an external logic but, rather, to express as much as possible these conditions with set-theoretic types. For instance, we track the dependency between input and output types of functions using intersection types (cf. Code 1 in Table 1), while type-case expressions are typed using intersection and negation types to refine the typing environments of the branches. Our approach is more global since, not only our analysis strives to infer type information by analyzing all types of results (and not just `true` or `false`), but also tries to perform this analysis for all possible expressions (and not just for a restricted set of expressions). This allows our system to type all the examples given in [Tobin-Hochstadt and Felleisen 2010] (and contrary to the cited work, without needing any annotations) and many more but, as we explain at the end of this section, at the expense of an immediate compatibility with the presence of side-effects.

In a previous work [Castagna et al. 2021] we already used characteristics of semantic subtyping to improve occurrence typing but the approach we used there was completely different from the one presented here. Instead of relying on bindings to track the different occurrences of a same expression, we enriched type environments so that they mapped occurrences of expressions (expressed in terms of paths) to types. This yielded a type-theoretic approach with non standard features (the type environments) that, contrary to the present one, could not capture the flow of information between variables and thus failed to type Code 3 of Table 1. Furthermore, the connection with the union elimination rule was completely missing.

Set-theoretic types have also been used by [Kent 2019, Chapter 5] to extend the logical techniques developed for Typed Racket to track under which hypotheses an expression returns false or not. Kent uses set-theoretic types to express type predicates (a predicate that holds only for a type t has type $p : (t \to \mathtt{True}) \wedge (\neg t \to \mathtt{False})$) as well as to express in a more compact (and, sometimes, more precise) way the types of several built-in Typed Racket functions. It also uses the properties of set-theoretic types to deduce the logical types (i.e., the propositions that hold when an expressions produces `false` or not) of arguments of function applications. The main difference of Kent's approach with respect to ours is that, since it builds on the logical propositions approach, then it focuses the use of set-theoretic types and of the analysis of arguments of applications of a selected set of pure expressions (while we use all expressions) to determine when an expression yields a result of type `False` or $\neg$`False` (while we use all types of results). The consequence is that not only Kent's approach covers fewer cases than ours and cannot infer intersection types, but also the very

fact of focusing on truthy vs. false results may make Kent's analysis fail even for pure Boolean tests where it would be naively expected to work. The approach has however the advantage of building on Typed Racked which provides a mature and high-performing implementation. The reader will find in [Castagna et al. 2021, see section on related work] an extensive and detailed comparison between current approaches of occurrence typing and those based on set-theoretic types.

Our approach is based on program transformation: we transform expressions into MSC-forms. A similar approach is used by Rondon et al. [2008] who transform expressions into *A-normal forms* (ANF) [Sabry and Felleisen 1992] and track precise type information for every sub-expression by keeping this information for the variables. While this solution is close to ours it does not achieve the same degree of precision for the simple reason that, contrary to MSC-forms, ANFs were not designed to target occurrence typing. MSC-forms' rationale is to give a unique name to every α-equivalent sub-expression of the initial term, ANFs instead ensure that arguments of applications are immediate values. While the result looks similar, there are key differences: since the sharing of α-equivalent subterms is used only for typing, it does not need to preserve the semantics of the original term. For example, sub-expressions in the branches of a conditional are hoisted outside the conditional (crucial for occurrence-typing), which must not be done for ANFs. Conversely, all proper subterms of an application must be variables in MSC-forms but not in ANFs.

The typing algorithm we present in Section 5 works as a bi-directional typing algorithm: the definition of a variable gives a forward constraint on its type while the use of a variable (e.g., in a type-case or as part of an application) gives a backward constraint that is added to its definition. From the extensive survey by Dunfield and Krishnaswami [2019a] on bi-directional typing, we see that this technique is well-suited for the type-checking or type-inference of complex features such as, for instance, in [Pierce and Turner 2000] (local type inference in the presence of subtyping), [Pottier and Régis-Gianas 2006] (bi-directional type propagation for typing generalized algebraic data-types), or [Dunfield and Krishnaswami 2019b] (bi-directional type checking for higher rank polymorphism). The two latter works, in particular, seem to indicate that our approach remains viable when extending the present work with parametric polymorphism.

A feature we completely omitted in our study is gradual typing. Works such as [Chaudhuri et al. 2017] (for Flow) or [Rastogi et al. 2015] (for TypeScript), account for the presence of unsafe, already written code, by using a form of gradual typing. Castagna et al. [2021] outline how gradual typing can be integrated in a system with semantic subtyping and occurrence typing using work by [Castagna et al. 2017; 2019]: we think that those ideas can be adapted to the work presented here.

We end this presentation of related work with a discussion on side effects, a crucial feature for dynamic languages. Although in our system we did not take into account side-effects—and actually our system works because all the expressions of our language are pure—it is interesting to see how the different approaches of occurrence typing position themselves with respect to the problem of handling side effects, since this helps to better place our work in the taxonomy of the current literature. As Sam Tobin-Hochstadt insightfully noticed, one can distinguish the approaches that use types to reason about the dynamic behavior of programs according to the set of expressions that are taken into account by the analysis. In the case of occurrence typing, this set is often determined by the way impure expressions are handled. On the one end of the spectrum lies our approach (both this work and the one in Castagna et al. [2021]): our analysis takes into account *all* expressions but, in its current formulation, it works only for pure languages. On the other end of the spectrum we find the approach of Typed Racket whose analysis reasons about a limited and predetermined set of *pure* operations: all data structure accessors. Somewhere in-between lies the approach of the Flow language—whose core features were formalized by Chaudhuri et al. [2017]—which implements a complex effect systems to determine pure expressions. While the system presented here does not work for impure languages, we argue that its foundational nature

predisposes it to be adapted to handle impure expressions as well, by adopting existing solutions or proposing new ones. For instance, it is not hard to modify our system so that it takes into account only a set of predetermined pure expressions, as done by Typed Racket: it suffices to instruct the transformation in MSC-form to use distinct bind variables for distinct occurrences of expressions that are not in this set. However, such a solution would be marginally interesting since by excluding from the analysis all applications, we would lose most of the advantages of our approach with respect to the one with logical propositions. Thus a more interesting solution would be to use some external static analysis tools—e.g., to graft the effect system of Chaudhuri et al. [2017] on ours—to detect impure expressions. The idea would be to mark different occurrences of a same impure expression using different marks and, again, instruct the transformation in MSC-form to use distinct bind variables for expressions with distinct marks. For instance, consider the test $(f\,x \in \mathsf{Int})\,?\,\ldots : \ldots$: if fx were flagged as impure then an occurrence of fx in the "then" branch would not be supposed to be of type Int since the MSC-form of this expressions would use two distinct variables to bind fx occurring in the test and the one in the branch. Although this would certainly improve our analysis, is would still significantly limit the sharing. Which is why we believe that, ultimately, our system should not resort to external static analysis tools to detect impure expressions but, rather, it has to integrate this analysis with the typing one, so as to mark *only* those impure expressions whose side-effects may affect the semantics of some type-cases. For instance, consider a JavaScript object `obj` that we modify as follows: `obj["key"] = 3`. If the field `"key"` is already present in `obj` with type Int and we do not test it more than about this type, then it is not necessary to mark different occurrences of `obj` with different marks, since the result of the type-case will not be changed by the assignment; the same holds true if the field is absent but type-cases do not discriminate on its presence. Otherwise, some occurrences of `obj` must use different marks: the analysis will determine which ones. We leave this study for future work.

8 CONCLUSION

Although the technical development of our work may appear complex, the unfolding of the logical sequence of its steps can be easily summarized. In Section 1 we argued that the essence of occurrence typing can be captured by adding three typing rules, $[\vee]$, $[\in_1]$, and $[\in_2]$: the union elimination rule can split the type of any expressions into a union of two types that can be tested separately and the rules for type-cases distribute these tests differently on the two branches of a type-case. The addition of these three rules yields the system of Section 2 which captures the spirit of occurrence typing, covers the examples proposed by existing approaches, but is not algorithmic. To obtain an algorithmic system, four technical problems are to be solved: (*i*) how to choose on which expressions the rule $[\vee]$ must be applied; (*ii*) given an expression chosen for applying $[\vee]$, how to choose which sub-expression of this expression and which occurrences of this sub-expression should the system use to apply $[\vee]$; (*iii*) how to determine the union of types into which the system should split the type of a sub-expression chosen for $[\vee]$; (*iv*) how to determine the arrows that form the intersection type of a λ-abstraction that is not annotated. Section 3 solves the first two problems—which made the system *non syntax-directed*—by the definition of MSC-forms: the fact that MSC-forms bind atoms whose all proper sub-expressions are variables means that the system chooses to apply $[\vee]$ on *all* sub-expressions, while the maximal sharing property of MSC-forms means that the system chooses *all* occurrences of each sub-expression since it replaces all of them by the same variable. Section 4 solves the last two problems—which made the system *non analytic*—by the definition of annotations: annotations state how to split the type of the bound variables into a union of types (when the variable is bound by a λ this corresponds to splitting the type of the λ-abstraction into an intersection, when the variable is bound by a `bind` this corresponds to splitting the type of the argument of the `bind`-expression into a union). By this sequence of steps

we reduced the problem of typing expressions with occurrence typing to the problem of choosing annotations for MSC-forms and shown that this choice corresponds to determining how to split types into unions for `bind`-expressions and into intersection for λ-abstractions. Section 5 suggests that the choice of how to split these types can be based on a program analysis that focuses on the types tested in type-cases or involved in applications of overloaded functions. Section 6 implements these choices demonstrating the practical implications of our work.

In summary, the logical sequence described above highlights the connection between union elimination and occurrence typing techniques via the addition of negation types and their use in the typing of type-case expressions. It also provides an effective way to reduce this typing problem to the inference of some specific annotations.

From a theoretical viewpoint, our work is a step forward in the quest of an inversion lemma for the union elimination rule. Although we are still far from an inversion lemma, the results of Sections 3 and 4 show that for a well-typed term e of the source language (or of Barbanera et al. [1995]) there exists a canonical way to use the union rule to derive its type, which corresponds to the derivation encoded by $\mathsf{MSC}(e)$. Thus the problem now is no longer when to use the rule, but how to determine the split of the type of the argument of the union rule into the union of two types, which coincides with inferring the annotations for the corresponding binding-expression.

From a practical viewpoint, our work reframes the problem of occurrence typing into a classical setting that has been actively studied for thirty years and for which a wealth of results and techniques already exists. We want to transpose some of them to our specific setting, in particular the extension to polymorphism and the generation and resolution of systems of constraints, to infer the polymorphic types we hinted at in Section 6. For this we count reusing the theory of polymorphic types with semantic subtyping [Castagna and Xu 2011] together with the typing techniques and algorithms developed for CDuce, both for its explicitly typed version [Castagna et al. 2015, 2014] and the implicitly typed one [Castagna et al. 2016; Petrucciani 2019]. Eminently of practical interest is also the fact that we effectively reduced type inference to a very specific problem, namely, the reconstruction of some specific annotations. The algorithm we described in Section 5 is just one possible solution to this problem, but our formal setting opens the way to the definition of other different techniques. In particular, we are studying the feasibility of switching from the current system that at each pass generates type refinements for the variables of the term, to one that generates, instead, sets of type constraints (such as those defined by Petrucciani [2019, Chapter 4]) whose resolution would yield these (and hopefully better) refinements. This seems an obvious choice if we want to handle polymorphism and it would also improve the precision of our algorithm which currently works poorly when higher-order function parameters are not explicitly annotated. This shortcoming is expected—and shared among the approaches that lack polymorphism—since our algorithm initializes higher-order parameters with the type $\mathbb{0}\to\mathbb{1}$ while, if type variables were available, the algorithm could instead initialize them with $\alpha\to\beta$ where α and β are fresh. This would allow the system to better track and refine the types of these parameters.

ACKNOWLEDGMENTS

This research was partially supported by Labex DigiCosme (project ANR-11-LABEX-0045- DIGICOSME) operated by ANR as part of the program «Investissement d'Avenir» Idex Paris-Saclay (ANR-11-IDEX-0003-02), by the « Chaire Langages Dynamiques pour les Données » of the Paris-Saclay foundation, and by a Google PhD fellowship. The authors would like to thank Delia Kesner for her help with the rewriting systems.

REFERENCES

Franco Barbanera, Mariangiola Dezani-Ciancaglini, and Ugo de'Liguoro. 1995. Intersection and Union Types. *Inf. Comput.* 119, 2 (June 1995), 202–230. https://doi.org/10.1006/inco.1995.1086

Giuseppe Castagna. 2020. Covariance and Controvariance: a fresh look at an old issue (a primer in advanced type systems for learning functional programmers). *Logical Methods in Computer Science* 16, 1 (2020), 15:1–15:58. https://doi.org/10.23638/LMCS-16(1:15)2020

Giuseppe Castagna and Victor Lanvin. 2017. Gradual Typing with Union and Intersection Types. *Proc. ACM Program. Lang.* 1, ICFP, Article 41 (Aug. 2017), 28 pages. https://doi.org/10.1145/3110285

Giuseppe Castagna, Victor Lanvin, Mickaël Laurent, and Kim Nguyễn. 2021. Revisiting Occurrence Typing. (oct 2021). arXiv:1907.05590 To appear in *Science of Computer Programming*, Elsevier.

Giuseppe Castagna, Victor Lanvin, Tommaso Petrucciani, and Jeremy G. Siek. 2019. Gradual Typing: a New Perspective. *Proc. ACM Program. Lang.* 3, POPL '19 46th ACM Symposium on Principles of Programming Languages, Article 16 (Jan. 2019), 32 pages. https://doi.org/10.1145/3290329

Giuseppe Castagna, Mickaël Laurent, Kim Nguyễn, and Matthew Lutze. 2022. *Prototype for Article: On Type-Cases, Union Elimination, and Occurrence Typing*. https://doi.org/10.1145/3462306 Online interactive version available at https://typecaseunion.github.io.

Giuseppe Castagna, Kim Nguyễn, Zhiwu Xu, and Pietro Abate. 2015. Polymorphic functions with set-theoretic types. Part 2: local type inference and type reconstruction. In *Proceedings of the 42nd Annual ACM SIGPLAN Symposium on Principles of Programming Languages (POPL '15)*. 289–302. https://doi.org/10.1145/2676726.2676991

Giuseppe Castagna, Kim Nguyễn, Zhiwu Xu, Hyeonseung Im, Sergueï Lenglet, and Luca Padovani. 2014. Polymorphic Functions with Set-Theoretic Types. Part 1: Syntax, Semantics, and Evaluation. In *Proceedings of the 41st Annual ACM SIGPLAN Symposium on Principles of Programming Languages (POPL '14)*. 5–17. https://doi.org/10.1145/2676726.2676991

Giuseppe Castagna, Tommaso Petrucciani, and Kim Nguyễn. 2016. Set-Theoretic Types for Polymorphic Variants. In *ICFP '16, 21st ACM SIGPLAN International Conference on Functional Programming*. 378–391. https://doi.org/10.1145/2951913.2951928

Giuseppe Castagna and Zhiwu Xu. 2011. Set-theoretic Foundation of Parametric Polymorphism and Subtyping. In *ICFP '11: 16th ACM-SIGPLAN International Conference on Functional Programming*. 94–106. https://doi.org/10.1145/2034773.2034788

CDuce. *The CDuce Compiler*. CDuce https://www.cduce.org

Arthur Charguéraud. 2012. The Locally Nameless Representation. *J. Autom. Reason.* 49, 3 (2012), 363–408. https://doi.org/10.1007/s10817-011-9225-2

Avik Chaudhuri, Panagiotis Vekris, Sam Goldman, Marshall Roch, and Gabriel Levi. 2017. Fast and Precise Type Checking for JavaScript. *Proc. ACM Program. Lang.* 1, OOPSLA, Article 48 (Oct. 2017), 30 pages. https://doi.org/10.1145/3133872

Mariangiola Dezani-Ciancaglini. 2020. Personal communication.

Mariangiola Dezani-Ciancaglini, Alain Frisch, Elio Giovannetti, and Yoko Motohama. 2003. The Relevance of Semantic Subtyping. *Electronic Notes in Theoretical Computer Science* 70, 1 (2003), 88 – 105. https://doi.org/10.1016/S1571-0661(04)80492-4 ITRS '02, Intersection Types and Related Systems (FLoC Satellite Event).

Jana Dunfield and Neel Krishnaswami. 2019a. Bidirectional Typing. *CoRR* abs/1908.05839 (2019). arXiv:1908.05839

Jana Dunfield and Neelakantan R. Krishnaswami. 2019b. Sound and Complete Bidirectional Typechecking for Higher-Rank Polymorphism with Existentials and Indexed Types. *Proc. ACM Program. Lang.* 3, POPL, Article 9 (Jan. 2019), 28 pages. https://doi.org/10.1145/3290322

Facebook. *Flow*. Facebook https://flow.org/

Alain Frisch. 2004. *Théorie, conception et réalisation d'un langage de programmation adapté à XML*. Ph. D. Dissertation. Université Paris Diderot. http://www.cduce.org/papers/frisch_phd.pdf

Alain Frisch, Giuseppe Castagna, and Véronique Benzaken. 2002. Semantic Subtyping. In *LICS '02, 17th Annual IEEE Symposium on Logic in Computer Science*. IEEE Computer Society Press, 137–146. https://doi.org/10.1109/LICS.2002.1029823

Alain Frisch, Giuseppe Castagna, and Véronique Benzaken. 2008. Semantic subtyping: dealing set-theoretically with function, union, intersection, and negation types. *Journal of the ACM* 55, 4 (Sept. 2008), 19:1–19:64. http://doi.acm.org/10.1145/1391289.1391293

J. Roger Hindley and Jonathan P. Seldin. 2008. *Lambda-Calculus and Combinators An Introduction*. Cambridge University Press.

Andrew M. Kent. 2019. *Advanced Logical Type Systems for Untyped Languages*. Ph. D. Dissertation. Indiana University. https://pnwamk.github.io/docs/dissertation.pdf

David MacQueen, Gordon Plotkin, and Ravi Sethi. 1986. An ideal model for recursive polymorphic types. *Information and Control* 71, 1 (1986), 95–130. https://doi.org/10.1016/S0019-9958(86)80019-5

Per Martin-Löf. 1994. *Analytic and Synthetic Judgements in Type Theory*. Springer Netherlands, Dordrecht, 87–99. https://doi.org/10.1007/978-94-011-0834-8_5

Microsoft. *TypeScript*. Microsoft https://www.typescriptlang.org/

Tommaso Petrucciani. 2019. *Polymorphic Set-Theoretic Types for Functional Languages*. Ph. D. Dissertation. Joint Ph.D. Thesis, Università di Genova and Université Paris Diderot. https://tel.archives-ouvertes.fr/tel-02119930

Benjamin C. Pierce and David N. Turner. 2000. Local Type Inference. *ACM Trans. Program. Lang. Syst.* 22, 1 (Jan. 2000), 1–44. https://doi.org/10.1145/345099.345100

François Pottier and Yann Régis-Gianas. 2006. Stratified type inference for generalized algebraic data types. In *Proceedings of the 33rd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2006, Charleston, South Carolina, USA, January 11-13, 2006*, J. Gregory Morrisett and Simon L. Peyton Jones (Eds.). ACM, 232–244. https://doi.org/10.1145/1111037.1111058

Aseem Rastogi, Nikhil Swamy, Cédric Fournet, Gavin Bierman, and Panagiotis Vekris. 2015. Safe and Efficient Gradual Typing for TypeScript. In *Proceedings of the 42nd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages* (Mumbai, India) *(POPL '15)*. Association for Computing Machinery, New York, NY, USA, 167–180. https://doi.org/10.1145/2676726.2676971

Patrick Maxim Rondon, Ming Kawaguchi, and Ranjit Jhala. 2008. Liquid types. In *Proceedings of the ACM SIGPLAN 2008 Conference on Programming Language Design and Implementation, Tucson, AZ, USA, June 7-13, 2008*, Rajiv Gupta and Saman P. Amarasinghe (Eds.). ACM, 159–169. https://doi.org/10.1145/1375581.1375602

Amr Sabry and Matthias Felleisen. 1992. Reasoning about Programs in Continuation-Passing Style.. In *Proceedings of the 1992 ACM Conference on LISP and Functional Programming (LFP '92)*. Association for Computing Machinery, 288–298. https://doi.org/10.1145/141471.141563

Sam Tobin-Hochstadt and Matthias Felleisen. 2008. The Design and Implementation of Typed Scheme. In *Proceedings of the 35th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages* (San Francisco, California, USA) *(POPL '08)*. ACM, New York, NY, USA, 395–406. https://doi.org/10.1145/1328438.1328486

Sam Tobin-Hochstadt and Matthias Felleisen. 2010. Logical types for untyped languages. In *Proceedings of the 15th ACM SIGPLAN International Conference on Functional Programming* (Baltimore, Maryland, USA) *(ICFP '10)*. ACM, New York, NY, USA, 117–128. https://doi.org/10.1145/1863543.1863561

Types 2019. What exactly should we call syntax-directed inference rules? Discussion on the Types mailing list. http://lists.seas.upenn.edu/pipermail/types-list/2019/002138.html.

Wikipedia. 2021. Peter Parker principle. https://en.wikipedia.org/wiki/With_great_power_comes_great_responsibility [Online; accessed 22-October-2021].

Andrew K. Wright and Matthias Felleisen. 1994. A Syntactic Approach to Type Soundness. *Information and Computation* 115, 1 (1994), 38–94. https://doi.org/10.1006/inco.1994.1093

A SUPPLEMENTAL DEFINITIONS

A.1 Subtyping Relation

Subtyping is defined by giving a set-theoretic interpretation of the types of Definition 2.1 into a suitable domain $\mathcal{D}$:

Definition A.1 (Interpretation domain [Frisch et al. 2008]). *The* interpretation domain $\mathcal{D}$ *is the set of finite terms d produced inductively by the following grammar*

$$d ::= c \mid (d, d) \mid \{(d, \partial), \ldots, (d, \partial)\}$$
$$\partial ::= d \mid \Omega$$

where c ranges over the set C of constants and where Ω is such that $\Omega \notin \mathcal{D}$.

The elements of $\mathcal{D}$ correspond, intuitively, to (denotations of) the results of the evaluation of expressions. In particular, in a higher-order language, the results of computations can be functions which, in this model, are represented by sets of finite relations of the form $\{(d_1, \partial_1), \ldots, (d_n, \partial_n)\}$, where Ω (which is not in $\mathcal{D}$) can appear in second components to signify that the function fails (i.e., evaluation is stuck) on the corresponding input. This is implemented by using in the second projection the meta-variable ∂ which ranges over $\mathcal{D}_\Omega = \mathcal{D} \cup \{\Omega\}$ (we reserve d to range over $\mathcal{D}$, thus excluding Ω). This constant Ω is used to ensure that $\mathbb{1} \to \mathbb{1}$ is not a supertype of all function types: if we used d instead of ∂, then every well-typed function could be subsumed to $\mathbb{1} \to \mathbb{1}$ and, therefore, every application could be given the type $\mathbb{1}$, independently from its argument as long as this argument is typable (see Section 4.2 of [Frisch et al. 2008] for details). The restriction to *finite* relations corresponds to the intuition that the denotational semantics of a function is given by the set of its finite approximations, where finiteness is a restriction necessary (for cardinality reasons) to give the semantics to higher-order functions.

We define the interpretation $[\![t]\!]$ of a type t so that it satisfies the following equalities, where $\mathcal{P}_{\text{fin}}$ denotes the restriction of the powerset to finite subsets and $\mathbb{B}$ denotes the function that assigns to each basic type the set of constants of that type, so that for every constant c we have $c \in \mathbb{B}(\boldsymbol{b}_c)$ (we use $\boldsymbol{b}_c$ to denote the basic type of the constant c):

$$[\![\mathbb{0}]\!] = \emptyset \qquad [\![t_1 \vee t_2]\!] = [\![t_1]\!] \cup [\![t_2]\!] \qquad [\![\neg t]\!] = \mathcal{D} \setminus [\![t]\!]$$
$$[\![b]\!] = \mathbb{B}(b) \qquad [\![t_1 \times t_2]\!] = [\![t_1]\!] \times [\![t_2]\!]$$
$$[\![t_1 \to t_2]\!] = \{R \in \mathcal{P}_{\text{fin}}(\mathcal{D} \times \mathcal{D}_\Omega) \mid \forall (d, \partial) \in R.\, d \in [\![t_1]\!] \implies \partial \in [\![t_2]\!]\}$$

We cannot take the equations above directly as an inductive definition of $[\![]\!]$ because types are not defined inductively but coinductively. Notice however that the contractivity condition of Definition 2.1 ensures that the binary relation $\triangleright \subseteq \mathbf{Types} \times \mathbf{Types}$ defined by $t_1 \vee t_2 \triangleright t_i$, $t_1 \wedge t_2 \triangleright t_i$, $\neg t \triangleright t$ is Noetherian. This gives an induction principle[8] on **Types** that we use combined with structural induction on $\mathcal{D}$ to give the following definition, which validates these equalities.

Definition A.2 (Set-theoretic interpretation of types [Frisch et al. 2008]). *We define a binary predicate $(d : t)$ ("the element d belongs to the type t"), where $d \in \mathcal{D}$ and $t \in$ **Types**, by*

[8] In a nutshell, we can do proofs and give definitions by induction on the structure of unions and negations—and, thus, intersections—but arrows, products, and basic types are the base cases for the induction.

induction on the pair (d, t) *ordered lexicographically. The predicate is defined as follows:*

$$\begin{aligned}
(c : b) &= c \in \mathbb{B}(b) \\
((d_1, d_2) : t_1 \times t_2) &= (d_1 : t_1) \text{ and } (d_2 : t_2) \\
(\{(d_1, \partial_1), ..., (d_n, \partial_n)\} : t_1 \to t_2) &= \forall i \in [1..n].\ \text{if } (d_i : t_1) \text{ then } (\partial_i : t_2) \\
(d : t_1 \vee t_2) &= (d : t_1) \text{ or } (d : t_2) \\
(d : \neg t) &= \text{not } (d : t) \\
(\partial : t) &= \text{false} \qquad \textit{otherwise}
\end{aligned}$$

We define the set-theoretic interpretation $[\![]\!] : \mathbf{Types} \to \mathcal{P}(\mathcal{D})$ *as* $[\![t]\!] = \{d \in \mathcal{D} \mid (d : t)\}$.

Finally, we define the subtyping preorder and its associated equivalence relation as follows.

Definition A.3 (Subtyping relation [Frisch et al. 2008]). *We define the* subtyping *relation* $\leq$ *and the* subtyping equivalence *relation* $\simeq$ *as* $t_1 \leq t_2 \stackrel{\text{def}}{\iff} [\![t_1]\!] \subseteq [\![t_2]\!]$ *and* $t_1 \simeq t_2 \stackrel{\text{def}}{\iff} (t_1 \leq t_2)$ and $(t_2 \leq t_1)$.

A.2 Capture Avoiding Substitution

$$c\{e'/x\} = c \tag{9}$$
$$x\{e'/x\} = e' \tag{10}$$
$$y\{e'/x\} = y \qquad x \neq y \tag{11}$$
$$(\lambda x.e)\{e'/x\} = \lambda x.e \tag{12}$$
$$(\lambda y.e)\{e'/x\} = \lambda y.(e\{e'/x\}) \qquad x \neq y, y \notin \text{fv}(e') \tag{13}$$
$$(\lambda y.e)\{e'/x\} = \lambda z.(e\{z/y\}\{e'/x\}) \qquad x \neq y, y \in \text{fv}(e'), z \text{ fresh} \tag{14}$$
$$(e_1 e_2)\{e'/x\} = (e_1\{e'/x\})(e_2\{e'/x\}) \tag{15}$$
$$(e_1, e_2)\{e'/x\} = (e_1\{e'/x\}, e_2\{e'/x\}) \tag{16}$$
$$(\pi_i e)\{e'/x\} = \pi_i(e\{e'/x\}) \tag{17}$$
$$((e_1 \in \tau)\ ?\ e_2 : e_3)\{e'/x\} = (e_1\{e'/x\} \in \tau)\ ?\ e_2\{e'/x\} : e_3\{e'/x\} \tag{18}$$

A.3 Canonical Declarative Deductions

$$[\text{Const}]\ \frac{}{\Gamma \vdash_C c : \boldsymbol{b_c}} \qquad [\text{Ax}]\ \frac{}{\Gamma \vdash_C x : \Gamma(x)}\ x \in \text{dom}(\Gamma)$$

$$[\to\text{I}^{(\wedge)}]\ \frac{\forall i \in I \quad \Gamma, x : s_i \vdash_C e : t_i}{\Gamma \vdash_C \lambda x.e : \bigwedge_{i \in I} s_i \to t_i} \qquad [\to\text{E}^{(\leq)}]\ \frac{\Gamma \vdash_C e_1 : t \leq t_1 \to t_2 \quad \Gamma \vdash_C e_2 : t_1}{\Gamma \vdash_C e_1 e_2 : t_2}$$

$$[\times\text{I}]\ \frac{\Gamma \vdash_C e_1 : t_1 \qquad \Gamma \vdash_C e_2 : t_2}{\Gamma \vdash_C (e_1, e_2) : t_1 \times t_2} \qquad [\times\text{E}_1^{(\leq)}]\ \frac{\Gamma \vdash_C e : t \leq t_1 \times t_2}{\Gamma \vdash_C \pi_1 e : t_1} \qquad [\times\text{E}_2^{(\leq)}]\ \frac{\Gamma \vdash_C e : t \leq t_1 \times t_2}{\Gamma \vdash_C \pi_2 e : t_2}$$

$$[\vee+^{(\leq)}]\ \frac{\Gamma \vdash_C e' : \bigvee_{i \in I} t_i \qquad (\forall i \in I) \quad \Gamma, x : t_i \vdash_C e : s_i \leq t}{\Gamma \vdash_C e\{e'/x\} : t}\ I \neq \varnothing$$

$$[\mathbb{0}]\ \frac{\Gamma \vdash_C e : \mathbb{0}}{\Gamma \vdash_C (e \in t)\ ?\ e_1 : e_2 : \mathbb{0}} \qquad [\in_1^{(\leq)}]\ \frac{\Gamma \vdash_C e : t_\circ \leq t \quad \Gamma \vdash_C e_1 : t_1}{\Gamma \vdash_C (e \in t)\ ?\ e_1 : e_2 : t_1} \qquad [\in_2^{(\leq)}]\ \frac{\Gamma \vdash_C e : t_\circ \leq \neg t \quad \Gamma \vdash_C e_2 : t_2}{\Gamma \vdash_C (e \in t)\ ?\ e_1 : e_2 : t_2}$$

A.4 Operators on Types

The various systems presented in this work use the following type-operators:

$$\begin{aligned}
\mathrm{dom}(t) &= \max\{u \mid t \leq u \to \mathbb{1}\} \\
t \circ s &= \min\{u \mid t \leq s \to u\} \\
t \blacksquare s &= \min\{u \mid t \circ (\mathrm{dom}(t) \setminus u) \leq \neg s\} \\
t \blacktriangleright s &= \max\{u \mid t \circ u \leq s\} \\
\boldsymbol{\pi_1}(t) &= \min\{u \mid t \leq u \times \mathbb{1}\} \\
\boldsymbol{\pi_2}(t) &= \min\{u \mid t \leq \mathbb{1} \times u\}
\end{aligned}$$

In words, $t \circ s$ is the best (i.e., smallest wrt $\leq$) type we can deduce for the application of a function of type t to an argument of type s; $t \blacksquare s$ is the largest type in $\mathrm{dom}(t)$ such that the application of a function of type t to an argument of that type will not surely give a result in $\neg s$, that is, it is the largest set of valid arguments that when applied to a function of type t *may return* a result in s; $t \blacktriangleright s$ is the largest set of valid arguments that when applied to a function of type t *only return* results in s. Projection and domain are standard. All these operators can be effectively computed as shown below (see Castagna et al. [2021]; Frisch et al. [2008] for details and proofs).

For $t \simeq \bigvee_{i\in I}\left(\bigwedge_{p\in P_i}(s_p \to t_p) \wedge \bigwedge_{n\in N_i}\neg(s'_n \to t'_n)\right)$, the first four operators are computed by:

$$\mathrm{dom}(t) = \bigwedge_{i\in I}\bigvee_{p\in P_i} s_p$$

$$t \circ s = \bigvee_{i\in I}\left(\bigvee_{\{Q\subseteq P_i \mid s\not\leq\bigvee_{q\in Q} s_q\}}\left(\bigwedge_{p\in P_i\setminus Q} t_p\right)\right) \qquad (\text{for } s \leq \mathrm{dom}(t))$$

$$t \blacksquare s = \mathrm{dom}(t) \wedge \bigvee_{i\in I}\left(\bigwedge_{\{P\subseteq P_i \mid s\leq\bigvee_{p\in P}\neg t_p\}}\left(\bigvee_{p\in P}\neg s_p\right)\right)$$

$$t \blacktriangleright s = \bigwedge_{i\in I}\left(\bigvee_{\{P\subseteq P_i \mid \bigwedge_{p\in P} t_p\leq s\}}\left(\bigwedge_{p\in P} s_p\right)\right)$$

For $t \simeq \bigvee_{i\in I}\left(\bigwedge_{p\in P_i}(s_p, t_p) \wedge \bigwedge_{n\in N_i}\neg(s'_n, t'_n)\right)$ the last two operators are computed by

$$\boldsymbol{\pi_1}(t) = \bigvee_{i\in I}\bigvee_{N'\subseteq N_i}\left(\bigwedge_{p\in P_i} s_p \wedge \bigwedge_{n\in N'}\neg s'_n\right)$$

$$\boldsymbol{\pi_2}(t) = \bigvee_{i\in I}\bigvee_{N'\subseteq N_i}\left(\bigwedge_{p\in P_i} t_p \wedge \bigwedge_{n\in N'}\neg t'_n\right)$$

Furthermore the algorithm for reconstructing annotations uses the operator $t \circ_{\mathbb{1}} s$ defined as

$$t \circ_{\mathbb{1}} s = \begin{cases} t \circ s & \text{if } s \leq \mathsf{dom}(t) \\ \mathbb{1} & \text{otherwise} \end{cases}$$

that can be easily computed from $\mathsf{dom}(s)$ and $t \circ s$.

A.5 Unwinding

$$\begin{aligned}
\lceil c \rceil &= c \\
\lceil x \rceil &= x \\
\lceil \lambda x.\boldsymbol{e} \rceil &= \lambda x.\lceil \boldsymbol{e} \rceil \\
\lceil \boldsymbol{e}_1 \boldsymbol{e}_2 \rceil &= \lceil \boldsymbol{e}_1 \rceil \lceil \boldsymbol{e}_2 \rceil \\
\lceil (\boldsymbol{e}_1, \boldsymbol{e}_2) \rceil &= (\lceil \boldsymbol{e}_1 \rceil, \lceil \boldsymbol{e}_2 \rceil) \\
\lceil \pi_i \boldsymbol{e} \rceil &= \pi_i \lceil \boldsymbol{e} \rceil && i = 1, 2 \\
\lceil (\boldsymbol{e} \in \tau)\, ?\, \boldsymbol{e}_1 : \boldsymbol{e}_2 \rceil &= (\lceil \boldsymbol{e} \rceil \in \tau)\, ?\, \lceil \boldsymbol{e}_1 \rceil : \lceil \boldsymbol{e}_2 \rceil \\
\lceil \mathtt{bind}\, x = \boldsymbol{e}_1\, \mathtt{in}\, \boldsymbol{e}_2 \rceil &= \lceil \boldsymbol{e}_2 \rceil \{ \lceil \boldsymbol{e}_1 \rceil / x \}
\end{aligned}$$

A.6 Reduction Semantics of the Intermediate Language

For the goals of this work it is not necessary to define a reduction semantics for the intermediate language defined in Section 3.1. This system was introduced to encode typing derivations, so what really matters is that any typable intermediate term has a type that can be deduced also for its unwinding. Nevertheless, it is interesting to define the reduction semantics of the annotated terms so that their reduction encodes the reduction of their unwindings.

The idea of this definition is that the bind-expressions must be evaluated only when their result is needed. In other words, binding-expressions follow a call-by-need reduction strategy. This can be formalized by using some specific contexts as follows.

A *context* C is an expression with a hole (written $[\,]$) in it. We write $C[e]$ for the expression obtained by replacing the hole in C with e. We write $C\lfloor e \rceil$ for $C[e]$ when the free variables of e are not bound by C: for example, $\mathtt{bind}\, x = e_1\, \mathtt{in}\, x$ is of the form $C[x]$ – with $C \equiv (\mathtt{bind}\, x = e_1\, \mathtt{in}\, [\,])$ – but not of the form $C\lfloor x \rceil$; conversely, $\mathtt{bind}\, x = e_1\, \mathtt{in}\, y$ is both of the form $C[y]$ and $C\lfloor y \rceil$.

Evaluation contexts E are the subset of contexts generated by the following grammar:

$$E ::= [\,] \mid vE \mid Ee \mid (v, E) \mid (E, e) \mid \pi_i E \mid (E \in \tau)\, ?\, e : e \mid \mathtt{bind}\, x = e\, \mathtt{in}\, E$$

We then add to the notions of reduction the following one:

$$\mathtt{bind}\, x = e\, \mathtt{in}\, E\lfloor x \rceil \;\rightsquigarrow\; (E\lfloor x \rceil)\{e/x\} \tag{19}$$

This implements the reduction defined for the declarative system (i.e., $\lceil e \rceil \rightsquigarrow \lceil e' \rceil$ implies $e \rightsquigarrow^+ e'$). If we want to implement the parallel reduction of Appendix D.1.1, then we have to add also the following production to the definition of evaluation context:

$$E ::= \mathtt{bind}\, x = E\, \mathtt{in}\, E\lfloor x \rceil$$

and replace the previous notion of reduction by the following one:

$$\mathtt{bind}\, x = v\, \mathtt{in}\, E\lfloor x \rceil \;\rightsquigarrow\; (E\lfloor x \rceil)\{v/x\} \tag{20}$$

A.7 Canonical Forms for the Intermediate Language

The definition of the intermediate expressions is a step forward in solving the problem of typing a declarative expression, but it also brings a new problem, since we now have to decide where to put the bindings in a declarative expression so as to make it a typable intermediate expression. We can get rid of this problem simply by adding bindings wherever it is possible, so that every sub-expression of the original declarative expression will be bound to a variable. This corresponds to considering intermediate expressions that have a very specific form that we call *canonical forms* and that constitute a sub-language of the intermediate expressions.

An intermediate expression $\boldsymbol{e}$ is a *canonical form* if it is produced by the following grammar.

$$\begin{array}{lrcl} \textbf{Atomic expressions} & \boldsymbol{a} & ::= & x \mid c \mid \lambda x.\boldsymbol{\kappa} \mid (x,x) \mid xx \mid (x{\in}\tau)\,?\,x:x \mid \pi_i x \\ \textbf{Canonical Forms} & \boldsymbol{\kappa} & ::= & x \mid \mathtt{bind}\, x = \boldsymbol{a}\, \mathtt{in}\, \boldsymbol{\kappa} \end{array} \tag{21}$$

Canonical forms, ranged over by $\boldsymbol{\kappa}$, are variables possibly preceded by a list of bindings of variables to atoms. Atoms are either λ-abstractions whose body is a canonical form or any other expression in which all proper sub-expressions are variables. Therefore, bindings can appear in a canonical form either at top-level or at the beginning of the body of a function. Notice that variables are atoms and, therefore, it is possible to have aliasing (e.g., $\mathtt{bind}\, x = y\, \mathtt{in}\, \boldsymbol{\kappa}$): we will get rid of aliasing in the next section, but having it here yields a simpler definition of the transformation $[\![.]\!]$ later in this section.

Since canonical forms are also intermediate expressions, then the typing rules and the definition of unwinding for intermediate terms of Section 3.2 apply to canonical forms, too. Canonical forms are enough to "represent" well typed intermediate expressions since we have the following (non trivial) property:

Proposition A.4. *For every intermediate expression $\boldsymbol{e}$, if $\Gamma \vdash_I \boldsymbol{e} : t$, then there exists a canonical form $\boldsymbol{\kappa}$ such that $\Gamma \vdash_I \boldsymbol{\kappa} : t$ and $\lceil \boldsymbol{e} \rceil = \lceil \boldsymbol{\kappa} \rceil$.*

Since a well-typed intermediate expression represents a class of derivations for the source language expression obtained by its unwinding, then the property above tells us that canonical forms suffice to provide such a representation.

We can prove the property above by defining a transformation from an intermediate expression to a canonical form that satisfies the property.

Let Δ denote a possibly empty list of mappings from variables to atoms. We note these lists extensionally by separating elements by a semicolon, that is, $x_1 \mapsto \boldsymbol{a}_1; \ldots; x_n \mapsto \boldsymbol{a}_n$ and use ε to denote the empty list. Next we define an operation $\mathsf{term}(\Delta, x)$ which takes a list of mappings Δ and a variable x and constructs the canonical form whose binding are those listed in Δ and whose body is x, that is:

$$\begin{array}{c} \mathsf{term}(\varepsilon, x) \stackrel{\text{def}}{=} x \\ \mathsf{term}((y{\mapsto}\boldsymbol{a}; \Delta), x) \stackrel{\text{def}}{=} \mathtt{bind}\, y = \boldsymbol{a}\, \mathtt{in}\, \mathsf{term}(\Delta, x) \end{array}$$

We can now define the function $[\![\boldsymbol{e}]\!]$ that transforms an expression $\boldsymbol{e}$ into a pair (Δ, x) formed by a list of mappings Δ and a variable x that will be bound to the atom representing $\boldsymbol{e}$. The definition

is as follows, where $x_\circ$ is a fresh variable.

$$
\begin{aligned}
[\![c]\!] &= ((x_\circ \mapsto c), x_\circ) \\
[\![x]\!] &= (\varepsilon, x) \\
[\![\lambda x.\boldsymbol{e}]\!] &= ((x_\circ \mapsto \lambda x.\mathsf{term}[\![\boldsymbol{e}]\!]), x_\circ) \\
[\![\pi_i \boldsymbol{e}]\!] &= ((\Delta; x_\circ \mapsto \pi_i x), x_\circ) && \text{where } (\Delta, x) = [\![\boldsymbol{e}]\!] \\
[\![\boldsymbol{e}_1 \boldsymbol{e}_2]\!] &= ((\Delta_1; \Delta_2; x_\circ \mapsto x_1 x_2), x_\circ) && \text{where } (\Delta_1, x_1) = [\![\boldsymbol{e}_1]\!],\ (\Delta_2, x_2) = [\![\boldsymbol{e}_2]\!] \\
[\![(\boldsymbol{e}_1, \boldsymbol{e}_2)]\!] &= ((\Delta_1; \Delta_2; x_\circ \mapsto (x_1, x_2)), x_\circ) && \text{where } (\Delta_1, x_1) = [\![\boldsymbol{e}_1]\!],\ (\Delta_2, x_2) = [\![\boldsymbol{e}_2]\!] \\
[\![(\boldsymbol{e} \in \tau)\ ?\ \boldsymbol{e}_1 : \boldsymbol{e}_2]\!] &= ((\Delta; \Delta_1; \Delta_2; x_\circ \mapsto (x \in \tau)\ ?\ x_1 : x_2), x_\circ) \\
&\qquad \text{where } (\Delta, x) = [\![\boldsymbol{e}]\!]\ ,\ (\Delta_1, x_1) = [\![\boldsymbol{e}_1]\!]\ ,\ (\Delta_2, x_2) = [\![\boldsymbol{e}_2]\!] \\
[\![\mathtt{bind}\, x = \boldsymbol{e}_1\, \mathtt{in}\, \boldsymbol{e}_2]\!] &= ((\Delta_1; x \mapsto x_1; \Delta_2), x_2) && \text{where } (\Delta_1, x_1) = [\![\boldsymbol{e}_1]\!],\ (\Delta_2, x_2) = [\![\boldsymbol{e}_2]\!]
\end{aligned}
$$

Notice that if we remove the rule for bindings (i.e., the very last rule), the remaining rules define a transformation of the terms of the source language into a canonical form.

It is easy to see that $\lceil \mathsf{term}([\![\boldsymbol{e}]\!]) \rceil = \lceil \boldsymbol{e} \rceil$ (or that $\lceil \mathsf{term}([\![e]\!]) \rceil = e$ if e is a term of the source language). Moreover, besides unwindings, this transformation preserves also types: if $\Gamma \vdash_{\mathcal{I}} \boldsymbol{e} : t$, then $\Gamma \vdash_{\mathcal{I}} \mathsf{term}([\![\boldsymbol{e}]\!]_\varepsilon) : t$. These two results prove Proposition A.4.

We can thus use the result of Proposition A.4 to refine the Completeness Theorem 3.2 as follows:

Theorem A.5 (Completeness of Canonical Forms). *If $\Gamma \vdash e : t$ then $\exists \boldsymbol{\kappa}, t'$ such that $\lceil \boldsymbol{\kappa} \rceil = e$, $t' \leq t$, and $\Gamma \vdash_{\mathcal{I}} \boldsymbol{\kappa} : t'$*

This combined with the soundness Theorem 3.1 for intermediate expressions (recall that canonical forms are intermediate expressions) tells us that an expression of the source language is well-typed if and only if it is the unwinding of a well-typed canonical form.

A.8 Maximal Sharing Canonical Forms

The transformation in Section A.7 returns just one of the possible canonical forms that satisfy Proposition A.4, but there are many of them. In order to infer types for the source language, we are interested in the canonical forms that satisfy four particular properties.

Definition A.6 (MSC Forms). *A* maximal sharing canonical form *(abbreviated as* MSC-form*) is (any canonical form α-equivalent to) a canonical form $\boldsymbol{\kappa}$ such that:*

(1) if $\mathtt{bind}\, x_1 = \boldsymbol{a}_1\, \mathtt{in}\, \boldsymbol{\kappa}_1$ and $\mathtt{bind}\, x_2 = \boldsymbol{a}_2\, \mathtt{in}\, \boldsymbol{\kappa}_2$ are distinct sub-expressions of $\boldsymbol{\kappa}$, then $\lceil \boldsymbol{a}_1 \rceil \not\equiv_\alpha \lceil \boldsymbol{a}_2 \rceil$
(2) if $\mathtt{bind}\, x = \boldsymbol{a}\, \mathtt{in}\, \boldsymbol{\kappa}'$ is a sub-expression of $\boldsymbol{\kappa}$, then $\boldsymbol{a}$ is not a variable.
(3) if $\lambda x.\boldsymbol{\kappa}_1$ is a sub-expression of $\boldsymbol{\kappa}$ and $\mathtt{bind}\, y = \boldsymbol{a}\, \mathtt{in}\, \boldsymbol{\kappa}_2$ a sub-expression of $\boldsymbol{\kappa}_1$, then $fv(\boldsymbol{a}) \not\subseteq fv(\lambda x.\boldsymbol{\kappa}_1)$
(4) if $\mathtt{bind}\, x = \boldsymbol{a}\, \mathtt{in}\, \boldsymbol{\kappa}'$ is a sub-expression of $\boldsymbol{\kappa}$, then $x \in fv(\boldsymbol{\kappa}')$.

MSC-forms are defined modulo α-conversion.[9] The first property states that distinct variables denote different (i.e., not α-convertible) expressions of the source language. The second property forbids aliasing. The third property requires that bindings must extrude λ abstractions whenever possible. The fourth condition states that there is no useless bind (the bound variable must occur in the body of the bind).

[9]For instance, both $\lambda x.\mathtt{bind}\, z = x\, y\, \mathtt{in}\, z\, y$ and $\lambda x.\mathtt{bind}\, z = x\, y\, \mathtt{in}\, z$ are two distinct atoms that can occur in the same MSC-form, even though the atom $x\, y$ appears in both: an α-renaming of x makes the first MSC-property hold.

The first two properties ensure the maximal sharing of common sub-expressions in the source language, where *common sub-expressions* designate sets composed by different occurrences of sub-expressions that are equal (in our case, α-convertible). In other terms if we start from a source language term and we put it into a MSC-form, then all common sub-expressions occurring in it will be bound by the same variable. For instance, if we start from the term $(f3, f3)$, then its MSC-form will be (α-equivalent to) $\mathtt{bind}\, x = 3\, \mathtt{in}\, \mathtt{bind}\, y = fx\, \mathtt{in}\, \mathtt{bind}\, z = (y, y)\, \mathtt{in}\, z$: both occurrences of $f3$ are bound to y. [10]

The first three properties of Definition A.6 are important since they ensure that an expression of the source language is typable *if and only if* it is the unwinding of a typable MSC-form. For the first two properties, this is because reducing the bindings in an intermediate expression—while preserving unwinding—increases the typeability of a term: if we can type an intermediate term in which two distinct variables bind the same sub-expression, then the same term in which this sub-expression is bound by a single variable can also be typed by assigning to the unique variable the intersection of the types of the distinct variables, but the converse does not hold. For the third property this is because outer bindings may produce better types. For instance, consider the expression $\mathtt{bind}\, x = \boldsymbol{a}\, \mathtt{in}\, \lambda y.\ x$, where $\boldsymbol{a}$ is an expression that can be either an integer or a Boolean. This expression can be typed with $(\mathbb{1} \to \mathsf{Int}) \vee (\mathbb{1} \to \mathsf{Bool})$. However for the expression $\lambda y.\ (\mathtt{bind}\, x = \boldsymbol{a}\, \mathtt{in}\, x)$ which has the same unwinding as the previous one, the most precise type one can deduce is $\mathbb{1} \to (\mathsf{Int} \vee \mathsf{Bool})$, which is strictly larger than $(\mathbb{1} \to \mathsf{Int}) \vee (\mathbb{1} \to \mathsf{Bool})$.

The last property of Definition A.6 is important because it ensures that given a source language expression e there exists a unique (modulo α-conversion and the order of bindings) MSC-form whose unwinding is e (cf. Proposition A.8): we denote this MSC-form by $\mathsf{MSC}(e)$.

An important property of MSC-forms is that given an expression e of the source language, all its MSC-forms (i.e., all MSC-form whose unwinding is e) are the same modulo the order in which their bindings appear. Formally, we define the following congruence on canonical forms:

Definition A.7 (Canonical equivalence). *We denote by $\equiv_\kappa$ the smallest congruence on canonical forms that is closed by α-conversion and such that*

$$\mathtt{bind}\, x_1 = \boldsymbol{a}_1\, \mathtt{in}\, \mathtt{bind}\, x_2 = \boldsymbol{a}_2\, \mathtt{in}\, \boldsymbol{\kappa} \ \equiv_\kappa \ \mathtt{bind}\, x_2 = \boldsymbol{a}_2\, \mathtt{in}\, \mathtt{bind}\, x_1 = \boldsymbol{a}_1\, \mathtt{in}\, \boldsymbol{\kappa} \qquad x_1 \notin fv(\boldsymbol{a}_2), x_2 \notin fv(\boldsymbol{a}_1) \quad (22)$$

Then we prove that all the MSC forms of a source language expression are equivalent:

Proposition A.8. *If $\boldsymbol{\kappa}_1$ and $\boldsymbol{\kappa}_2$ are two MSC-forms and $\lceil \boldsymbol{\kappa}_1 \rceil \equiv_\alpha \lceil \boldsymbol{\kappa}_2 \rceil$, then $\boldsymbol{\kappa}_1 \equiv_\kappa \boldsymbol{\kappa}_2$.*

It is easy to observe that the canonical equivalence preserves typeability (this is a direct consequence that type environments are mappings in which order does not matter).

It is easy to transform a canonical form into a MSC-form that has the same type and the same unwinding. This can be done by applying the rewriting rules below, that are confluent and normalizing.

[10] Notice that this would not be true if aliasing were allowed: for instance $(f3, f3)$ could be transformed into $\mathtt{bind}\, x = 3\, \mathtt{in}\, \mathtt{bind}\, w = x\, \mathtt{in}\, \mathtt{bind}\, y_1 = fx\, \mathtt{in}\, \mathtt{bind}\, y_2 = fw\, \mathtt{in}\, \mathtt{bind}\, z = (y_1, y_2)\, \mathtt{in}\, z$

$$\begin{array}{rcll}
\begin{array}{l}\mathsf{bind}\, x_1 = \boldsymbol{a}_1 \,\mathsf{in}\\ \mathsf{bind}\, x_2 = \boldsymbol{a}_2 \,\mathsf{in}\, \boldsymbol{\kappa}\end{array} & \dashrightarrow & \mathsf{bind}\, x_1 = \boldsymbol{a}_1 \,\mathsf{in}\, \boldsymbol{\kappa}\{x_1/x_2\} & \boldsymbol{a}_1 \equiv_\alpha \boldsymbol{a}_2 \quad (23)\\
\mathsf{bind}\, x = \boldsymbol{a} \,\mathsf{in}\, \boldsymbol{\kappa} & \dashrightarrow & \boldsymbol{\kappa} & x \notin \mathsf{fv}(\boldsymbol{\kappa}) \quad (24)\\
\lambda x.(\mathsf{bind}\, y = x \,\mathsf{in}\, \boldsymbol{\kappa}) & \dashrightarrow & \lambda x.\boldsymbol{\kappa}\{x/y\} & \quad (25)\\
\begin{array}{l}\mathsf{bind}\, x = \boldsymbol{a} \,\mathsf{in}\\ \mathsf{bind}\, y = x \,\mathsf{in}\, \boldsymbol{\kappa}\end{array} & \dashrightarrow & \mathsf{bind}\, x = \boldsymbol{a} \,\mathsf{in}\, \boldsymbol{\kappa}\{x/y\} & \quad (26)\\
\begin{array}{l}\mathsf{bind}\, x = \lambda y.(\\ \quad \mathsf{bind}\, z = \boldsymbol{a} \,\mathsf{in}\, \boldsymbol{\kappa}_\circ)\\ \mathsf{in}\, \boldsymbol{\kappa}\end{array} & \dashrightarrow & \begin{array}{l}\mathsf{bind}\, z = \boldsymbol{a} \,\mathsf{in}\\ \mathsf{bind}\, x = \lambda y.\boldsymbol{\kappa}_\circ \,\mathsf{in}\, \boldsymbol{\kappa}\end{array} & y \notin \mathsf{fv}(\boldsymbol{a}), z \notin \mathsf{fv}(\boldsymbol{\kappa}) \quad (27)
\end{array}$$

$$\boldsymbol{\kappa}_1 \quad \dashrightarrow_\kappa \quad \boldsymbol{\kappa}_2 \qquad\qquad \exists \boldsymbol{\kappa}_1'.\ \boldsymbol{\kappa}_1 \equiv_\kappa \boldsymbol{\kappa}_1' \dashrightarrow \boldsymbol{\kappa}_2 \qquad (28)$$

Rule (23) implements the maximal sharing: if two variables bind atoms with the same unwinding (modulo α-conversion), then the variables are unified. Rule (24) removes useless bindings while (25) and (26) removes aliases. Rule (27) extrudes bindings from abstractions of variables that do not occur in the argument of the binding. Rule (28) applies the previous rule modulo the canonical equivalence: in practice it applies the swap of binding defined in (22) as many times as it is needed to apply one of the other rules. As customary, these rules can be applied under any context.

Since the transformation above transforms every well-typed canonical form into an MSC-form that has the same type (or a more precise one) and the same unwinding, the completeness theorem of canonical forms already holds for MSC-form. The theorem can thus be stated as follows:

Theorem A.9 (Completeness of MSC-Forms). *If $\vdash e : t$ then $\exists \boldsymbol{\kappa}, t'$ such that $\boldsymbol{\kappa}$ is a maximal sharing canonical form, $\lceil \boldsymbol{\kappa} \rceil \equiv_\alpha e$, $t' \leq t$, and $\vdash_{\mathcal{I}} \boldsymbol{\kappa} : t'$*

Notice that now we used α-conversion instead of equality, since e may contain α-equivalent but not equal subterms that the MSC-form $\boldsymbol{\kappa}$ would of course unify.

Putting it All Together. The corollary of these propositions is that an expression e is typable if and only if its unique (modulo $\equiv_\kappa$) MSC-form is typable, too. More formally, given an expressions e of the source language, let us denote by $\mathsf{MSC}(e)$ any element of the set $\{\boldsymbol{\kappa} \mid e \equiv_\alpha \lceil \boldsymbol{\kappa} \rceil$ and $\boldsymbol{\kappa}$ is a MSC-form$\}$ that is, the unique (modulo $\equiv_\kappa$) MSC-form of e. Then we have

Corollary A.10 (Soundness and Completeness). *For every closed term e of the source language*

$$\begin{array}{rcll}
\vdash e : t & \Rightarrow & \vdash_{\mathcal{I}} \mathsf{MSC}(e) : t' \leq t & \textit{(completeness)}\\
\vdash e : t & \Leftarrow & \vdash_{\mathcal{I}} \mathsf{MSC}(e) : t & \textit{(soundness)}
\end{array}$$

Finally, it is straightforward to generate a particular MSC-form for a closed source language expression e: simply apply the rewriting rules in (23)–(28) to term$[\![e]\!]$. Corollary A.10 states that this MSC-form is typable if and only if e is: we reduced the problem of typing e to the one of typing a MSC-form of e, form that we can effectively produce from e and for which we have a syntax-directed type system.

A.9 Algorithmic Typing Rules

$$[\text{Const-Alg}]\ \frac{}{\Gamma \vdash_{\mathscr{A}} c : \boldsymbol{b_c}} \qquad [\text{Ax-Alg}]\ \frac{}{\Gamma \vdash_{\mathscr{A}} x : \Gamma(x)}\ x \in \mathsf{dom}(\Gamma)$$

$$[\to\text{I-Alg}]\ \frac{(\forall j \in J) \qquad \Gamma, x : t_j \vdash_{\mathscr{A}} \kappa : s_j}{\Gamma \vdash_{\mathscr{A}} \lambda x{:}\{\Gamma_i \triangleright t_i\}_{i\in I}.\kappa : \bigwedge_{j\in J} t_j \to s_j}\ J = \{i \in I \mid \Gamma \leq \Gamma_i\} \neq \varnothing$$

$$[\to\text{E-Alg}]\ \frac{\Gamma \vdash_{\mathscr{A}} x_1 : t_1 \quad \Gamma \vdash_{\mathscr{A}} x_2 : t_2}{\Gamma \vdash_{\mathscr{A}} x_1 x_2 : t_1 \circ t_2}\ \begin{array}{l} t_1 \leq \mathbb{0} \to \mathbb{1} \\ t_2 \leq \mathsf{dom}(t_1) \end{array}$$

$$[\times\text{I-Alg}]\ \frac{\Gamma \vdash_{\mathscr{A}} x_1 : t_1 \qquad \Gamma \vdash_{\mathscr{A}} x_2 : t_2}{\Gamma \vdash_{\mathscr{A}} (x_1, x_2) : t_1 \times t_2}$$

$$[\times\text{E}_1\text{-Alg}]\ \frac{\Gamma \vdash_{\mathscr{A}} x : t \leq (\mathbb{1} \times \mathbb{1})}{\Gamma \vdash_{\mathscr{A}} \pi_1 x : \pi_1(t)} \qquad [\times\text{E}_2\text{-Alg}]\ \frac{\Gamma \vdash_{\mathscr{A}} x : t \leq (\mathbb{1} \times \mathbb{1})}{\Gamma \vdash_{\mathscr{A}} \pi_2 x : \pi_2(t)} \qquad [\mathbb{0}\text{-Alg}]\ \frac{\Gamma \vdash_{\mathscr{A}} x : \mathbb{0}}{\Gamma \vdash_{\mathscr{A}} (x{\in}t)\ ?\ x_1 : x_2 : \mathbb{0}}$$

$$[\in_1\text{-Alg}]\ \frac{\Gamma \vdash x : t_0 \leq t \qquad \Gamma \vdash x_1 : t_1}{\Gamma \vdash (x{\in}t)\ ?\ x_1 : x_2 : t_1}\ t_0 \not\simeq \mathbb{0} \qquad [\in_2\text{-Alg}]\ \frac{\Gamma \vdash_{\mathscr{A}} x : t_0 \leq \neg t \qquad \Gamma \vdash x_2 : t_2}{\Gamma \vdash_{\mathscr{A}} (x{\in}t)\ ?\ x_1 : x_2 : t_2}\ t_0 \not\simeq \mathbb{0}$$

$$[\vee_1\text{-Alg}]\ \frac{\Gamma \vdash_{\mathscr{A}} \kappa : s}{\Gamma \vdash_{\mathscr{A}} \mathtt{bind}\, x{:}\{\Gamma_i \triangleright t_i\}_{i\in I} = a\ \mathtt{in}\ \kappa\ : s}\ \begin{array}{l} x \notin \mathsf{dom}(\Gamma) \\ \{i \in I \mid \Gamma \leq \Gamma_i\} = \varnothing \end{array}$$

$$[\vee_2\text{-Alg}]\ \frac{\Gamma \vdash_{\mathscr{A}} a : \bigvee_{j\in J} t_j \qquad (\forall j \in J) \qquad \Gamma, x : t_j \vdash_{\mathscr{A}} \kappa : s_j}{\Gamma \vdash_{\mathscr{A}} \mathtt{bind}\, x{:}\{\Gamma_i \triangleright t_i\}_{i\in I} = a\ \mathtt{in}\ \kappa\ : \bigvee_{j\in J} s_j}\ J = \{i \in I \mid \Gamma \leq \Gamma_i\} \neq \varnothing$$

B ALGORITHM FOR RECONSTRUCTING ANNOTATIONS

In this section we give the complete definition of the algorithm for the reconstruction of annotations together with all the auxiliary operations it uses. We start in Section B.1 with the definitions that concern the refinement of the type environments. In Section B.2 we define the operations that manipulate type environments, annotations and their types, in particular to (1) `partition` a set of types into a set of disjoint types, to (2) manipulate expressions, in particular to `restrict` and `empty` their annotations and to `merge` several expressions that differ only by their annotations and (3) to `extract` and `propagate` the information provided by sets of refinements. Section B.3 present the inference rules that define a single pass of our algorithm.

B.1 Type Environment Refinements

During the annotation reconstruction process, we start from a generic context and generic annotations (initially $\mathbb{1}$) and specialize them when necessary as we progress into the expression. In order to refine an environment, we use the following operator.

Definition B.1 (Refinement of environments). *Let Γ a type environment, x a variable and t a type. We define the refinement $\Gamma[x :\triangleq t]$ as follows:*

$$\Gamma[x :\triangleq t] \stackrel{\text{def}}{=} \begin{cases} (\Gamma \setminus \{x \mapsto \Gamma(x)\}) \cup \{x \mapsto \Gamma(x) \wedge t\} & \text{if } x \in dom(\Gamma) \text{ and } (\Gamma(x) \simeq \mathbb{0} \text{ or } \Gamma(x) \wedge t \not\simeq \mathbb{0}) \\ \text{undefined} & \text{otherwise} \end{cases}$$

Note that this operator is undefined when $x \notin \mathsf{dom}(\Gamma)$: we do not want to consider refinements on variables that are not in the context. It is also undefined when $\Gamma(x) \not\simeq \mathbb{0}$ and $\Gamma(x) \wedge t \simeq \mathbb{0}$: we do not want to consider refinements that require a variable to have an empty type, except if this variable already had an empty type before the refinement.

Necessary Refinements. In a term in canonical form, type-cases test the type of variables bound to atoms. So, morally we are examining expressions of the form $(a \in t)\ ?\ a_1 : a_2$. To precisely type such an expression we need to determine the conditions under which each branch is selected or not. The "conditions" at issue are given as possible refinements of the current type environment. More precisely, given a type environment Γ and an atom a that is typable under the type environment Γ, we want to refine the types of the free variables of a in Γ so that any result of a under this refined context will possibly be of type t.

Rather than a single refinement we will look a finite set of refinements which will be described by a finite set $\{\Gamma_i\}_{i \in I}$ of type environments. Each of these environments Γ_i will be subsumed (in the sense of Definition 4.1) by the initial environment Γ.

In particular, we are interested in refinements that are *necessary* (but may not be sufficient) to ensure that a will produce results of type t. This will allow the system to give a precise typing to the branches of typecase expressions by integrating the information that if the branch was selected, then the type-test failed/succeeded.

More precisely, we define a quaternary relations that takes an atom a, a type t (into which a must reduce), the current type-environment Γ (under which a is typable) and a finite set $\{\Gamma_i\}_{i \in I}$ of type environments subsumed by Γ. We denote this relation by the following judgment (we use the modal symbol $\Box$ to stress that the atom a does not diverge and reduces to a value in t):

$$[\Gamma \vdash \Box(a \rightsquigarrow t)] \ \supset\ \{\Gamma_i\}_{i \in I}$$

meaning that if a must reduce to values of type t (connective $\Box$), then it is *necessary* (connective $\supset$) that *at least one* of the refinements Γ_i of Γ holds.

In particular $[\Gamma \vdash \Box(a \rightsquigarrow t)] \ \supset\ \{\}$ means that it is impossible under the hypothesis Γ that a produces a value of type t; $[\Gamma \vdash \Box(a \rightsquigarrow t)] \ \supset\ \{\Gamma\}$ means that Γ already provides all conditions that

are necessary for a to produce a value of type t. For example, we have: $[\Gamma \vdash \square(42\rightsquigarrow\mathsf{Bool})] \supset \{\}$, $[\Gamma \vdash \square(42\rightsquigarrow\mathsf{Int})] \supset \{\Gamma\}$, and $[x{:}\mathbb{1} \vdash \square((x,x)\rightsquigarrow(\mathsf{Int}\times\mathsf{Int})\vee(\mathsf{Bool}\times\mathsf{Bool}))] \supset \{(x{:}\mathsf{Int}), (x{:}\mathsf{Bool})\}$. The latter states that for (x,x) to reduce to a value of type $(\mathsf{Int}\times\mathsf{Int})\vee(\mathsf{Bool}\times\mathsf{Bool}$ it is necessary that either x is of type Int or x is of type Bool.

The quaternary relation is defined by induction on atoms as follows:

$$[\Gamma \vdash \square(c\rightsquigarrow t)] \supset \{\} \qquad \boldsymbol{b}_c \wedge t \simeq \mathbb{0} \tag{29}$$

$$[\Gamma \vdash \square(c\rightsquigarrow t)] \supset \{\Gamma\} \qquad \boldsymbol{b}_c \wedge t \not\simeq \mathbb{0} \tag{30}$$

$$[\Gamma \vdash \square(x_1\,x_2\rightsquigarrow t)] \supset \{\Gamma[x_1 :\hat{=} t_i][x_2 :\hat{=} t_i \blacksquare t] \mid i \in I\} \quad \Gamma(x_1) \overset{\text{DNF}}{\cong} \bigvee_{i\in I} t_i \tag{31}$$

$$[\Gamma \vdash \square(\lambda x.\kappa\rightsquigarrow t)] \supset \{\} \qquad (\mathbb{0}\to\mathbb{1}) \wedge t \simeq \mathbb{0} \tag{32}$$

$$[\Gamma \vdash \square(\lambda x.\kappa\rightsquigarrow t)] \supset \{\Gamma\} \qquad (\mathbb{0}\to\mathbb{1}) \wedge t \not\simeq \mathbb{0} \tag{33}$$

$$[\Gamma \vdash \square(\pi_1 x\rightsquigarrow t)] \supset \{\Gamma[x :\hat{=} t\times\mathbb{1}]\} \tag{34}$$

$$[\Gamma \vdash \square(\pi_2 x\rightsquigarrow t)] \supset \{\Gamma[x :\hat{=} \mathbb{1}\times t]\} \tag{35}$$

$$[\Gamma \vdash \square((x_1,x_2)\rightsquigarrow \textstyle\bigvee_{i\in I}(t_i\times s_i))] \supset \{\Gamma[x_1 :\hat{=} t_i][x_2 :\hat{=} s_i] \mid i \in I\} \tag{36}$$

$$[\Gamma \vdash \square((x{\in}\tau)\,?\,x_1 : x_2\rightsquigarrow t)] \supset \{\Gamma[x_1 :\hat{=} t][x :\hat{=} \tau]\,,\ \Gamma[x_2 :\hat{=} t][x :\hat{=} \neg\tau]\} \tag{37}$$

with the convention that the sets on the right-hand side of the relations contain only the type-environments for which the operations are defined. So for instance in (34) if $(t\times\mathbb{1}) \wedge \Gamma(x) \simeq \mathbb{0}$, then $\Gamma[x :\hat{=} t\times\mathbb{1}]$ is undefined and therefore $[\Gamma \vdash \square(\pi_1 x\rightsquigarrow t)] \supset \{\}$ holds.

Let us explain the rules for each atom. If the atom is a constant c then (29) states that it is impossible that the constant produces a result of type t if $\boldsymbol{b}_c \wedge t \simeq \mathbb{0}$; if instead $\boldsymbol{b}_c \wedge t \not\simeq \mathbb{0}$, then (30) states that Γ does not need to be refined (actually, it cannot be refined since the atom c has no free variables to refine) to ensure that c may produce such a result.

The case (31) for the application of a function x_1 of type $\bigvee_{i\in I} t_i$ to an argument x_2 is the most interesting one and needs detailed explanation. In short, rule (31) states that if the application must produce a result of type t, then there must exist $i \in I$ such that the function is of type t_i, t_i is a functional type (i.e., a subtype of $\mathbb{0}\to\mathbb{1}$), and the argument has type $t_i \blacksquare t$ which, by definition, ensures the property. Let us explain each single bit. First of all, the rule states $\Gamma(x_1) \overset{\text{DNF}}{\cong} \bigvee_{i\in I} t_i$. This means that we take the type $\Gamma(x_1)$ of x_1 and we transform it in its *disjunctive normal form* as defined by Frisch et al. [2008, Section 6.1]. This is a union of intersections of literals of the same form. A literal is an atomic type or its negation. An atomic type (and, thus, literals) has three possible forms: it is either a basic type or an arrow type or a product type. For instance, if t is a function type, that is, $t \le \mathbb{0}\to\mathbb{1}$, then it is equivalent to a union of intersections of arrows and their negations: $t \overset{\text{DNF}}{\cong} \bigvee_{i\in I}(\bigwedge_{p\in P_i}(s_p \to t_p) \wedge \bigwedge_{n\in N_i}\neg(s'_n \to t'_n))$ for some P_i's and N_i's, a property we used in Appendix A.4. Also in Appendix A.4 there is the definition of $t_i \blacksquare t$ which is the largest type we can give to an argument of a function of type t_i so that the application may yield a result of type t, which is exactly what we need here. Also notice that $t_i \blacksquare t$ is defined only for $t_i \le \mathbb{0}\to\mathbb{1}$, which means that a refinement will be produced only for those t_i of the disjunctive normal form of $\Gamma(x_1)$ that are functional types. Finally, disjunctive normal forms are not unique but the best results for our algorithm are obtained when the disjunctive normal forms for products are formed by disjoint sets of minimum cardinality (e.g., $(\mathsf{Int}, \mathsf{Int}\vee\mathsf{Bool}) \vee (\mathsf{Int}, \mathsf{Int}\vee\mathsf{String})$ will be decomposed as $(\mathsf{Int}, \mathsf{Int}\vee\mathsf{Bool}\vee\mathsf{String})$ rather than as $(\mathsf{Int}, \mathsf{Int}) \vee (\mathsf{Int}, \mathsf{Bool}) \vee (\mathsf{Int}, \mathsf{String})$) while soundness of our algorithm requires that the disjunctive normal form for arrows has minimum cardinality (obviously they cannot be disjoint unions, since $\mathbb{1}\to\mathbb{0}$ is in the intersection of any pair of arrows). In practice in our implementation we will use the result of the `normalize` function provided by the CDuce API for types.

The cases for λ-abstraction are just rough approximations since we do not try to refine the type of the variables that are free in the body of a function to determine the type of that function.[11] As a consequence, the treatment of λ-abstractions is similar to the one for constants. In particular, (33) states that if t contains some functions, then we do not need to do anything to ensures that the λ-abstraction may be of type t.

The other cases are straightforward. For a projection to yield a result of a certain type the projected expression must be of the corresponding product types (34-35); for a pair to yield a value in a union of products, it must yield a value in at least one of the summands of the union; finally, a type-case will yield a result in t if and only if the branch that is selected does it.

B.2 Auxiliary Definitions

The rules in the next section use several auxiliary functions, some of which where already introduced and more or less formally described in Section 5. We recall all of them with their definitions.

partition$(\{t_i\}_{i\in I})$ is the smallest (in terms of cardinality) non empty set of types $\{s_j\}_{j\in J}$ such that (i) $\bigvee_{j\in J} s_j \simeq \bigvee_{i\in I} t_i$, (ii) $\forall j \in J.\, \forall j' \in J.\, j \neq j' \Rightarrow s_j \wedge s_{j'} \simeq \mathbb{0}$, and (iii) $\forall j \in J.\, \forall i \in I.\, s_j \leq t_i$ or $s_j \wedge t_i \simeq \mathbb{0}$. Notice that since `partition` must return a non-empty set, then for $\bigvee_{i\in I} t_i \simeq \mathbb{0}$ we have $\texttt{partition}(\{t_i\}_{i\in I}) = \{\mathbb{0}\}$.

empty(φ) (where φ, we recall, denotes either an algorithmic atom a or an algorithmic expression κ) replaces all the annotations in φ by the empty annotation $\{\}$.

merge$_\varphi(\{\varphi_i\}_{i\in I})$ is defined when all φ_i are the same except for their annotations (i.e., they all have the same erasure $\langle\varphi_i\rangle$) and produces a new annotated expression that concatenates all these annotations. If $I = \varnothing$, then it returns $\texttt{empty}(\varphi)$.

propagate$_{x,a,t}(\mathbb{\Gamma})$ propagates to the types of the free variables of a any refinement of t specified in the typings of x in the environments in $\mathbb{\Gamma}$. Essentially it applies $[\Gamma \vdash \square(a\!\rightsquigarrow\!\Gamma(x))] \supset \mathbb{\Gamma}'$ for each $\Gamma \in \mathbb{\Gamma}$ for which a refinement must be propagated. It is defined as:

$$\texttt{propagate}_{x,a,t}(\{\Gamma_i\}_{i\in I}) \stackrel{\text{def}}{=} \bigcup_{i\in I} \mathbb{\Gamma}_i \quad \text{with } \forall i \in I.\ \begin{cases} \mathbb{\Gamma}_i = \{\Gamma_i\} & \text{if } t \leq \Gamma_i(x) \\ [\Gamma_i \vdash \square(a\!\rightsquigarrow\!\Gamma_i(x))] \supset \mathbb{\Gamma}_i & \text{otherwise} \end{cases}.$$

extract$_x(\mathbb{\Gamma})$ extracts from $\mathbb{\Gamma}$ all the hypotheses about x to create a new annotation that it returns with the set of type environments from which these hypotheses were removed, that is, $\texttt{extract}_x(\mathbb{\Gamma}) \stackrel{\text{def}}{=} (\{(\Gamma\!\setminus\!x) \triangleright \Gamma(x) \mid \Gamma \in \mathbb{\Gamma}\}, \{\Gamma\!\setminus\!x \mid \Gamma \in \mathbb{\Gamma}\})$ where $\Gamma\!\setminus\!x \stackrel{\text{def}}{=} \Gamma \setminus \{x \mapsto \Gamma(x)\}$.

($\Gamma\triangleright A$**)** denotes the set of the types of the annotation A that are compatible with (i.e., whose hypotheses subsume) Γ, that is, $(\Gamma\triangleright A) \stackrel{\text{def}}{=} \{t \mid \Gamma'\triangleright t \in A \text{ and } \Gamma \leq \Gamma'\}$. We use $\bigvee(\Gamma\triangleright A)$ to denote the union of these types.

restrict$_\Gamma(A)$ refines all the type environments in the annotation A with the hypotheses in Γ, that is $\texttt{restrict}_\Gamma(A) \stackrel{\text{def}}{=} \{(\Gamma \wedge \Gamma')\triangleright t \mid \Gamma'\triangleright t \in A\}$ where $\Gamma \wedge \Gamma'$ denotes the pointwise intersection of two type environments with possibly distinct domains, which is formally defined as:

$$(\Gamma \wedge \Gamma')(x) \stackrel{\text{def}}{=} \begin{cases} \Gamma(x) & \text{if } x \in \mathrm{dom}(\Gamma) \setminus \mathrm{dom}(\Gamma') \\ \Gamma'(x) & \text{if } x \in \mathrm{dom}(\Gamma') \setminus \mathrm{dom}(\Gamma) \\ \Gamma(x) \wedge \Gamma'(x) & \text{if } x \in \mathrm{dom}(\Gamma) \cap \mathrm{dom}(\Gamma') \\ \text{undefined} & \text{otherwise} \end{cases}$$

restrict$_\Gamma(\varphi)$ replaces every annotation A in φ by $\texttt{restrict}_\Gamma(A)$.

We have now all the notions to formally define the inference rules of our algorithm.

[11] As a matter of fact, it is possible to handle this case more precisely, but for the sake of simplicity we do not do it here.

B.3 Annotations Reconstruction Rules

The rules below use the convention that the sets on the right-hand side of the conclusion contain only the type-environments for which the operations are defined. In particular, only the environment refinements $\Gamma[x :\hat{=} t]$ for which $x \in \mathsf{dom}(\Gamma)$ and ($\Gamma(x) \simeq \mathbb{0}$ or $\Gamma(x) \wedge t \not\simeq \mathbb{0}$) are considered. This in particular means that the set notation $\{\Gamma[x :\hat{=} t_i]\}_{i\in I}$ used in the rules must be considered as a shorthand for $\{\Gamma_i \mid i \in I, \Gamma_i = \Gamma[x :\hat{=} t_i], \Gamma_i(x) \not\simeq \mathbb{0}\}$. We list all the rules below and comment them next.

$$[\textsc{Const}]\ \frac{\boldsymbol{b}_c \leq t}{\Gamma \vdash_{\mathcal{R}} c : t \Rightarrow (c, \{\Gamma\})} \qquad [\textsc{ConstUntypable}]\ \frac{\boldsymbol{b}_c \not\leq t}{\Gamma \vdash_{\mathcal{R}} c : t \Rightarrow (c, \{\})}$$

$$[\textsc{ProjEmpty}]\ \frac{\Gamma(x) \simeq \mathbb{0}}{\Gamma \vdash_{\mathcal{R}} \pi_i x : t \Rightarrow (\pi_i x, \{\Gamma\})}$$

$$[\textsc{Proj}_1]\ \frac{\Gamma(x) \wedge (t \times \mathbb{1}) \overset{\text{DNF}}{\cong} \bigvee_{i\in I} t_i \times s_i}{\Gamma \vdash_{\mathcal{R}} \pi_1 x : t \Rightarrow (\pi_1 x, \{\Gamma[x :\hat{=} t_i \times s_i]\}_{i\in I})} \quad [\textsc{Proj}_2]\ \frac{\Gamma(x) \wedge (\mathbb{1} \times t) \overset{\text{DNF}}{\cong} \bigvee_{i\in I} t_i \times s_i}{\Gamma \vdash_{\mathcal{R}} \pi_2 x : t \Rightarrow (\pi_2 x, \{\Gamma[x :\hat{=} t_i \times s_i]\}_{i\in I})}$$

$$[\textsc{PairEmpty}]\ \frac{\Gamma(x_1) \times \Gamma(x_2) \simeq \mathbb{0}}{\Gamma \vdash_{\mathcal{R}} (x_1, x_2) : t \Rightarrow ((x_1, x_2), \{\Gamma\})}$$

$$[\textsc{Pair}]\ \frac{t \wedge (\mathbb{1} \times \mathbb{1}) \overset{\text{DNF}}{\cong} \bigvee_{i\in I} t_i \times s_i}{\Gamma \vdash_{\mathcal{R}} (x_1, x_2) : t \Rightarrow ((x_1, x_2), \{\Gamma[x_1 :\hat{=} t_i][x_2 :\hat{=} s_i]\}_{i\in I})}$$

$$[\textsc{CaseEmpty}]\ \frac{\Gamma(x) \simeq \mathbb{0}}{\Gamma \vdash_{\mathcal{R}} (x{\in}t)\,?\,x_1 : x_2 : t \Rightarrow ((x{\in}t)\,?\,x_1 : x_2, \{\Gamma\})}$$

$$[\textsc{Case}]\ \frac{}{\Gamma \vdash_{\mathcal{R}} (x{\in}s)\,?\,x_1 : x_2 : t \Rightarrow ((x{\in}s)\,?\,x_1 : x_2, \{\Gamma[x :\hat{=} s][x_1 :\hat{=} t], \Gamma[x :\hat{=} \neg s][x_2 :\hat{=} t]\})}$$

$$[\textsc{AppREmpty}]\ \frac{\Gamma(x_2) \simeq \mathbb{0} \qquad \Gamma(x_1) \leq \mathbb{0} \to \mathbb{1}}{\Gamma \vdash_{\mathcal{R}} x_1 x_2 : t \Rightarrow (x_1 x_2, \{\Gamma\})} \qquad [\textsc{AppLEmpty}]\ \frac{\Gamma(x_1) \simeq \mathbb{0} \qquad x_2 \in \mathsf{dom}(\Gamma)}{\Gamma \vdash_{\mathcal{R}} x_1 x_2 : t \Rightarrow (x_1 x_2, \{\Gamma\})}$$

$$[\textsc{AppR}]\ \frac{\Gamma(x_1) \overset{\text{DNF}}{\cong} \bigwedge_{i\in I}(s_i \to t_i) \wedge \bigwedge_{j\in J}(\neg(s'_j \to t'_j))}{\Gamma \vdash_{\mathcal{R}} x_1 x_2 : t \Rightarrow (x_1 x_2, \{\Gamma[x_1 :\hat{=} (s_i \wedge \Gamma(x_2)) \to t][x_2 :\hat{=} s_i]\}_{i\in I})}$$

$$[\textsc{AppL}]\ \frac{\Gamma(x_1) \wedge (\mathbb{0} \to \mathbb{1}) \overset{\text{DNF}}{\cong} \bigvee_{i\in I} s_i \qquad x_2 \in \mathsf{dom}(\Gamma)}{\Gamma \vdash_{\mathcal{R}} x_1 x_2 : t \Rightarrow (x_1 x_2, \{\Gamma[x_1 :\hat{=} s_i]\}_{i\in I})}$$

$$[\textsc{Abs}]\ \frac{\begin{array}{c} t \overset{\text{DNF}}{\cong} \bigwedge_{j\in J}(s_j \to t_j) \qquad (\Gamma{\triangleright}A) \neq \{\} \qquad \bigvee_{j\in J} s_j \leq \bigvee(\Gamma{\triangleright}A) \\ \{s_i\}_{i\in I} = \mathtt{partition}((\Gamma{\triangleright}A) \cup \{s_j \mid j \in J\}) \qquad \forall i \in I.\, \Gamma, (x : s_i) \vdash_{\mathcal{R}} \kappa : t \circ_{\mathbb{1}} s_i \Rightarrow (\kappa_i, \mathbb{\Gamma}_i) \\ \forall i \in I.\, (A_i, \mathbb{\Gamma}'_i) = \mathtt{extract}_x(\mathbb{\Gamma}_i) \qquad A' = \bigcup_{i\in I} A_i \qquad \bigvee_{j\in J} s_j \leq \bigvee\{s' \mid (\Gamma'{\triangleright}s') \in A'\} \end{array}}{\Gamma \vdash_{\mathcal{R}} \lambda x{:}A.\kappa : t \Rightarrow (\lambda x{:}A'.\, \mathtt{merge}_\kappa(\{\kappa_i\}_{i\in I}), \bigcup_{i\in I} \mathbb{\Gamma}'_i)}$$

$$[\textsc{AbsUntypable}]\ \frac{}{\Gamma \vdash_{\mathcal{R}} \lambda x{:}A.\kappa : t \Rightarrow (\lambda x{:}\{\}.\mathtt{empty}(\kappa), \{\})}$$

$$[\textsc{UndefinedVar}]\ \frac{}{\Gamma \vdash_{\mathcal{R}} a : t \Rightarrow (a, \{\})}$$

$$[\textsc{BindArgSkip}]\ \frac{\Gamma \triangleright A = \{\} \qquad \Gamma \vdash_{\mathcal{R}} \kappa : t \Rightarrow (\kappa', \mathbb{\Gamma})}{\Gamma \vdash_{\mathcal{R}} \mathtt{bind}\, x{:}A = a\, \mathtt{in}\, \kappa\ : t \Rightarrow (\mathtt{bind}\, x{:}\{\} = \mathtt{empty}(a)\, \mathtt{in}\, \kappa', \mathbb{\Gamma})}$$

$$[\textsc{BindArgUntyp}]\ \frac{\Gamma \vdash_{\mathcal{R}} a : \bigvee(\Gamma \triangleright A) \Rightarrow (a', \{\}) \qquad \Gamma \vdash_{\mathcal{R}} \kappa : t \Rightarrow (\kappa', \mathbb{\Gamma})}{\Gamma \vdash_{\mathcal{R}} \mathtt{bind}\, x{:}A = a\, \mathtt{in}\, \kappa\ : t \Rightarrow (\mathtt{bind}\, x{:}\{\} = a'\, \mathtt{in}\, \kappa', \mathbb{\Gamma})}$$

$$[\textsc{BindArgRefEnv}]\ \frac{\begin{array}{c}\Gamma \vdash_{\mathcal{R}} a : \bigvee(\Gamma \triangleright A) \Rightarrow (a', \mathbb{\Gamma}) \\ \kappa' = \mathtt{restrict}_{\Gamma}(\kappa) \qquad A' = \mathtt{restrict}_{\Gamma}(A)\end{array}}{\Gamma \vdash_{\mathcal{R}} \mathtt{bind}\, x{:}A = a\, \mathtt{in}\, \kappa\ : t \Rightarrow (\mathtt{bind}\, x{:}A' = a'\, \mathtt{in}\, \kappa', \mathbb{\Gamma} \cup \{\Gamma\})}\ \mathbb{\Gamma} \neq \{\Gamma\}$$

$$[\textsc{BindArgRefAnns}]\ \frac{\Gamma \vdash_{\mathcal{R}} a : \bigvee(\Gamma \triangleright A) \Rightarrow (a', \{\Gamma\}) \qquad \Gamma \vdash_{\mathcal{R}} \mathtt{bind}\, x{:}A = a'\, \mathtt{in}\, \kappa\ : t \Rightarrow (\kappa', \mathbb{\Gamma})}{\Gamma \vdash_{\mathcal{R}} \mathtt{bind}\, x{:}A = a\, \mathtt{in}\, \kappa\ : t \Rightarrow (\kappa', \mathbb{\Gamma})}\ a' \neq a$$

$$[\textsc{Bind}]\ \frac{\begin{array}{c}\Gamma \vdash_{\mathcal{R}} a : \bigvee(\Gamma \triangleright A) \Rightarrow (a, \{\Gamma\}) \\ \Gamma \vdash_{\mathcal{A}} a : s \qquad \{s_i\}_{i \in I} = \mathtt{partition}(\{s \wedge u \mid u \in (\Gamma \triangleright A)\}) \qquad (\forall i \in I) \\ \Gamma, (x : s_i) \vdash_{\mathcal{R}} \kappa : t \Rightarrow (\kappa_i, \mathbb{\Gamma}_i) \qquad \mathbb{\Gamma}'_i = \mathtt{propagate}_{x,a,s_i}(\mathbb{\Gamma}_i) \qquad (A_i, \mathbb{\Gamma}''_i) = \mathtt{extract}_x(\mathbb{\Gamma}'_i)\end{array}}{\Gamma \vdash_{\mathcal{R}} \mathtt{bind}\, x{:}A = a\, \mathtt{in}\, \kappa\ : t \Rightarrow (\mathtt{bind}\, x{:}\bigcup_{i \in I} A_i = a'\, \mathtt{in}\, \mathtt{merge}_{\kappa}(\{\kappa_i\}_{i \in I}), \bigcup_{i \in I} \mathbb{\Gamma}''_i)}$$

$$[\textsc{Var}]\ \frac{}{\Gamma \vdash_{\mathcal{R}} x : t \Rightarrow (x, \{\Gamma[x :\hat{=} t]\})}$$

The rules above are listed in priority order, meaning that a rule applies only if no other previous rule does.

In Section 5 we said that we omitted the rules for empty types. A first example of such rules is the rule [ProjEmpty] that states that when x is of type $\mathbb{0}$ (i.e., the variable is bound to an expression that diverges), then the atom $\pi_i x$ is well-typed (since by subsumption it has type $t \times \mathbb{1}$ and $\mathbb{1} \times t$, that can be used for each specific π_i).

The rules [Proj$_i$] are as in Section 5 with the only difference that instead of $\simeq$ they use the relation $\overset{\text{DNF}}{\cong}$ we defined in Appendix B.1. The reason is that we want a deterministic algorithm and therefore these rules simply apply to the types on the left-hand side the normalization algorithm by Frisch et al. [2008] yielding the type on the right-hand side.

The rule [PairEmpty] follows the same logic as [ProjEmpty], where $\Gamma(x_1) \times \Gamma(x_2) \simeq \mathbb{0}$ is just a notational trick to state that either $\Gamma(x_1) \simeq \mathbb{0}$ or $\Gamma(x_2) \simeq \mathbb{0}$.

The rule [Pair] states that for a pair to have a type t, it must inhabit the product part of t, that is $t \wedge (\mathbb{1} \times \mathbb{1})$. The rule then performs the decomposition of this part in its disjunctive normal form.

The [CaseEmpty] states that if in type-case expression the tested expression diverges, then the expression is well typed. The rule [Case] was explained in Section 5.

The rules [AppLEmpty] and [AppREmpty] reflect the use of our left to right evaluation strategy: if x_1 diverges then the application is well typed provided x_2 is defined; if x_2 diverges then the application is well typed provided x_1 has a functional type and thus, implicitly, it already converged to a λ-abstraction.

The rule [AppR] is as the one presented and explained in Section 5 apart from two details. First, as for the other rules, instead of checking the equivalence $\simeq$, we use $\overset{\text{DNF}}{\simeq}$ which transforms the type of the function into its disjunctive normal form. Second, even though this has no consequence on the conclusion of the rule, we stress that this transformation can make some negated arrow types appear. We omitted this detail in the main presentation because to see that this is possible one needs to examine the details of the definition of `partition`, that in the rule [Abs] is used to partition the domain of the function. If we have a function whose parameter is annotated with some functional type, say, Int→Int and this parameter was initially given type $\mathbb{1}$, then `partition` will produce for these two types the set $\{(\mathsf{Int} \to \mathsf{Int}), \neg(\mathsf{Int} \to \mathsf{Int})\}$ which contains a negated arrow. The presence of negated arrows becomes important for the rules [Abs] and [AbsUntypable].

We explained the rule [Abs] in Section 5. However the rule presented there was a simplified version. Let us pinpoint the differences. As customary, rather than checking the equivalence $\simeq$, we use $\overset{\text{DNF}}{\simeq}$ which transforms the checked type t into its disjunctive normal form. Notice, however, that the rule applies only if the disjunctive normal form does not contain any negated arrow type. Indeed, for a given λ-abstraction there is no way to ensure that it will have a specific negated arrow type (this is possible in CDuce since λ-abstractions are explicitly annotated, but here in general we have no annotation in the source language to enforce it). So in case there are any negated arrow types, the type constraint t must be considered not satisfiable and this case is handled by the rule [AbsUntypable]. The rule [Abs] above uses the operator $t \circ_{\mathbb{1}} s_i$ given in Appendix A.4 whereas the rule in Section 5 used $t \circ s_i$. The former is defined as $t \circ s_i$ but it returns $\mathbb{1}$ when $s_i \not\leq \mathsf{dom}(t)$. This forces the system to check whether it is possible to type the function under the hypothesis that $x : s_i$ even if s_i is not in the *current* domain that was deduced for the function. The reason is that we are determining this domain: at the beginning all we know about a function is that, if it is well typed, then it will be of type $\mathbb{0} \to \mathbb{1}$. Clearly we do not want to test for the function only the $\mathbb{0}$ domain, but also the domains suggested by the current annotation for x (initially $\mathbb{1}$). The annotation A' produced will retain only those for which the test will have succeeded. Still in the rule [Abs], the additional checks $(\Gamma \triangleright A) \neq \{\}$ and $\bigvee_{j\in J} s_j \leq \bigvee(\Gamma \triangleright A)$ absent in the version of Section 5 are there to ensure that the algorithm will only refine the initial annotations and not enlarge them (this is needed for the—conjectured—termination of the algorithm). The last condition added, namely, $\bigvee_{j\in J} s_j \leq \bigvee\{s' \mid (\Gamma' \triangleright s') \in A'\}$, is a necessary (but far from sufficient) condition to ensure that the annotated λ-abstraction produced by the pass has type t: if all the types in the produced annotation A' (independently from their guards) do not cover $\mathsf{dom}(t)$ (i.e., $\bigvee_{j\in J} s_j$) then there is no way by which a lambda abstraction of the form $\lambda x{:}A'.\kappa$ could have type t.

If any of the conditions added in the rule [Abs] fail, or if the checked type t has any negated arrow type, then there is no way that $\lambda x{:}A.\kappa$ can be given type t and the pass fails. This is done by the rule [AbsUntypable]. Notice that for this rule the returned expression is the initial one with all annotations emptied. This is necessary because even if the typing of this term under Γ failed, it may succeed under different hypotheses and thus the merging of this atom with the successful one should not perturb the latter.

The rule [UndefVar] is the default case for the typing of atoms. It means that if none of the previous rules can be applied (recall that the rules are given in priority order), then the algorithm must return a failure. We called it [UndefVar] since this happens when one of the variables of a is not in $\mathsf{dom}(\Gamma)$.

The rule [UndefVar] concludes the rules for algorithmic atoms. The rules that follow are for algorithmic expressions, that is, bind-expressions and variables. We already explained in detail the rules for bind-expressions in Section 5 where we gave the complete rules with just two simplifications. First, in the rule [BindArgSkip] we omitted to apply the `empty` function to a. As in the case for [AbsUntypable] this must be done in order to avoid to perturb the merge with other

successful annotations. Second in the rule [BindArgRefEnv], when the typing of the argument a needs more refinements, it is not sufficient to forward these refinements to the whole pass, since these refinements may impact the annotations already present in the MSC-form, that are thus refined by applying the `restrict` function.

Finally, the very last rule, [Var] states that in order to ensure that a variable has type t the obvious solution is to refine $\Gamma(x)$ with t. Simply notice that if $\Gamma(x)$ is a subtype of t, then the rule returns $\{\Gamma\}$, that is success.

C EXTENSIONS

In this section we present two extensions of our source language of Section 2, that add let-expressions and records. The former is a minimum requirement for any practical programming language, the latter plays a key role if we want our theory to be applicable to dynamic languages.

C.1 Let Bindings

C.1.1 Declarative Type System. Let bindings can easily be added to the syntax of our language:

$$\textbf{Expressions} \quad e \quad ::= \quad \cdots \mid \texttt{let}\, x = e\, \texttt{in}\, e \tag{38}$$

For the reduction semantics, we just add the following notion of reduction and definition of evaluation context:

$$\texttt{let}\, x = v\, \texttt{in}\, e \quad \rightsquigarrow \quad e\{v/x\}$$

$$\textbf{Evaluation Context} \qquad E ::= \cdots \mid \texttt{let}\, x = E\, \texttt{in}\, e$$

and the typing rule is straightforward:

$$[\textsc{Let}]\ \frac{\Gamma \vdash e_1 : t_1 \qquad \Gamma, (x : t_1) \vdash e_2 : t_2}{\Gamma \vdash \texttt{let}\, x = e_1\, \texttt{in}\, e_2\ : t_2}$$

C.1.2 Intermediate System. We add the same production as in (38) in the grammar for intermediate expressions. The definition of unwinding is then straightforward:

$$\lceil \texttt{let}\, x = e_1\, \texttt{in}\, e_2 \rceil = \texttt{let}\, x = \lceil e_1 \rceil\, \texttt{in}\, \lceil e_2 \rceil$$

The definition of canonical forms instead changes in a more surprising way since we add as atom for let expressions the following canonical form:

$$\textbf{Atomic expr} \quad a \quad ::= \quad \cdots \mid \texttt{let}\, x\, \texttt{in}\, x \tag{39}$$

Surprising as it may be, the intuition is rather simple: to produce the atom for the expression $\texttt{let}\, x = e_1\, \texttt{in}\, e_2$ we must replace each subexpression by a variable which would yield something of the form $\texttt{let}\, x = x_1\, \texttt{in}\, x_2$. It easy to see that since the body of the let-expression is a variable, then the variable x is completely useless. The same expressivity can be obtained by specifying only the other two variables, which yields $\texttt{let}\, x_1\, \texttt{in}\, x_2$ and which explains the definition of the atom for let expressions. To say it into a different way, we proceed as before, and define canonical forms so that every subexpression that is not a variable is isolated in the definition of a `bind` (in this way every such subexpression can be designated by a variable). If we were to proceed as before then we should add to atoms the let expression in which all subexpressions are variables. We then add to the transformation function the following clause to transform the let expressions:

$$\begin{aligned}[\![\texttt{let}\, x = e_1\, \texttt{in}\, e_2]\!] = (\Delta_1; \Delta_2; x_\circ \mapsto \texttt{let}\, x_1\, \texttt{in}\, x_2\, , x_\circ) \\ \text{where } (\Delta_1, x_1) = [\![e_1]\!], (\Delta_2, x_2) = [\![e_2\{x_1/x\}]\!]\end{aligned}$$

yielding the following canonical form for the example expression $\texttt{let}\, x = \lambda y.y\, \texttt{in}\, (x, x)$:

$$\begin{aligned}&\texttt{bind}\, x_1 = \lambda y.y\, \texttt{in} \\ &\texttt{bind}\, x_2 = (x_1, x_1)\, \texttt{in} \\ &\texttt{bind}\, x_\circ = (\texttt{let}\, x_1\, \texttt{in}\, x_2\,)\, \texttt{in}\, x_\circ\end{aligned}$$

The variable x is no longer present in the expression. It is unneeded as it is an alias for the variable x_1.

We do the same for algorithmic expressions, since we do not want to add an annotation in an atom $\texttt{let}\, x_1\, \texttt{in}\, x_2$: such annotations will be directly put on the bind-expressions that bind x_1 and x_2.

C.1.3 Annotation Reconstruction Rules. The extension of the algorithm for reconstruction is straightforward. We add to the clauses of Appendix B.1 the following clause:

$$[\Gamma \vdash \square(\texttt{let}\, x_1\, \texttt{in}\, x_2 \rightsquigarrow t)] \;\supset\; \{\Gamma[x_1 :\hat{=} \mathbb{1}][x_2 :\hat{=} t]\} \tag{40}$$

In a word, the type t of the expression matches the type of x_2, while we also ensure that x_1 is well-typed simply by refining its current type by the top type $\mathbb{1}$.

$$[\textsc{Let}]\ \frac{}{\Gamma \vdash_{\mathcal{R}} \texttt{let}\, x_1\, \texttt{in}\, x_2 \;:\; t \Rightarrow (\texttt{let}\, x_1\, \texttt{in}\, x_2\,, \Gamma[x_1 :\hat{=} \mathbb{1}][x_2 :\hat{=} t])}$$

The [Let] rule that defines the algorithm pass for the new atom we added matches the refinement rule: x_1 must be well-typed, while the type of x_2 refines to the type of the entire expression.

C.2 Records

In languages such as JavaScript, the fundamental object type is implemented as an extensible record. Record expressions are sometimes an afterthought in the definition of a calculus, as their semantics can typically be reduced to that of the pair. Extending their operations beyond projection to include field update and deletion, however, warrants additional attention.

C.2.1 Terms. New expressions are added to the source language to create and manipulate records: the empty record, a record update expression, a field deletion expression, and a field projection expression. Record values consist of empty records and record update expressions whose constituent expressions are themselves values.

$$\begin{array}{lrcl} \textbf{Expressions} & e & ::= & \cdots \mid \{\} \mid \{e\ \texttt{with}\ \ell = e\} \mid e\backslash\ell \mid e.\ell \\ \textbf{Values} & v & ::= & \cdots \mid \{\} \mid \{v\ \texttt{with}\ \ell = v\} \end{array} \tag{41}$$

To reduce verbosity, we use syntactic sugar for nonempty records. Assuming all the labels are distinct, $\{\{\{\{\}\ \texttt{with}\ \ell_1 = e_1\}\ \texttt{with}\ \ell_2 = e_2\} \ldots\ \texttt{with}\ \ell_n = e_n\}$ is represented by $\{\ell_1 = e_1, \ell_2 = e_2, \ldots \ell_n = e_n\}$.

The record expressions of the source language correspond directly[12] to operations on objects in JavaScript:

JavaScript	Source Language
`obj.field`	`obj.field`
`delete obj.field`	`obj\field`
`obj.field = val`	`{obj with field = val}`

C.2.2 Declarative Type System. Reduction of record expressions is straightforward. It is worth noting that in this representation, multiple identical labels may exist in a record expression, but this is equivalent to limiting to one label, as projection reduces to the last-applied field, and deletion

[12]One important difference is that the operations in JavaScript are effectful. Field update and deletion modify the object on which they are operating, rather than returning a new object. To complicate things further, update and projection operations may actually call setter and getter methods on the object, rather than directly modifying the object's properties. Lastly, property accesses may be forwarded to an object's prototype if not present on the object itself. We use a more naïve model for comparison.

removes all instances of a label from the record:

$$\{v' \texttt{ with } \ell = v\}.\ell \rightsquigarrow v \tag{42}$$

$$\{v' \texttt{ with } \ell' = v\}.\ell \rightsquigarrow v'.\ell \qquad \ell' \not\equiv \ell \tag{43}$$

$$\{\}\backslash\ell \rightsquigarrow \{\} \tag{44}$$

$$\{v' \texttt{ with } \ell = v\}\backslash\ell \rightsquigarrow v'\backslash\ell \tag{45}$$

$$\{v' \texttt{ with } \ell' = v\}\backslash\ell \rightsquigarrow \{v'\backslash\ell \texttt{ with } \ell' = v\} \qquad \ell' \not\equiv \ell \tag{46}$$

Evaluation of the expressions is performed left-to-right, as in the rest of the language:

$$\textbf{Evaluation Context} \quad E \quad ::= \quad \cdots \mid \{E \texttt{ with } \ell = e\} \mid \{v \texttt{ with } \ell = E\} \mid E\backslash\ell \mid E.\ell \tag{47}$$

C.2.3 Types.

$$\begin{aligned} &\textbf{Types} \quad t \quad ::= \quad \cdots \mid \{f \cdots f\} \mid \{f \cdots f \texttt{ ..}\} \\ &\textbf{Fields} \quad f \quad ::= \quad \ell = t \mid \ell =? t \end{aligned} \tag{48}$$

In the syntax for record types, we distinguish between two kinds of record types. An open record type, denoted by $\{\ldots \texttt{ ..}\}$, is the type of records whose labels *include* those explicitly written. A closed record type, denoted by $\{\ldots\}$, is the type of records whose labels are *exactly* those explicitly written. Formally, this is syntactic sugar for the the record types of Frisch [2004], where record types are *quasi constant functions*, that is, functions that map label into types and are constant apart from on a finite number of labels. A closed record type $\{\ell_1 = t_1, \ell_2 = t_2\}$ maps ℓ_1 into t_1, ℓ_2 into t_2 and *all other labels* into the constant Undef meaning that the field is "absent". Undef is a type that is not inhabited by any value of the language. Undef and can be seen as the type of the result of projection of a missing label. Undef is particular in that it is not considered a normal type, that is, $\text{Undef} \wedge \mathbb{1} = \varnothing$. This property allows us to encode open record types, by considering them as quasi constant functions where all the labels not explicitly written are mapped to $\text{Undef} \vee \mathbb{1}$ (i.e., they are either absent, or they have some type).

The syntax of types does not allow us to explicitly refer to the Undef constant. The open/closed record syntax provides a way to set it for the infinitely many constant fields that are not explicitly written in the record type. For a single label, the access to the Undef constant is provided via the syntax of fields. There are two kinds of fields. The former, denoted by $\ell = t$, indicates the field is present in the record. The latter, denoted by $\ell =? t$ is syntactic sugar for $\ell = (t \vee \text{Undef})$, indicating that a label ℓ may be present, and if so, it has the type t. Note the special case $\ell =? \mathbb{0}$, which indicates that the field for ℓ is absent.

$$t.\ell = \begin{cases} \min\{u \mid t \leq \{\ell = u \texttt{ ..}\}\} & \text{if } t \leq \{\ell = \mathbb{1} \texttt{ ..}\} \\ \text{Undef} & \text{otherwise} \end{cases} \tag{49}$$

$$t_1 + t_2 = \min\left\{u \,\middle|\, \forall \ell \in \text{Labels}. \begin{cases} u.\ell \geq t_2.\ell & \text{if } t_2.\ell \leq \neg\text{Undef} \\ u.\ell \geq t_1.\ell \vee (t_2.\ell\backslash\text{Undef}) & \text{otherwise} \end{cases}\right\} \tag{50}$$

$$t\backslash\ell = \min\left\{u \,\middle|\, \forall \ell' \in \text{Labels}. \begin{cases} u.\ell' \geq \text{Undef} & \text{if } \ell' = \ell \\ u.\ell' \geq t.\ell' & \text{otherwise} \end{cases}\right\} \tag{51}$$

Three operators are introduced for record types. Record projection (49) represents the union of the possible types the label ℓ could have, or is undefined if the record type does not surely have a label ℓ. Record concatenation (50) is the right-favored merging of two records. If a label is present in just one of the records, then the type of that label is used. If it is present in both records, the type of the right label is used. Record label deletion (51) marks the label as Undef.

The typing rules for records to add to the declarative system are straightforward:

$$[\textsc{Record}]\ \frac{}{\Gamma \vdash \{\} : \mathbf{\{\}}} \qquad [\textsc{Update}]\ \frac{\Gamma \vdash e_1 : t_1 \qquad t_1 \leq \mathbf{\{\ ..\}} \qquad \Gamma \vdash e_2 : t_2}{\Gamma \vdash \{e_1 \texttt{ with } \ell = e_2\} : t_1 + \mathbf{\{}\ell = t_2\mathbf{\}}}$$

$$[\textsc{Delete}]\ \frac{\Gamma \vdash e : t \qquad t \leq \mathbf{\{\ ..\}}}{\Gamma \vdash e\backslash\ell : t\backslash\ell} \qquad [\textsc{Select}]\ \frac{\Gamma \vdash e : t \qquad t \leq \mathbf{\{}\ell = \mathbb{1}\ \mathbf{..\}}}{\Gamma \vdash e.\ell : t.\ell}$$

The empty record value has the closed record type. Record update uses the type operator for extension and is defined provided that the type of e_1 is a record type (i.e., $t_1 \leq \mathbf{\{\ ..\}}$). Field deletion uses the corresponding type operator and so does field projection provided that the selected field ℓ is present the expression e (i.e., $t \leq \mathbf{\{}\ell = \mathbb{1}\ \mathbf{..\}}$).

C.2.4 Intermediate Type System. The record typing rules for the intermediate type system are identical to those in the declarative system. The unwinding rules are described below.

$$\begin{aligned}
\lceil\{\}\rceil &= \{\} \\
\lceil\{\boldsymbol{e}_1 \texttt{ with } \ell = \boldsymbol{e}_2\}\rceil &= \{\lceil\boldsymbol{e}_1\rceil \texttt{ with } \ell = \lceil\boldsymbol{e}_2\rceil\} \\
\lceil\boldsymbol{e}\backslash\ell\rceil &= \lceil\boldsymbol{e}\rceil\backslash\ell \\
\lceil\boldsymbol{e}.\ell\rceil &= \lceil\boldsymbol{e}\rceil.\ell
\end{aligned}$$

C.2.5 Canonical Forms. The atomic expressions are, as before, those containing only variables as their subexpressions.

$$\textbf{Atomic expressions} \quad a \quad ::= \quad \cdots \mid \{\} \mid \{x \texttt{ with } \ell = x\} \mid x.\ell \mid x\backslash\ell \tag{52}$$

They are obtained by adding to the definition of the transformation function given in Appendix A.7 the following clauses:

$$\begin{aligned}
[\![\boldsymbol{e}\backslash\ell]\!] &= ((\Delta; x_\circ \mapsto x\backslash\ell), x_\circ) && \text{where}(\Delta, x) = [\![\boldsymbol{e}]\!] \\
[\![\boldsymbol{e}.\ell]\!] &= ((\Delta; x_\circ \mapsto x.\ell), x_\circ) && \text{where}(\Delta, x) = [\![\boldsymbol{e}]\!] \\
[\![\{\boldsymbol{e}_1 \texttt{ with } \ell = \boldsymbol{e}_2\}]\!] &= ((\Delta_1; \Delta_2; x_\circ \mapsto \{x_1 \texttt{ with } \ell = x_2\}, x_\circ) \\
& && \text{where } (\Delta_1, x_1) = [\![\boldsymbol{e}_1]\!],\ (\Delta_2, x_2) = [\![\boldsymbol{e}_2]\!]
\end{aligned}$$

C.2.6 Annotation Reconstruction Rules. We add to the clauses of Appendix B.1 the following clauses:

$$[\Gamma \vdash \square(\{\} \rightsquigarrow t)] \supset \{\} \qquad \mathbf{\{\}} \wedge t \simeq \mathbb{0} \tag{53}$$

$$[\Gamma \vdash \square(\{\} \rightsquigarrow t)] \supset \{\Gamma\} \qquad \mathbf{\{\}} \wedge t \not\simeq \mathbb{0} \tag{54}$$

$$[\Gamma \vdash \square(x.\ell \rightsquigarrow t)] \supset \{\Gamma[x \mathrel{:\hat{=}} \mathbf{\{}\ell = t\ \mathbf{..\}}]\} \tag{55}$$

$$[\Gamma \vdash \square(x\backslash\ell \rightsquigarrow \textstyle\bigvee_{i\in I} t_i)] \supset \{\Gamma[x \mathrel{:\hat{=}} t_i\backslash\ell + \mathbf{\{}\ell =? \mathbb{1}\mathbf{\}}] \mid i \in I, \mathsf{Undef} \leq t_i.\ell\} \tag{56}$$

$$[\Gamma \vdash \square(\{x_1 \texttt{ with } \ell = x_2\} \rightsquigarrow \textstyle\bigvee_{i\in I} t_i)] \supset \{\Gamma[x_1 \mathrel{:\hat{=}} t_i\backslash\ell + \mathbf{\{}\ell =? \mathbb{1}\mathbf{\}}][x_2 \mathrel{:\hat{=}} (t_i \wedge \mathbf{\{}\ell = \mathbb{1}\ \mathbf{..\}}).\ell] \mid i \in I\} \tag{57}$$

The necessary typing refinements for the empty record value are equivalent to those for other constants. For projection, the type of the record is refined only to records containing the projected label with the expected type. Field deletion and update split a union type into its components and share the expression $t_i\backslash\ell + \mathbf{\{}\ell =? \mathbb{1}\mathbf{\}}$. This expression removes all information about the label ℓ

from the record type t_i. Note that this cannot be achieved by simply removing the label as in $t_i\backslash\ell$, as this instead sets the record field to $\{\cdots \ell =? \mathbb{0} \cdots\}$. Indeed, the latter type expression denotes records for which it is statically known that label ℓ does not occur. The field deletion rule uses does it for t_i only if the field ℓ of t_i is optional or for which there is no information: every t_i for which the field ℓ has a given type (i.e., for which $\mathsf{Undef} \not\leq t_i.\ell$) is discarded because it is not possible that $x\backslash\ell$ reduces to a value that has such a type t_i. Field update removes any information about ℓ in x_1 (thus weakening the constraints on it), consider only those t_i which contain records with a field ℓ (i.e., for which $t_i \wedge \{\ell = \mathbb{1}\ ..\}$ is not empty), and refines the type of x_2 with the type of that field.

Algorithm $\vdash_{\mathcal{R}}$ (Section B.3) is extended with the rule below, plus two rules for the empty record value that we omit since they are the same as the two rules for constants given in Section B.3 (just, replace $\{\}$ for c and $\{\}$ for $\boldsymbol{b}_c$):

$$[\textsc{SelectEmpty}]\ \frac{\Gamma(x) \simeq \mathbb{0}}{\Gamma \vdash_{\mathcal{R}} x.\ell : t \Rightarrow (x.\ell, \{\Gamma\})} \qquad [\textsc{Select}]\ \frac{\Gamma(x) \wedge \{\ell = t\ ..\} \overset{\text{DNF}}{\cong} \bigvee_{i\in I} t_i}{\Gamma \vdash_{\mathcal{R}} x.\ell : t \Rightarrow (x.\ell, \{\Gamma[x :\hat{=} t_i]\}_{i\in I})}$$

$$[\textsc{UpdateEmpty}]\ \frac{\Gamma(x_1) \times \Gamma(x_2) \simeq \mathbb{0}}{\Gamma \vdash_{\mathcal{R}} \{x_1\ \mathtt{with}\ \ell = x_2\} : t \Rightarrow (\{x_1\ \mathtt{with}\ \ell = x_2\}, \{\Gamma\})}$$

$$[\textsc{Update}]\ \frac{\{x_1, x_2\} \subseteq \mathsf{dom}(\Gamma) \qquad t \wedge \{\ell = \Gamma(x_2)\ ..\} \overset{\text{DNF}}{\cong} \bigvee_{i\in I} t_i}{\Gamma \vdash_{\mathcal{R}} \{x_1\ \mathtt{with}\ \ell = x_2\} : t \Rightarrow (\{x_1\ \mathtt{with}\ \ell = x_2\}, \{\Gamma[x_1 :\hat{=} (t_i\backslash\ell) + \{\ell =? \mathbb{1}\}][x_2 :\hat{=} t_i.\ell]\}_{i\in I})}$$

$$[\textsc{DeleteEmpty}]\ \frac{\Gamma(x) \simeq \mathbb{0}}{\Gamma \vdash_{\mathcal{R}} x\backslash\ell : t \Rightarrow (x\backslash\ell, \{\Gamma\})}$$

$$[\textsc{Delete}]\ \frac{t \wedge \{\ell =? \mathbb{0}\ ..\} \overset{\text{DNF}}{\cong} \bigvee_{i\in I} t_i}{\Gamma \vdash_{\mathcal{R}} x\backslash\ell : t \Rightarrow (x\backslash\ell, \{\Gamma[x :\hat{=} (t_i\backslash\ell) + \{\ell =? \mathbb{1}\}]\}_{i\in I})}$$

These rules work in a way similar to the rules for products (pairs and projections). Each new atom is handled by two cases. In the case where the variable(s) at play have the empty type, the input environment Γ is returned as a singleton, denoting success. Otherwise, the relevant record part of the input type is isolated using an intersection with the top record type (augmented with the relevant field), split into a union of records, and the input environment is refined accordingly. In particular, [Select] refines the type of x so that it becomes a record type in which the field ℓ has a subtype of t. The rule [Update] refines the type of x_1 to conform the expected type t but without touching any type information about the type of ℓ in x (since this information has no effect on the final type of the update) and refines the type of x_2 so that it is a subtype of the type of the field ℓ in the checked type t. Finally, [Delete] refines the type of x so that it becomes a subtype of the checked type t but without considering and touching the type information of the field ℓ in the type of x (since it does not inflence the typing of $x \setminus \ell$ whose ℓ field is of type $\mathsf{Undef} \vee \mathbb{0}$).

D PROOFS

D.1 Declarative Type System

D.1.1 Parallel Semantics. One technical difficulty in the proof of the subject reduction property is that reducing an expression e might break the use of a $[\vee]$ rule. Indeed, if in the original typing derivation a rule $[\vee]$ substitutes multiple occurrences of the expression e by a variable x, reducing one occurrence of e but not the others would alter the application of this rule (correlation between the reduced e and the other occurrences of e will be lost).

To circumvent this issue, we introduce a notion of parallel reduction which forces to reduce all occurrences of a sub-expression at the same time.

The idea is to remember, when applying a reduction under a context, which reduction has been performed inside this context. For that, each step of reduction is labeled with a statement of the form $e_1 \mapsto e_2$ which denotes the inner reduction that has been performed. Then, this label is used by the context rule (rule $[\kappa]$ below) which will substitute occurrences of e_1 by e_2 everywhere in the expression (not only under the current context).

The semantics based on parallel reduction is given below.

For convenience, we denote $e \overset{e\mapsto e'}{\rightsquigarrow} e'$ by $e \overset{Id}{\rightsquigarrow} e'$ and by $e \overset{-}{\rightsquigarrow} e'$ a step of reduction of the parallel semantics, regardless of the value on the top of the arrow.

$$(\lambda x.e)v \overset{Id}{\rightsquigarrow} e\{v/x\} \tag{58}$$

$$\pi_1(v_1, v_2) \overset{Id}{\rightsquigarrow} v_1 \tag{59}$$

$$\pi_2(v_1, v_2) \overset{Id}{\rightsquigarrow} v_2 \tag{60}$$

$$(v\in\tau)\ ?\ e_1 : e_2 \overset{Id}{\rightsquigarrow} e_1 \qquad \text{if } v \in \tau \tag{61}$$

$$(v\in\tau)\ ?\ e_1 : e_2 \overset{Id}{\rightsquigarrow} e_2 \qquad \text{if } v \in \neg\tau \tag{62}$$

The contexts are not exactly those of the original semantics: nesting of contexts is now handled by the rule $[\kappa]$. This yields the following definition:

$$\textbf{Evaluation Context} \quad \bar{E} ::= v[\,] \mid [\,]e \mid (v, [\,]) \mid ([\,], e) \mid ([\,]\in\tau)\ ?\ e : e$$

Context reductions:

$$[\kappa]\ \frac{e \overset{e_r\mapsto e_r'}{\rightsquigarrow} e'}{\bar{E}[e] \overset{e_r\mapsto e_r'}{\rightsquigarrow} (\bar{E}[e'])\{e_r'/e_r\}}$$

Here is an example of a reduction step using the parallel semantics:

$$[\kappa]\ \frac{[\beta]\ \dfrac{}{(\lambda x.\ x+1)\ 1 \overset{(\lambda x.\ x+1)\ 1\ \mapsto\ 2}{\rightsquigarrow} 2}}{\texttt{if } (\lambda x.\ x+1)\ 1 \in \texttt{Int then } (\lambda x.\ x+1)\ 1 \texttt{ else } 0 \overset{(\lambda x.\ x+1)\ 1\ \mapsto\ 2}{\rightsquigarrow} \texttt{if } 2 \in \texttt{Int then } 2 \texttt{ else } 0}$$

Notice that the rule $[\kappa]$ applies a substitution from an expression to an expression. This is formally defined as follows:

Definition D.1 (Expression substitutions). *Expression substitutions, ranged over by ρ, map an expression into another expression. The application of an expressions substitution ρ to an expression e, noted $e\rho$ is the capture avoiding replacement defined as follows:*

- *If $e' \equiv_\alpha e''$, then $e''\{e/e'\} = e$.*
- *If $e' \not\equiv_\alpha e''$, then $e''\{e/e'\}$ is inductively defined as*

$$
\begin{aligned}
c\{e/e'\} &= c \\
x\{e/e'\} &= x \\
(e_1 e_2)\{e/e'\} &= (e_1\{e/e'\})(e_2\{e/e'\}) \\
(\lambda x.e_\circ)\{e/e'\} &= \lambda x.e_\circ && x \in fv(e') \\
(\lambda x.e_\circ)\{e/e'\} &= \lambda x.(e_\circ\{e/e'\}) && x \notin fv(e) \cup fv(e') \\
(\lambda x.e_\circ)\{e/e'\} &= \lambda y.((e_\circ\{y/x\})\{e/e'\}) && x \notin fv(e), x \in fv(e'), y \text{ fresh} \\
(\pi_i e_\circ)\{e/e'\} &= \pi_i(e_\circ\{e/e'\}) \\
(e_1, e_2)\{e/e'\} &= (e_1\{e/e'\}, e_2\{e/e'\}) \\
((e_1 \in t)\,?\,e_2 : e_3)\{e/e'\} &= (e_1\{e/e'\} \in t)\,?\,e_2\{e/e'\} : e_3\{e/e'\}
\end{aligned}
$$

Notice that the expression substitutions are up to alpha-renaming and perform only one pass.

D.1.2 Normalization Lemmas. See 3 for the full delcarative system.

In the proofs below, the $[\vee+]$ and $[\wedge+]$ rules will be used instead of the $[\vee]$ and $[\wedge]$ rules.

Lemma D.2 (Monotonicity). *If $\Gamma \vdash e : t$ and $\Gamma' \leq \Gamma$, then $\Gamma' \vdash e : t$.*

Proof. By induction on the derivation of the judgement $\Gamma \vdash e : t$. □

Lemma D.3 (Intersection). *If $\Gamma \vdash e : t_1$ and $\Gamma \vdash e : t_2$, then $\Gamma \vdash e : t_1 \wedge t_2$.*

Proof. Straightforward, by using a rule $[\wedge+]$. □

Lemma D.4 (Union). *If $\Gamma, x : t_1 \vdash e : t$ and $\Gamma, x : t_2 \vdash e : t$, then $\Gamma, x : (t_1 \vee t_2) \vdash e : t$.*

Proof. Straightforward, by using a rule $[\vee+]$ of the following form:

$$
[\vee+]\ \frac{\Gamma, x : (t_1 \vee t_2) \vdash x : t_1 \vee t_2 \qquad \Gamma, x : (t_1 \vee t_2), y : t_1 \vdash e : t \qquad \Gamma, x : (t_1 \vee t_2), y : t_2 \vdash e : t}{\Gamma, x : (t_1 \vee t_2) \vdash e\{x/y\} : t}
$$

□

Lemma D.5 (Normalization of $[\leq]$ rules). *Any derivation of $\Gamma \vdash e : t$ can be transformed so that every application of $[\leq]$ is:*

- *At the root of the derivation, or*
- *The first premise of a $[\in_1]$ or $[\in_2]$ rule, or*
- *The nth premise ($n \geq 2$) of a $[\vee+]$ rule, or*
- *The premise of a $[\times E_1]$ or $[\times E_2]$ rule, or*
- *The first premise of a $[\to E]$ rule*

Proof. We can transform any derivation into a derivation that satisfies these properties. We proceed by induction on the depth of the derivation, without counting the $[\leq]$ rules nor the axioms ([Ax] and [Const]).

When there are two consecutive $[\leq]$ rules, they can trivially be merged into one $[\leq]$ rule.

The base case is trivial (if there is a $[\leq]$ rule, it is at the root of the derivation).

Now we consider the last rule of the derivation which is not a [≤], and assume that its premises satisfy these properties.

If the last rule is a [∧+] with one of its premises being a [≤] rule:

$$\dfrac{\dfrac{\dfrac{A}{\Gamma \vdash e : t_1'}}{\Gamma \vdash e : t_1}[\leq] \qquad \dfrac{B_i}{\Gamma \vdash e : t_i}\ \forall i \in I}{\Gamma \vdash e : t_1 \wedge \bigwedge_{i\in I} t_i}[\wedge+] \quad \longrightarrow \quad \dfrac{\dfrac{\dfrac{A}{\Gamma \vdash e : t_1'} \qquad \dfrac{B_i}{\Gamma \vdash e : t_i}\ \forall i \in I}{\Gamma \vdash e : t_1' \wedge \bigwedge_{i\in I} t_i}[\wedge+]}{\Gamma \vdash e : t_1 \wedge \bigwedge_{i\in I} t_i}[\leq]$$

If the last rule is a [∨+] with its first premise being a [≤], we apply the following transformation and then proceed inductively on the transformed B_i premises:

$$\dfrac{\dfrac{\dfrac{A}{\Gamma \vdash e' : s'}}{\Gamma \vdash e' : \bigvee_{i\in I} s_i}[\leq] \qquad \dfrac{B_i}{\Gamma, : s_i \vdash e : t}\ \forall i \in I}{\Gamma \vdash e\{e'/x\} : t}[\vee+]$$

$$\downarrow$$

$$\dfrac{\dfrac{\dfrac{A}{\Gamma \vdash e' : \bigvee_{i\in I}(s_i \wedge s')} \qquad \dfrac{\text{Easily derived from } B_i}{\Gamma, (x : s_i \wedge s') \vdash e : t}\ \forall i \in I}{\Gamma \vdash e\{e'/x\} : t}[\vee+]}{\Gamma \vdash e\{e'/x\} : t}[\leq]$$

The other cases are trivial or similar. □

Lemma D.6 (Normalization of [∧+] rules). *Any derivation of* $\Gamma \vdash e : t$ *can be transformed so that all the applications of [∧+] have only [→I] rules as premises.*

Proof. We can transform any derivation into a derivation that satisfies these properties. First, we apply the [≤] normalization lemma on the derivation, so that [∧+] rules cannot have a [≤] rule as premise. Then, we proceed by induction on the size of the derivation (i.e. the total number of rule applications) without counting the applications of [≤] nor the axioms ([Ax] and [Const]).

The base case (size 0) is trivially true, as there are no instances of [∧+].

In the inductive case, if the last rule of the derivation is not a [∧+], we can directly conclude by induction. If the last rule is a [∧+] with one of its premises being another [∧+] rule, we can easily merge the two [∧+] rules and proceed inductively on the result.

If the last rule is a [∧+] with one of its premises being a [∨+] rule, we can apply the following transformation and proceed inductively on the premises:

$$\dfrac{\dfrac{\dfrac{A}{\Gamma \vdash e' : \bigvee_{i\in I} s_i} \quad \dfrac{B_i}{\Gamma, x : s_i \vdash e : t_1}\ \forall i \in I}{\Gamma \vdash e\{e'/x\} : t_1}\ [\vee+] \quad \dfrac{D_j}{\Gamma \vdash e\{e'/x\} : t_j}\ \forall j \in J}{\Gamma \vdash e\{e'/x\} : t_1 \wedge \bigwedge_{j\in J} t_j}\ [\wedge+]$$

$$\downarrow$$

$$\dfrac{\dfrac{\dfrac{A}{\Gamma \vdash e' : \bigvee_{i\in I} s_i} \quad \dfrac{\text{Easily derived from } B_i}{\Gamma, x : s_i \vdash \bar{e} : t_1} \quad \dfrac{\text{Easily derived from } D_j}{\Gamma, x : s_i \vdash \bar{e} : t_j}\ \forall j \in J}{\Gamma, x : s_1 \vdash \bar{e} : t_1 \wedge \bigwedge_{j\in J} t_j}\ [\wedge+]\ \forall i \in I}{\Gamma \vdash \bar{e}\{e'/x\} : t_1 \wedge \bigwedge_{j\in J} t_j}\ [\vee+]$$

with $\bar{e} = e\{x/e'\}$

If the last rule is a $[\wedge+]$ and all its premises are a $[\to\text{E}]$ rule, we can apply the following transformation and proceed inductively on the premises:

$$\dfrac{\dfrac{\dfrac{A_i}{\Gamma \vdash e_1 : t_1^i \to t_2^i} \quad \dfrac{B_i}{\Gamma \vdash e_2 : t_1^i}}{\Gamma \vdash e_1 e_2 : t_2^i}\ [\to\text{E}]\ \forall i \in I}{\Gamma \vdash e_1 e_2 : \bigwedge_{i\in I} t_2^i}\ [\wedge+]$$

$$\downarrow$$

$$\dfrac{\dfrac{\dfrac{\dfrac{A_i}{\Gamma \vdash e_1 : t_1^i \to t_2^i}\ \forall i \in I}{\Gamma \vdash e_1 e_2 : \bigwedge_{i\in I}(t_1^i \to t_2^i)}\ [\wedge+] \quad \dfrac{B_i}{\Gamma \vdash e_2 : t_1^i}\ \forall i \in I}{\Gamma \vdash e_1 e_2 : (\bigwedge_{i\in I} t_1^i) \to (\bigwedge_{i\in I} t_2^i)}\ [\leq] \quad \Gamma \vdash e_2 : \bigwedge_{i\in I} t_1^i\ [\wedge+]}{\Gamma \vdash e_1 e_2 : \bigwedge_{i\in I} t_2^i}\ [\to\text{E}]$$

The other cases are trivial. □

Lemma D.7 (Normalization of $[\vee+]$ rules). *Any derivation of $\Gamma \vdash e : t$ can be transformed so that every application of $[\vee+]$ that uses the substitution $\{e'/x\}$ satisfies one of these conditions:*

- *It is the nth premise ($n \geq 2$) of a (possibly empty) succession of $[\vee+]$ rules at the root of the derivation*
- *It is the nth premise ($n \geq 2$) of a (possibly empty) succession of $[\vee+]$ rules used as a premise of a $[\to I]$ rule that introduces a variable y such that $y \in fv(e')$*
- *It is the nth premise ($n \geq 2$) of a (possibly empty) succession of $[\vee+]$ rules used as a premise of a $[\vee+]$ rule that introduces a variable y such that $y \in fv(e')$*

Proof. We can transform any derivation into a derivation that satisfies these properties. First, we apply the [∧+] normalization lemma on the derivation, so that [∧+] rules cannot have a [∨+] rule as premise. Then, we proceed by structural induction on the derivation.

The base cases are trivially true, as there is no instance of [∨+].

Now, we consider the last rule of the derivation and assume that its premises satisfy these properties.

If the last rule is a [∨+] with another [∨+] rule as first premise:

$$\dfrac{\dfrac{\dfrac{A}{\Gamma \vdash e'' : \bigvee_{j\in J} s_j} \quad \dfrac{B_j}{\Gamma, y : s_j \vdash e' : \bigvee_{i\in I} t_i}\ \forall j \in J}{\Gamma \vdash e'\{e''/y\} : \bigvee_{i\in I} t_i}\ [\vee+] \quad \dfrac{C_i}{\Gamma, x : t_i \vdash e : t}\ \forall i \in I}{\Gamma \vdash e\{e'\{e''/y\}/x\} : t}\ [\vee+]$$

$$\downarrow$$

$$\dfrac{\dfrac{A}{\Gamma \vdash e'' : \bigvee_{j\in J} s_j} \quad \dfrac{\dfrac{B_j}{\Gamma, y : s_j \vdash e' : \bigvee_{i\in I} t_i} \quad \dfrac{\text{Easily derived from } C_i}{\Gamma, y : s_j, x : t_i \vdash e : t}\ \forall i \in I}{\Gamma, y : s_j \vdash e\{e'/x\} : t}\ [\vee+]\ \forall j \in J}{\Gamma \vdash (e\{e'/x\})\{e''/y\} : t}\ [\vee+]$$

with $y \notin \mathrm{fv}(e)$ (y can be renamed otherwise)

If the last rule is a [→I], introducing a variable y, with a [∨+] rule as premise, such that $y \notin \mathrm{fv}(e')$:

$$\dfrac{\dfrac{\dfrac{A}{\Gamma, y : t_1 \vdash e' : \bigvee_{i\in I} s_i} \quad \dfrac{B_i}{\Gamma, y : t_1, x : s_i \vdash e : t_2}\ \forall i \in I}{\Gamma, y : t_1 \vdash e\{e'/x\} : t_2}\ [\vee+]}{\Gamma \vdash \lambda y.\ (e\{e'/x\}) : t_1 \to t_2}\ [\to\mathrm{I}]$$

$$\downarrow$$

$$\dfrac{\dfrac{\text{Easily derived from } A}{\Gamma \vdash e' : \bigvee_{i\in I} s_i} \quad [\to\mathrm{I}]\ \dfrac{\dfrac{B_i}{\Gamma, x : s_i, y : t_1 \vdash e : t_2}}{\Gamma, x : s_i \vdash \lambda y.\ e : t_1 \to t_2}\ \forall i \in I}{\Gamma \vdash (\lambda y.\ e)\{e'/x\} : t_1 \to t_2}\ [\vee+]$$

In order to apply the transformation above, we can swap two independent [∨+] rules if necessary: if we have a [∨+] rule that uses the substitution $\{e''/y\}$ as the nth premise ($n \geq 2$) of another [∨+] rule that uses the substitution $\{e'/x\}$, and such that $x \notin \mathrm{fv}(e'')$, then we can swap the order of these two [∨+] rules in the following way.

$$[\vee+]\ \dfrac{\dfrac{A}{\Gamma \vdash e' : t_1 \vee \bigvee_{i\in I} t_i} \qquad [\vee+]\ \dfrac{\dfrac{B}{\Gamma, x : t_1 \vdash e'' : \bigvee_{j\in J} s_j} \qquad \dfrac{C_j}{\Gamma, x : t_1, y : s_j \vdash e : t}\ \forall j \in J}{\Gamma, x : t_1 \vdash e\{e''/y\} : t} \qquad \dfrac{D_i}{\Gamma, x : t_i \vdash e\{e''/y\} : t}\ \forall i \in I}{\Gamma \vdash (e\{e''/y\})\{e'/x\} : t}$$

$$\downarrow$$

$$\dfrac{\text{Easily derived from } B}{\Gamma \vdash e'' : \bigvee_{j\in J} s_j} \qquad \dfrac{\text{Easily derived from } A}{\Gamma, y : s_j \vdash e' : t_1 \vee \bigvee_{i\in I} t_i}$$

$$[\vee+]\ \dfrac{[\vee+]\ \dfrac{\dfrac{\text{Easily derived from } C_j}{\Gamma, y : s_j, x : t_1 \vdash \bar{e} : t} \qquad \dfrac{\text{Easily derived from } D_i}{\Gamma, y : s_j, x : t_i \vdash \bar{e} : t}\ \forall i \in I}{\Gamma, y : s_j \vdash \bar{e}\{e'/x\} : t}\ \forall j \in J}{\Gamma \vdash (\bar{e}\{e'/x\})\{e''/y\} : t}$$

$$\text{with } \bar{e} = e\{y/e''\}$$

If the last rule is a [≤] with a [∨+] rule as premise:

$$[\leq]\ \dfrac{[\vee+]\ \dfrac{\dfrac{A}{\Gamma \vdash e' : \bigvee_{i\in I} s_i} \qquad \dfrac{B_i}{\Gamma, x : s_i \vdash e : t'}\ \forall i \in I}{\Gamma \vdash e\{e'/x\} : t'}}{\Gamma \vdash e\{e'/x\} : t}$$

$$\downarrow$$

$$[\vee+]\ \dfrac{\dfrac{A}{\Gamma \vdash e' : \bigvee_{i\in I} s_i} \qquad [\leq]\ \dfrac{\dfrac{B_i}{\Gamma, x : s_i \vdash e : t'}}{\Gamma, x : s_i \vdash e : t}\ \forall i \in I}{\Gamma \vdash e\{e'/x\} : t}$$

If the last rule is a [→E] with a [∨+] rule as first premise:

$$\dfrac{\dfrac{\dfrac{A}{\Gamma \vdash e' : \bigvee_{i\in I} s_i} \quad \dfrac{B_i}{\Gamma, x : s_i \vdash e_1 : t_1 \to t_2}\ \forall i \in I}{\Gamma \vdash e_1\{e'/x\} : t_1 \to t_2}\ [\vee+] \quad \dfrac{C}{\Gamma \vdash e_2 : t_1}}{\Gamma \vdash (e_1\{e'/x\})e_2 : t_2}\ [\to\text{E}]$$

$$\downarrow$$

$$\dfrac{\dfrac{A}{\Gamma \vdash e' : \bigvee_{i\in I} s_i} \quad \dfrac{\dfrac{B_i}{\Gamma, x : s_i \vdash e_1 : t_1 \to t_2} \quad \dfrac{\text{Easily derived from } C}{\Gamma, x : s_i \vdash e_2 : t_1}}{\Gamma, x : s_i \vdash e_1 e_2 : t_2}\ [\to\text{E}]\ \forall i \in I}{\Gamma \vdash (e_1 e_2)\{e'/x\} : t_2}\ [\vee+]$$

with $x \notin \text{fv}(e_2)$ (x can be renamed otherwise)

If the last rule is a [→E] with a [∨+] rule as second premise, the transformation is similar. The other cases are trivial or similar. □

Lemma D.8 (Deletion of value substitutions). *Any derivation of $\Gamma \vdash e : t$ can be transformed so that it does not contain any [∨+] rule with e' being a value.*

Proof. First, we apply the [≤], [∧+] and [∨+] normalization lemmas above to the derivation. In particular, this ensures that there are no [∨+] rules in the derivations of the first premises of the [∨+] rules, except as premise of a [→I] rule.

Now, let's suppose one of the [∨+] rule of our derivation is using a substitution $\{e'/x\}$ with e' being a value. Its first premise is of the form $\Gamma \vdash v : t'$ with $v \equiv e'$ and $t' \simeq \bigvee_{i\in I} t_i$. As the [≤] and [∨+] rules have been normalized, the derivation of this premise does not contain any [∨+] rule nor [≤] rule, except inside the derivation of the premise of a [→I] rule.

It can easily be deduced that t' can be constructed with the following syntax:

$$\textbf{Value Type} \quad \bar{t} \quad ::= \quad b \mid t \to t \mid \bar{t} \times \bar{t} \mid \bar{t} \wedge \bar{t}$$

A type constructed with the syntax above cannot be decomposed into a non-trivial union (in particular, a conjunction of arrows cannot be decomposed into a non-trivial union of arrows). Thus, we can deduce that the decomposition $t' \simeq \bigvee_{i\in I} t_i$ is such that $\exists i \in I.\ \forall j \in I.\ t_i \leq t_j$.

Then, it becomes easy to remove the application of the [∨+] rule from our derivation by replacing it by one of its premises (the one of the form $\Gamma, x : t_i \vdash e : t$ for some Γ, e and t) in which the applications of the rule [Ax] applied to v have been replaced by the first premise.

This transformation can be used successively to remove all such [∨+] rules in the derivation. □

Note that all the normalization lemmas above are compatible: by applying the transformations successively, we can transform a derivation into another one that satisfies all the lemmas D.5, D.6, D.7 and D.8.

D.1.3 Subject-Reduction.

Property D.9. *If $\Gamma \vdash v : \tau$, then $v \in \tau$.*

Proof. Straightforward, by induction on the derivation of the judgement $\Gamma \vdash v : \tau$. Note that the case of lambda-abstractions is trivial as τ can only be $\mathbb{0} \to \mathbb{1}$. □

Lemma D.10 (Substitution lemma). *If* $\Gamma, (x : t_\circ) \vdash e : t$ *and* $\Gamma \vdash e' : t_\circ$, *then* $\Gamma \vdash e\{e'/x\} : t$.

Proof. Straightforward, by using the rule [$\vee$] with $t_1 = t_2 = t_\circ$. □

The proof of the subject reduction requires a more permissive notion of reduction. In particular, for the inductive case [$\vee$+], we need our induction hypothesis to be able to reduce under any context and to consider that variables are values.

Thus, we introduce the following notion of reduction. Note that it does not contain any context rule (reductions can only happen at top-level): the context is handled in the statement of the subject reduction.

$$\textbf{Extended Values} \quad \bar{v} \quad ::= \quad c \mid \lambda x.e \mid (\bar{v}, \bar{v}) \mid x \tag{63}$$

$$(\lambda x.e)\bar{v} \rightsquigarrow_{\mathsf{Ex}} e\{\bar{v}/x\} \tag{64}$$
$$\pi_1(\bar{v}_1, \bar{v}_2) \rightsquigarrow_{\mathsf{Ex}} \bar{v}_1 \tag{65}$$
$$\pi_2(\bar{v}_1, \bar{v}_2) \rightsquigarrow_{\mathsf{Ex}} \bar{v}_2 \tag{66}$$
$$(v \in \tau)\ ?\ e_1 : e_2 \rightsquigarrow_{\mathsf{Ex}} e_1 \quad \text{if } v \in \tau \tag{67}$$
$$(v \in \tau)\ ?\ e_1 : e_2 \rightsquigarrow_{\mathsf{Ex}} e_2 \quad \text{if } v \in \neg\tau \tag{68}$$

Theorem D.11 (Generalized subject reduction). *If* $\Gamma \vdash e : t$ *and* $e_\circ \rightsquigarrow_{\mathsf{Ex}} e'_\circ$, *then* $\Gamma \vdash e\{e'_\circ/e_\circ\} : t$.

Proof. We apply all the normalization lemmas above to the derivation of the judgement $\Gamma \vdash e : t$, and we proceed by structural induction on it. We denote by ρ the substitution $\{e'_\circ/e_\circ\}$ and by e' the expression $e\rho$. If e contains no occurrence of $e_\circ$ (modulo alpha-renaming), this theorem is trivial. Thus, we will suppose in the following that e contains at least one occurrence of $e_\circ$.

Depending on the last rule used:

[Const] Impossible case (e cannot contain a reducible expression).

[Ax] Impossible case (e cannot contain a reducible expression).

[$\leq$] By induction on the premise $\Gamma \vdash e : t'$ (with $t' \leq t$), we get a derivation for $\Gamma \vdash e' : t'$, thus we can derive $\Gamma \vdash e' : t$ by using [$\leq$].

[$\wedge$+] Trivial (by induction on the premises as in the previous case).

[$\rightarrow$I] We have $e' \equiv \lambda x.\ (e_1\rho)$, thus we can conclude by induction on the premise $\Gamma, x : t_1 \vdash e_1 : t_2$ as in the previous case.

[$\times$I] We have $e' \equiv (e_1\rho, e_2\rho)$, thus we can conclude by induction on the premises as in the previous case.

[$\rightarrow$E] We have $e \equiv e_1e_2$. If $e_\circ$ is a subexpression of e_1 and/or e_2, we conclude trivially by induction (as in the previous cases).

Otherwise, the reduction $e_\circ \rightsquigarrow_{\mathsf{Ex}} e'_\circ$ uses the rule 58 and we know that $e_\circ \equiv e \equiv (\lambda x.\ e_\lambda)\bar{v}_2$ and $e'_\circ \equiv e' \equiv e_\lambda\{\bar{v}_2/x\}$.

We have the following premises:

(1) $\Gamma \vdash \lambda x.\ e_\lambda : t_1 \rightarrow t_2$ (with $t_2 \simeq t$)

(2) $\Gamma \vdash \bar{v}_2 : t_1$

As the [$\vee$+] rules of our derivation satisfy the normalization lemma D.7, we can extract from the first premise a collection of derivations of the judgements $\Gamma, x : s_i \vdash e_\lambda : s'_i$ for $i \in I$, such that $\bigwedge_{i\in I} s_i \rightarrow s'_i \leq t_1 \rightarrow t_2$.

Let's consider a partition $\{u_j\}_{j\in J}$ of t_1 that satisfies the following property:
$\forall i \in I.\ \forall j \in J.\ u_j \leq s_i$ or $u_j \wedge s_i = \emptyset$.

We can suppose that J is not empty: the case $t_1 \simeq \mathbb{0}$ is trivial. For every $j \in J$, we pose $I_j = \{i \in I \mid s_i \wedge u_j \neq \varnothing\}$ (I_j cannot be empty as $t_1 \leq \bigvee_{i\in I} s_i$). Note that for all $j \in J$ and $i \in I_j$, we have $u_j \leq s_i$.
According to the monotonicity lemma (D.2), for every $j \in J$ and $i \in I_j$ we can derive the judgement $\Gamma, x : u_j \vdash e_\lambda : s'_i$. Moreover, as $\bigwedge_{i\in I} s_i \to s'_i \leq t_1 \to t_2$, we have for every $j \in J$: $\bigwedge_{i\in I_j} s'_i \leq t_2$.
Consequently, for every $j \in J$, we can derive the judgement $\Gamma, x : u_j \vdash e_\lambda : t_2$ using the intersection lemma (D.3) on the judgements $\{\Gamma, x : u_j \vdash e_\lambda : s'_i\}_{i\in I_j}$. Using the union lemma (D.4) on the judgements $\{\Gamma, x : u_j \vdash e_\lambda : t_2\}_{i\in I}$, we can derive $\Gamma, x : t_1 \vdash e_\lambda : t_2$.
As $\Gamma \vdash \bar{v}_2 : t_1$, we can deduce, using the substitution lemma (D.10), a derivation for $\Gamma \vdash e_\lambda\{\bar{v}_2/x\} : t_2$.

[×E$_1$] We have $e \equiv \pi_1 e_1$. If $e_\circ$ is a subexpression of e_1, we conclude trivially by induction.
Otherwise, the reduction $e_\circ \rightsquigarrow_{\mathsf{Ex}} e'_\circ$ uses the rule 59 and we know that $e_\circ \equiv e \equiv \pi_1(\bar{v}_1, \bar{v}_2)$ and $e'_\circ \equiv e' \equiv \bar{v}_1$.
As the [∨+] rules of our derivation satisfy the normalization lemma D.7, we can extract from the premise $\Gamma \vdash (\bar{v}_1, \bar{v}_2) : t_1 \times t_2$ a collection of derivations of the judgements $\Gamma \vdash \bar{v}_1 : s_i$ and $\Gamma \vdash \bar{v}_2 : s'_i$ for $i \in I$, such that $\bigwedge_{i\in I}(s_i \times s'_i) \leq t_1 \times t_2$. This last property implies $\bigwedge_{i\in I} s_i \leq t_1$.
Therefore, we can conclude this case by using the intersection lemma (D.3) on the judgements $\{\Gamma \vdash \bar{v}_1 : s_i\}_{i\in I}$.

[×E$_2$] Similar to the previous case.

[∨+] We have $e \equiv e_1\{e_2/x\}$ (conclusion of the [∨+] rule), and thus $e' \equiv (e_1\{e_2/x\})\{e'_\circ/e_\circ\}$. We know that $e_\circ$ does not contain x as a free variable (otherwise there would be no occurrence of $e_\circ$ in $e_1\{e_2/x\}$). Moreover, $e'_\circ$ does not contain x neither, because a reduction step cannot introduce a new free variable.
There are several cases:

- $e_\circ$ does not contain e_2 and e_2 does not contains $e_\circ$. In this case, we have: $e' \equiv (e_1\{e_2/x\})\{e'_\circ/e_\circ\} \equiv (e_1\{e'_\circ/e_\circ\})\{e_2/x\}$. Thus, we can easily conclude with a [∨+] rule by keeping the first premise and applying the induction hypothesis on the others.
- e_2 contains $e_\circ$. In this case, we pose $e'_2 = e_2\{e'_\circ/e_\circ\}$.
  We have $e' \equiv (e_1\{e_2/x\})\{e'_\circ/e_\circ\} \equiv (e_1\{e'_\circ/e_\circ\})\{e'_2/x\}$. We can easily derive $\Gamma \vdash e'_2 : \bigvee_{i\in I} t_i$ by induction on the first premise, and $\Gamma, x : t_i \vdash e_1\{e'_\circ/e_\circ\} : t$ for all $i \in I$ by induction on the others. Thus, we can we can derive $\Gamma \vdash (e_1\{e'_\circ/e_\circ\})\{e'_2/x\} : t$ using the [∨+] rule.
- $e_\circ$ contains e_2 as a strict subexpression. In this case, we pose $e^1_\circ = e_\circ\{x/e_2\}$ and $e^2_\circ = e'_\circ\{x/e_2\}$.
  We have $e' \equiv (e_1\{e_2/x\})\{e'_\circ/e_\circ\} \equiv (e_1\{e^2_\circ/e^1_\circ\})\{e_2/x\}$. Again, there are several cases:
  - $e^1_\circ \rightsquigarrow_{\mathsf{Ex}} e^2_\circ$ This is the case if e_2 only appears in $e_\circ$ inside of a lambda abstraction, in a branch of a typecase, or in a value used as argument of an application or projection. In this case, we can easily conclude with a [∨+] rule by keeping the first premise and applying the induction hypothesis on the others.
  - $e^1_\circ \equiv x\bar{v}$ (for any $\bar{v}$) It means that e_2 is a lambda-abstraction. We can skip this case without loss of generality according to the lemma D.8.
  - $e^1_\circ \equiv \pi_1 x$ It means that e_2 is a value. We can skip this case without loss of generality according to the lemma D.8.
  - $e^1_\circ \equiv \pi_2 x$ Similar to the previous case.
  - $e^1_\circ \equiv (x\in\tau)\ ?\ e_t : e_e$ (for any τ, e_t, e_e) Similar to the previous case.

[𝟘] We have $e \equiv (e_1\in\tau)\ ?\ e_2 : e_3$. As values cannot have the type $\mathbb{0}$, we know that e_1 is not a value. Thus, $e' \equiv (e_1\rho\in\tau)\ ?\ e_2\rho : e_3\rho$. We can derive $\Gamma \vdash e_1\rho : \mathbb{0}$ by induction on the premise, thus we can derive $\Gamma \vdash e' : \mathbb{0}$ by using [𝟘].

[$\in_1$] We have $e \equiv (e_1 \in \tau)\ ?\ e_2 : e_3$. There are three cases:
- $e' \equiv (e_1\rho \in \tau)\ ?\ e_2\rho : e_3\rho$ We can easily conclude by induction on the premises.
- $e' \equiv e_2$ We can easily conclude by induction on the second premise.
- $e' \equiv e_3$ This case is impossible. Indeed, it implies that e_1 is a value. As $\Gamma \vdash e_1 : \tau$ (first premise), we can deduce using the property D.9 that $e_1 \in \tau$, which contradicts $e \rightsquigarrow_{\mathsf{Ex}} e_3$.

[$\in_2$] Similar to the previous case.

□

Corollary D.12 (Subject reduction). *If $\Gamma \vdash e : t$ and $e \rightsquigarrow e'$, then $\Gamma \vdash e' : t$.*

Proof. The derivation of the reduction $e \rightsquigarrow e'$ may use several $[\kappa]$ rules, but it must end with a reduction $e_\circ \rightsquigarrow e'_\circ$ that does not use rule $[\kappa]$. As the $\rightsquigarrow_{\mathsf{Ex}}$ semantics and the parallel semantics only differ on the context rule, we also have $e_\circ \rightsquigarrow_{\mathsf{Ex}} e'_\circ$.

Moreover, we have $e' \equiv e\{e'_\circ/e_\circ\}$. Thus, we can conclude by using the previous theorem. □

D.1.4 Progress.

Theorem D.13 (Generalized progress). *If $\Gamma \vdash e : t$ and if there is no evaluation context E and variable x such that $e \equiv E[x]$, then either e is a value or $\exists e'.\ e \rightsquigarrow e'$.*

Proof. We apply all the normalization lemmas above to the derivation of the judgement $\Gamma \vdash e : t$, and we proceed by structural induction on it.

Depending on the last rule used:

[Const] Trivial (e is a value).

[Ax] Impossible case (e cannot be a variable).

[$\leq$] Trivial (by induction on the premise).

[$\wedge$+] Trivial (by induction on one of the premises).

[$\to$I] Trivial (e is a value).

[$\times$I] We have $e \equiv (e_1, e_2)$.
- If e_1 is not a value, we know by applying the induction hypothesis that e_1 can be reduced. Thus, e can also be reduced using the rule $[\kappa]$.
- If e_1 is a value, then we can apply the induction hypothesis on the second premise (as e_1 is a value, we know that $\forall E, x.\ e_2 \not\equiv E[x]$). It gives that either e_2 is a value or it can be reduced. We can easily conclude in both cases (if e_2 is a value, then e is also a value, otherwise, e can be reduced using the rule $[\kappa]$).

[$\to$E] We have $e \equiv e_1 e_2$, with $\Gamma \vdash e_1 : s \to t$ and $\Gamma \vdash e_2 : s$.
- If e_1 is not a value, we know by applying the induction hypothesis that e_1 can be reduced. Thus, e can also be reduced using the rule $[\kappa]$.
- If e_1 is a value, we can apply the property D.9 on it. As $\Gamma \vdash e_1 : \mathbb{0} \to \mathbb{1}$, it gives that $e_1 \in \mathbb{0} \to \mathbb{1}$ and thus $e_1 \equiv \lambda x.\ e_\circ$. Moreover, we can apply the induction hypothesis on the second premise (as e_1 is a value, we know that $\forall E, x.\ e_2 \not\equiv E[x]$). It gives that either e_2 is a value or it can be reduced. We can easily conclude in both cases (if e_2 is a value, then e can be reduced using the rule 58, otherwise, e can be reduced using the rule $[\kappa]$).

[$\times$E$_1$] We have $e \equiv \pi_1 e_\circ$, with $\Gamma \vdash e_\circ : t \times s$. By induction on the premise, we know that $e_\circ$ is either a value or it can be reduced. If $e_\circ$ can be reduced, then e can also be reduced using the rule $[\kappa]$. Otherwise, as $\Gamma \vdash e_\circ : \mathbb{1} \times \mathbb{1}$, we know by using the property D.9 that $e_\circ \in \mathbb{1} \times \mathbb{1}$. Thus, $e_\circ \equiv (v_1, v_2)$ (with v_1 and v_2 two values) and consequently e can be reduced using the rule 59.

[$\times$E$_2$] Similar to the previous case.

[$\vee$+] We have $e \equiv e_\circ\{e'/x\}$, with $\Gamma \vdash e' : \bigvee_{i \in I} t_i$ and $\forall i \in I.\ \Gamma, x : t_i \vdash e_\circ : t$. There are two cases:

- There exists a reduction context E such that $e_\circ \equiv E[x]$. In this case, we know that there is no reduction context E' and variable y such that $e' \equiv E'[y]$, otherwise we would have $e \equiv E[E'[y]]$. Thus, we can apply the induction hypothesis on the first premise. It gives that either e' is a value or it can be reduced. The case where e' is a value can be skipped without loss of generality according to the lemma D.8. Thus, we can assume that e' can be reduced. Consequently, e can also be reduced using the rule $[\kappa]$.
- There is no reduction context E such that $e_\circ \equiv E[x]$. We also know that there is no reduction context E and variable y such that $y \neq x$ and $e_\circ \equiv E[y]$, otherwise we would have $e \equiv E[y]$. Thus, we can apply the induction hypothesis on the second premise. It gives that either $e_\circ$ is a value or it can be reduced. We can easily conclude in both cases (if $e_\circ$ is a value, then e is also a value, and if $e_\circ$ can be reduced, then e can also be reduced).

$[\mathbb{0}]$ We have $e \equiv (e_\circ \in \tau)\,?\,e_1 : e_2$, with $\Gamma \vdash e_\circ : \mathbb{0}$. As values cannot have the type $\mathbb{0}$, we know that $e_\circ$ is not a value. Thus, by induction on the premise, we know that $e_\circ$ can be reduced. Consequently, e can be reduced using the rule $[\kappa]$.

$[\in_1]$ We have $e \equiv (e_\circ \in \tau)\,?\,e_1 : e_2$, with $\Gamma \vdash e_\circ : \tau$. By induction on this premise, we know that $e_\circ$ is either a value or it can be reduced. If $e_\circ$ is a value, then e can be reduced using the rule 61. Otherwise, $e_\circ$ can be reduced and thus e can also be reduced using the rule $[\kappa]$.

$[\in_2]$ Similar to the previous case.

□

Corollary D.14 (Progress). *If $\varnothing \vdash e : t$, then either e is a value or $\exists e'.\ e \not\rightsquigarrow e'$.*

Proof. We can deduce from $\varnothing \vdash e : t$ that there is no evaluation context E and variable x such that $e \equiv E[x]$. Thus, we can apply the generalized progress theorem above. □

D.1.5 Equivalence of the Semantics. See 2.3 for the semantics of the paper.

Property D.15 (Inclusion of $\not\rightsquigarrow$ in $\rightsquigarrow$). *For any e and v, if $e \not\rightsquigarrow^* v$, then $e \rightsquigarrow^* v$. Moreover, for any e, if $e \not\rightsquigarrow^*$ (e diverges with $\not\rightsquigarrow$), then $e \rightsquigarrow^*$ (e diverges with $\rightsquigarrow$).*

Proof. For any e_1 and e_2, we will use the notation $e_1 \rightsquigarrow_{\mathsf{Top}} e_2$ to denote a reduction $e_1 \rightsquigarrow e_2$ that applies at top-level (i.e. under the empty evaluation context). Moreover, we will denote by C an expression with exactly one hole (it is more general than an evaluation context E).

First, we can easily prove by induction the following property:

for any context E and expressions e, e', e'', if $E[e] \overset{e \mapsto e'}{\rightsquigarrow} e''$, then $e'' \equiv E\{e'/e\}[e']$ and $e \rightsquigarrow_{\mathsf{Top}} e'$ and $E[e] \rightsquigarrow E[e']$.

Then, we show that for any context E and expressions $e, e', e'', e_1, \cdots, e_n$, if $E[e] \overset{e \mapsto e'}{\rightsquigarrow} e''$ and $\forall i \in [1\,..\,n].\ e_i \rightsquigarrow_{\mathsf{Top}} e_i'$, then for any C such that $C\{e_1'/e_1\} \cdots \{e_n'/e_n\} \equiv E$, there exists C' such that $C[e] \rightsquigarrow^* C'[e']$ and $C'\{e_1'/e_1\} \cdots \{e_n'/e_n\}\{e'/e\}[e'] \equiv e''$. The idea behind this result is that:

- If C is an evaluation context, we can directly conclude with the property above.
- Otherwise, we can successively reduce in $C[E]$ the expressions e_i such that $\exists E.\ E[e_i] \equiv C[e]$ using the fact that $\forall i \in [1\,..\,n].\ e_i \rightsquigarrow_{\mathsf{Top}} e_i'$, until C becomes an evaluation context.

The lemma we want to prove can easily be deduced from this result. □

Note that the other inclusion is also true, but is not required to prove the safety of our type system.

Theorem D.16 (Type safety). *For any expression e, if $\varnothing \vdash e : t$, then either $e \rightsquigarrow^* v$ with $\varnothing \vdash v : t$ or $e \rightsquigarrow^*$ (e diverges).*

Proof. Straightforward application of D.12, D.14 and D.15. □

D.2 Intermediate Type System

See 3 for the full declarative system and 4 for the full intermediate system.

D.2.1 Soundness.

Lemma D.17. *If $\Gamma \vdash e : t$ is derivable and $x \notin \Gamma$, then $\forall e'.\ \Gamma \vdash e\{e'/x\}$ is derivable.*

Proof. As $x \notin \Gamma$, the derivation of $\Gamma \vdash e : t$ cannot use the rule [Ax] on x, and thus it does not contain any typing derivation for x as a sub-derivation. Thus, we can transform the derivation of $\Gamma \vdash e : t$ into a derivation of $\Gamma \vdash e\{e'/x\}$ by replacing every occurrence of x by e' (straightforward induction). □

Theorem D.18 (Soundness). *If $\Gamma \vdash_{\mathcal{I}} \boldsymbol{e} : t$ then $\Gamma \vdash \lceil \boldsymbol{e} \rceil : t$*

Proof. We proceed by structural induction on the typing derivation of $\Gamma \vdash_{\mathcal{I}} \boldsymbol{e} : t$.
Depending on the last rule used (we use the variable names defined in this rule):

[Const-Int] Trivial.

[Ax-Int] Trivial.

[→I-Int] By induction on the premises, we get $\forall j \in J.\ \Gamma, x : t_j \vdash \lceil \boldsymbol{e} \rceil : s_j$. By applying the rule [→I] on each of these derivations, we get $\forall j \in J.\ \Gamma \vdash \lambda x.\lceil \boldsymbol{e} \rceil : t_j \to s_j$. We conclude by applying the rule [∧+].

[→E-Int] We have $t \simeq t_1 \circ t_2$. According to the definition of $\circ$, we can deduce that $t_1 \leq t_2 \to t$. Moreover, by induction on the premises, we get $\Gamma \vdash \lceil \boldsymbol{e}_1 \rceil : t_1$ and $\Gamma \vdash \lceil \boldsymbol{e}_2 \rceil : t_2$. By applying the [≤] rule, we can derive $\Gamma \vdash \lceil \boldsymbol{e}_1 \rceil : t_2 \to t$. We can then easily conclude with an application of the rule [→E].

[×I-Int] By induction on the premises, we get $\Gamma \vdash \lceil \boldsymbol{e}_1 \rceil : t_1$ and $\Gamma \vdash \lceil \boldsymbol{e}_2 \rceil : t_2$. We conclude by applying the rule [×I].

[×E$_1$-Int] By induction on the premise, we get $\Gamma \vdash \lceil \boldsymbol{e} \rceil : t$. According to the definition of pi_1, we can deduce that $t \leq (\pi_1 t) \times \mathbb{1}$. By applying the [≤] rule, we can derive $\Gamma \vdash \lceil \boldsymbol{e} \rceil : (\pi_1 t) \times \mathbb{1}$. We conclude by applying the rule [×E$_1$].

[×E$_2$-Int] Similar to the previous case.

[𝕆-Int] Similar to the previous case.

[∈$_1$-Int] By induction on the premises, we get $\Gamma \vdash \lceil \boldsymbol{e} \rceil : t_0$ with $t_0 \leq t$ and $\Gamma \vdash \lceil \boldsymbol{e}_1 \rceil : t_1$. By applying the [≤] rule, we can derive $\Gamma \vdash \lceil \boldsymbol{e} \rceil : t$. We conclude by applying the rule [∈$_1$].

[∈$_2$-Int] Similar to the previous case.

[∨$_1$-Int] By induction on the premise, we get $\Gamma \vdash \lceil \boldsymbol{e}_2 \rceil : s$. As $x \notin \Gamma$, we can transform our derivation into a derivation of $\Gamma \vdash \lceil \boldsymbol{e}_2 \rceil\{\lceil \boldsymbol{e}_1 \rceil / x\} : s$ using lemma D.17.

[∨$_2$-Int] By induction on the premises, we get $\Gamma \vdash \lceil \boldsymbol{e}_1 \rceil : \bigvee_{j \in J} t_j$ and $\forall j \in J.\ \Gamma, x : t_j \vdash \lceil \boldsymbol{e}_2 \rceil : s_j$. Using the rule [≤], we can derive $\forall j \in J.\ \Gamma, x : t_j \vdash \lceil \boldsymbol{e}_2 \rceil : \bigvee_{j \in J} s_j$. We conclude by applying the rule [∨+] (it gives a derivation for $\Gamma \vdash \lceil \boldsymbol{e}_2 \rceil\{\lceil \boldsymbol{e}_1 \rceil / x\} : \bigvee_{j \in J} s_j$).

□

D.2.2 Completeness.

See A.8 for all the definitions relative to the canonical form and the MSC-form.

Lemma D.19 (Monotonicity). *If $\Gamma \vdash_{\mathcal{I}} \boldsymbol{e} : t$ and $\Gamma' \leq \Gamma$, then $\Gamma' \vdash_{\mathcal{I}} \boldsymbol{e} : t'$ with $t' \leq t$.*

More generally, in any derivation for $\Gamma \vdash_{\mathcal{I}} \boldsymbol{e} : t$, we can replace any subderivation $\Gamma_\circ \vdash_{\mathcal{I}} \boldsymbol{e}_\circ : t_\circ$ by a derivation $\Gamma_\circ \vdash_{\mathcal{I}} \boldsymbol{e}_\circ : t'_\circ \leq t_\circ$ and still keep a valid derivation for $\Gamma \vdash_{\mathcal{I}} \boldsymbol{e} : t' \leq t$ by doing some minor transformations to the rest of the derivation, which involve:

- *Refinement of some types in the derivation,*
- *Refinement of the splits made by a [∨$_1$] rule (it may imply the removing of some branches and the strengthening of the environment of some other branches),*

- *Use of a [𝕆-Int] rule instead of a [$\in_1$-Int] or [$\in_2$-Int] rule.*

Proof. Straightforward induction on the typing derivation of $\Gamma \vdash_I \boldsymbol{e} : t$. □

Lemma D.20 (Intersection). *If* $\Gamma \vdash_I \boldsymbol{e} : t_1$ *and* $\Gamma \vdash_I \boldsymbol{e} : t_2$, *then* $\Gamma \vdash_I \boldsymbol{e} : t \leq t_1 \wedge t_2$.

Proof. It is a straightforward induction on the typing derivations of $\Gamma \vdash_I \boldsymbol{e} : t_1$ and $\Gamma \vdash_I \boldsymbol{e} : t_2$. We use the monotonicity lemma (D.19) when needed.

Here is the transformation to apply when both $\Gamma \vdash_I \boldsymbol{e} : t_1$ and $\Gamma \vdash_I \boldsymbol{e} : t_2$ use [$\vee_2$-Int] as last rule.

$$[\vee_2\text{-Int}]\ \frac{\dfrac{A}{\Gamma \vdash_I \boldsymbol{a} : \bigvee_{j\in J} t_j} \qquad \dfrac{B_j}{\Gamma, x : t_j \vdash_I \boldsymbol{\kappa} : s_j}}{\Gamma \vdash_I \mathtt{bind}\, x = \boldsymbol{a}\, \mathtt{in}\, \boldsymbol{\kappa} : \bigvee_{j\in J} s_j \simeq t} \quad [\vee_2\text{-Int}]\ \frac{\dfrac{A'}{\Gamma \vdash_I \boldsymbol{a} : \bigvee_{j\in J'} t'_j} \qquad \dfrac{B'_j}{\Gamma, x : t'_j \vdash_I \boldsymbol{\kappa} : s'_j}}{\Gamma \vdash_I \mathtt{bind}\, x = \boldsymbol{a}\, \mathtt{in}\, \boldsymbol{\kappa} : \bigvee_{j\in J'} s'_j \simeq t'}$$

$$\downarrow$$

$$[\vee_2\text{-Int}]\ \frac{\dfrac{\text{Derived by induction on } A \text{ and } A'}{\Gamma \vdash_I \boldsymbol{a} : t_\circ \simeq \bigvee_{i\in I} u_i} \qquad \dfrac{\text{Derived by induction on one of the } B_j \text{ and } B'_j}{\Gamma, x : u_i \vdash_I \boldsymbol{\kappa} : v_i \leq t \wedge t'}}{\Gamma \vdash_I \mathtt{bind}\, x = \boldsymbol{a}\, \mathtt{in}\, \boldsymbol{\kappa} : \bigvee_{i\in I} v_i \leq t \wedge t'}$$

$$\text{with } \{u_i\}_{i\in I} = \mathtt{partition}(\{t_j \wedge t_\circ\}_{j\in J} \cup \{t'_j \wedge t_\circ\}_{j\in J'})$$

The case when both $\Gamma \vdash_I \boldsymbol{e} : t_1$ and $\Gamma \vdash_I \boldsymbol{e} : t_2$ use [→I-Int] as last rule is quite similar (the new split to use is partition of the union of the two original splits).

The other cases are straightforward. □

Property D.21. *For any intermediate expression* $\boldsymbol{e}$, $\lceil \mathtt{term}(\llbracket \boldsymbol{e} \rrbracket) \rceil = \lceil \boldsymbol{e} \rceil$.

Proof. Straightforward structural induction on $\boldsymbol{e}$. □

In the following, we extend the function term so that it can take an arbitrary intermediate expression as second argument instead of just a variable.

Lemma D.22. *If* $\Gamma, (x : s) \vdash_I \boldsymbol{e} : t$ *and* $\Gamma \vdash_I \mathtt{term}(\Delta, x) : s$, *then* $\Gamma \vdash_I \mathtt{term}(\Delta, \boldsymbol{e}) : t'$ *with* $t' \leq t$.

Proof. We proceed by induction on the size of Δ.

If $\Delta = \varepsilon$, the property is trivial (we can directly use the rule [Ax-Int]).

Otherwise, we have $\Delta \stackrel{\text{def}}{=} y \mapsto \boldsymbol{a}; \Delta'$ and $\mathtt{term}(\Delta, x) = \mathtt{bind}\, y = \boldsymbol{a}\, \mathtt{in}\, \mathtt{term}(\Delta', x)$. The last rule of the derivation of $\Gamma \vdash_I \mathtt{term}(\Delta, x) : s$ can be:

[$\vee_1$-Int] In this case, we have the premise $\Gamma \vdash_I \mathtt{term}(\Delta', x) : s$ and thus, by induction, we can deduce $\Gamma \vdash_I \mathtt{term}(\Delta', \boldsymbol{e}) : t'$ with $t' \leq t$. We can derive $\Gamma \vdash_I \mathtt{term}(\Delta, \boldsymbol{e}) : t'$ by using the rule [$\vee_1$-Int].

[$\vee_2$-Int] In this case, we have the premises $\Gamma \vdash_I \boldsymbol{a} : \bigvee_{j\in J} t_j$ and $\forall j \in J.\, \Gamma, y : t_j \vdash_I \mathtt{term}(\Delta', x) : s_j$ with $s \simeq \bigvee_{j_i n J} s_j$. As $\Gamma, (x : s) \vdash_I \boldsymbol{e} : t$ and $\forall j \in J.\, s_j \leq s$, we know by monotonicity (D.19) that $\forall j \in J.\, \Gamma, (x : s_j) \vdash_I \boldsymbol{e} : t'_j$ with $t'_j \leq t$. By induction, we can deduce $\forall j \in J.\, \Gamma, y : t_j \vdash_I \mathtt{term}(\Delta', \boldsymbol{e}) : t'_j$. We can derive $\Gamma \vdash_I \mathtt{term}(\Delta, \boldsymbol{e}) : \bigvee_{j\in J} t'_j$ by using the rule [$\vee_2$-Int].

□

Lemma D.23. *If* $\Gamma, (x_1 : s) \vdash_\mathcal{I} \mathsf{term}(\Delta_2, x_2) : t$ *and* $\Gamma \vdash_\mathcal{I} \mathsf{term}(\Delta_1, x_1) : s$, *then* $\Gamma \vdash_\mathcal{I} \mathsf{term}((\Delta_1; \Delta_2), x_2) : t'$ *with* $t' \leq t$.

Proof. Straightforward application of the previous lemma with $\boldsymbol{e} = \mathsf{term}(\Delta_2, x_2)$. □

Property D.24. *If* $\Gamma \vdash_\mathcal{I} \boldsymbol{e} : t$ *then* $\Gamma \vdash_\mathcal{I} \mathsf{term}([\![\boldsymbol{e}]\!]) : t'$ *with* $t' \leq t$.

Proof. We proceed by structural induction on the expression $\boldsymbol{e}$.

c Trivial.

x Trivial.

$\lambda x.\, \boldsymbol{e}$ The last rule of the derivation of $\Gamma \vdash_\mathcal{I} \boldsymbol{e} : t$ is [→I-Int]. By induction on its premises, we get $\forall j \in J.\, \Gamma, x : t_j \vdash_\mathcal{I} \mathsf{term}([\![\boldsymbol{e}]\!]) : s'_j$ with $s'_j \leq s_j$. We can derive $\Gamma \vdash_\mathcal{I} \mathsf{term}([\![\lambda x.\, \boldsymbol{e}]\!]) : \bigwedge_{j\in J} s'_j$ by applying the rules [→I-Int] and [$\vee_2$-Int].

$\pi_1 \boldsymbol{e}$ The last rule of the derivation of $\Gamma \vdash_\mathcal{I} \boldsymbol{e} : t$ is [×E-Int]. By induction on its premise, we get $\Gamma \vdash_\mathcal{I} \mathsf{term}([\![\boldsymbol{e}]\!]) : t'$ with $t' \leq t \leq \mathbb{1} \times \mathbb{1}$ (we use the same variable names as the rule). Let us note $(\Delta, x) \stackrel{\text{def}}{=} [\![\boldsymbol{e}]\!]$. We can trivially derive $\Gamma, x : t' \vdash_\mathcal{I} \mathsf{term}((x_\circ \mapsto \pi_i x), x_\circ) : \pi_1(t')$. Thus, by applying D.23, we can deduce $\Gamma \vdash_\mathcal{I} \mathsf{term}((\Delta; x_\circ \mapsto \pi_i x), x_\circ) : \pi_1(t')$.

$\pi_2 \boldsymbol{e}$ Similar to the previous case.

$\boldsymbol{e}_1 \boldsymbol{e}_2$ The last rule of the derivation of $\Gamma \vdash_\mathcal{I} \boldsymbol{e} : t$ is [→E-Int]. By induction on its premises, we get $\Gamma \vdash_\mathcal{I} \mathsf{term}([\![\boldsymbol{e}_1]\!]) : t'_1$ with $t'_1 \leq t_1 \leq \mathbb{0} \to \mathbb{1}$, and $\Gamma \vdash_\mathcal{I} \mathsf{term}([\![\boldsymbol{e}_2]\!]) : t'_2$ with $t'_2 \leq t_2 \leq \mathsf{dom}(t_1)$ (we use the same variable names as the rule). By monotonicity (D.19) we also have $\Gamma, x_1 : t'_1 \vdash_\mathcal{I} \mathsf{term}([\![\boldsymbol{e}_2]\!]) : t'_2$. Let us note $(\Delta_1, x_1) \stackrel{\text{def}}{=} [\![\boldsymbol{e}_1]\!]$ and $(\Delta_2, x_2) \stackrel{\text{def}}{=} [\![\boldsymbol{e}_2]\!]$. We can trivially derive $\Gamma, x_1 : t'_1, x_2 : t'_2 \vdash_\mathcal{I} \mathsf{term}((x_\circ \mapsto x_1 x_2), x_\circ) : t'_1 \circ t'_2$. Thus, by applying D.23, we can deduce $\Gamma, x_1 : t'_1 \vdash_\mathcal{I} \mathsf{term}((\Delta_2; x_\circ \mapsto x_1 x_2), x_\circ) : t'_1 \circ t'_2$. By applying D.23 again, we can finally deduce $\Gamma \vdash_\mathcal{I} \mathsf{term}((\Delta_1; \Delta_2; x_\circ \mapsto x_1 x_2), x_\circ) : t'_1 \circ t'_2$.

$(\boldsymbol{e}_1, \boldsymbol{e}_2)$ Similar to the previous case.

$\boldsymbol{(e_\circ \in \tau)\ ?\ e_1 : e_2}$ The last rule of the derivation of $\Gamma \vdash_\mathcal{I} \boldsymbol{e} : t$ can be [$\mathbb{0}$-Int], [$\in_1$-Int] or [$\in_2$-Int]. We will only focus on the [$\in_1$-Int] case here, but the other cases use the same ideas.

By induction on the premises of the [$\in_1$-Int] rule, we get $\Gamma \vdash_\mathcal{I} \mathsf{term}([\![\boldsymbol{e}_\circ]\!]) : t'_\circ \leq t_\circ \leq \tau$ and $\Gamma \vdash_\mathcal{I} \mathsf{term}([\![\boldsymbol{e}_1]\!]) : t'_1 \leq t_1$ (we use the same variable names as the rule). By monotonicity (D.19) we also have $\Gamma, x_\circ : t'_\circ \vdash_\mathcal{I} \mathsf{term}([\![\boldsymbol{e}_1]\!]) : t'_1$. Let us note $(\Delta_\circ, x_\circ) \stackrel{\text{def}}{=} [\![\boldsymbol{e}_\circ]\!]$, $(\Delta_1, x_1) \stackrel{\text{def}}{=} [\![\boldsymbol{e}_1]\!]$ and $(\Delta_2, x_2) \stackrel{\text{def}}{=} [\![\boldsymbol{e}_2]\!]$. We can trivially derive $\Gamma, x_\circ : t'_\circ, x_1 : t'_1 \vdash_\mathcal{I} \mathsf{term}((\Delta_2; x \mapsto (x_\circ \in \tau)\ ?\ x_1 : x_2), x) : t'_1$ (we use the rule [$\vee_1$] to skip the definition Δ_2). Thus, by applying D.23, we can deduce $\Gamma, x_\circ : t'_\circ \vdash_\mathcal{I} \mathsf{term}((\Delta_1; \Delta_2; x \mapsto (x_\circ \in \tau)\ ?\ x_1 : x_2), x) : t'_1$. By applying D.23 again, we can finally deduce $\Gamma \vdash_\mathcal{I} \mathsf{term}((\Delta_\circ; \Delta_1; \Delta_2; x \mapsto (x_\circ \in \tau)\ ?\ x_1 : x_2), x) : t'_1$.

$\mathbf{bind}\, x = \boldsymbol{e}_1\, \mathbf{in}\, \boldsymbol{e}_2$ If the last rule of the derivation of $\Gamma \vdash_\mathcal{I} \boldsymbol{e} : t$ is [$\vee_1$-Int], we can derive $\Gamma \vdash_\mathcal{I} \mathsf{term}([\![\boldsymbol{e}_2]\!]) : s'$ with $s' \leq s$ by induction on the premise. We can easily derive $\Gamma \vdash_\mathcal{I} \mathsf{term}([\![\boldsymbol{e}]\!]) : s'$ from that by using the [$\vee_1$-Int] rule.

Now we can suppose that the last rule of the derivation of $\Gamma \vdash_\mathcal{I} \boldsymbol{e} : t$ is [$\vee_2$-Int]. By induction on its premises, we get $\Gamma \vdash_\mathcal{I} \mathsf{term}([\![\boldsymbol{e}_1]\!]) : t'$ with $t' \leq \bigvee_{j\in J} t_j$, as well as $\forall j \in J.\, \Gamma, x : t_j \vdash_\mathcal{I} \mathsf{term}([\![\boldsymbol{e}_2]\!]) : s'_j$ with $s'_j \leq s_j$. Let us note $(\Delta_1, x_1) \stackrel{\text{def}}{=} [\![\boldsymbol{e}_1]\!]$ and $(\Delta_2, x_2) \stackrel{\text{def}}{=} [\![\boldsymbol{e}_2]\!]$. We can trivially derive $\Gamma, x_1 : t' \vdash_\mathcal{I} \mathsf{term}(x \mapsto x_1, x) : t'$. Moreover, from $\forall j \in J.\, \Gamma, x : t_j \vdash_\mathcal{I} \mathsf{term}([\![\boldsymbol{e}_2]\!]) : s'_j$, we can derive by monotonicity (D.19) $\forall j \in J.\, \Gamma, x : t_j \wedge t' \vdash_\mathcal{I} \mathsf{term}(\Delta_2, x_2) : s''_j$ with $s''_j \leq s'_j$. Thus, by using the rule [$\vee_2$-Int], we can derive $\Gamma, x_1 : t' \vdash_\mathcal{I} ((x \mapsto x_1, \Delta_2), x_2) : \bigvee_{j\in J} s''_j$. By applying D.23, we can deduce $\Gamma \vdash_\mathcal{I} ((\Delta_1, x \mapsto x_1, \Delta_2), x_2) : \bigvee_{j\in J} s''_j$.

□

Property D.25 (Equivalence of MSC-forms). *If* $\boldsymbol{\kappa}_1$ *and* $\boldsymbol{\kappa}_2$ *are two MSC-forms and* $\lceil \boldsymbol{\kappa}_1 \rceil \equiv_\alpha \lceil \boldsymbol{\kappa}_2 \rceil$, *then* $\boldsymbol{\kappa}_1 \equiv_\kappa \boldsymbol{\kappa}_2$.

Proof. Let $e \equiv_\alpha \lceil \boldsymbol{\kappa}_1 \rceil \equiv_\alpha \lceil \boldsymbol{\kappa}_2 \rceil$. Without loss of generality, we can suppose that every variable in e has a unique name (we can always alpha-rename a variable when there is a conflict). We also suppose that every variable in $\boldsymbol{\kappa}_1$ and $\boldsymbol{\kappa}_2$ (from bindings and abstractions) have a unique name. Let us consider the set S of all the distinct subexpressions of e.

To each binding $\texttt{bind}\, x = a\, \texttt{in}\, \boldsymbol{\kappa}$ in $\boldsymbol{\kappa}_1$ or $\boldsymbol{\kappa}_2$, we associate the expression $E(x)$ obtained by starting from a and recursively inlining the definitions of the variables used (for variables that come from a binding). In other word, we associate to every bound variable the unwinding of its definition.

As $\boldsymbol{\kappa}_1$ and $\boldsymbol{\kappa}_2$ are in MSC-form, we know according to the property 4 of the MSC-form that every binding is used later. Thus, for every binding $\texttt{bind}\, x = a\, \texttt{in}\, \boldsymbol{\kappa}$, we know that $E(x)$ will appear in e and thus $E(x) \in S$.

From the properties 1 and 2 of the MSC-form definition, we can deduce that for every binding $\texttt{bind}\, x = a\, \texttt{in}\, \boldsymbol{\kappa}$ in $\boldsymbol{\kappa}_1$ or $\boldsymbol{\kappa}_2$, $E(x)$ is unique (there is no other binding $\texttt{bind}\, y = a'\, \texttt{in}\, \boldsymbol{\kappa}'$ such that $E(x) = E(y)$). It can be easily proved by induction on the number of bindings in the context of our binding $\texttt{bind}\, x = a\, \texttt{in}\, \boldsymbol{\kappa}$. From that, we can deduce that there is a one-to-one correspondence between the bindings of $\boldsymbol{\kappa}_1$ and the elements of S, and between the bindings of $\boldsymbol{\kappa}_2$ and the elements of S.

Thus, $\boldsymbol{\kappa}_1$ and $\boldsymbol{\kappa}_2$ have the exact same bindings modulo alpha-renaming (each binding corresponding to an expression of S). Consequently, the only difference between $\boldsymbol{\kappa}_1$ and $\boldsymbol{\kappa}_2$ is the location of these bindings. In particular, each binding is localized by:

- The lambda-abstraction it is in (if any) and
- The relative order of the binding (with respect to the other bindings) in this lambda-abstraction (or at top-level)

The property 3 of the MSC-form definition ensures that every binding is located in the outermost lambda-abstraction possible: a binding can only be nested inside a lambda-abstraction if its definition depends (directly or not) on the variable introduced by this abstraction.

Finally, the only difference between $\boldsymbol{\kappa}_1$ and $\boldsymbol{\kappa}_2$ is the relative order between the independent bindings that are in the same lambda-abstraction (or at top-level). This order can be rearranged with the rewriting rule 22 of the equivalence relation $\equiv_\kappa$, thus we have $\boldsymbol{\kappa}_1 \equiv_\kappa \boldsymbol{\kappa}_2$. □

Lemma D.26. *Let $\boldsymbol{e}_1, \boldsymbol{e}_2, C, \Gamma$ and t. If $\forall \Gamma_\circ \forall t_\circ.\ \Gamma_\circ \vdash_\mathcal{I} \boldsymbol{e}_1 : t_\circ \Rightarrow \Gamma_\circ \vdash_\mathcal{I} \boldsymbol{e}_2 : t'_\circ \leq t_\circ$ and if $\Gamma \vdash_\mathcal{I} C[\boldsymbol{e}_1] : t$, then $\Gamma \vdash_\mathcal{I} C[\boldsymbol{e}_2] : t' \leq t$.*

Proof. We can transform the derivation $\Gamma \vdash_\mathcal{I} C[\boldsymbol{e}_1] : t$ into a derivation for $\Gamma \vdash_\mathcal{I} C[\boldsymbol{e}_2] : t'$:

(1) We replace the relevant occurrence of $\boldsymbol{e}_1$ by $\boldsymbol{e}_2$ at the root of the derivation.
(2) We propagate this change. We stop when we reach a subderivation of the form $\Gamma' \vdash_\mathcal{I} \boldsymbol{e}_1 : s$ that should be transformed into $\Gamma' \vdash_\mathcal{I} \boldsymbol{e}_2 : s$.
(3) For each such subderivation $\Gamma' \vdash_\mathcal{I} \boldsymbol{e}_1 : s$, we replace it by a subderivation for $\Gamma' \vdash_\mathcal{I} \boldsymbol{e}_2 : s'$ with $s' \leq s$ (we use the hypothesis $\forall \Gamma_\circ \forall t_\circ.\ \Gamma_\circ \vdash_\mathcal{I} \boldsymbol{e}_1 : t_\circ \Rightarrow \Gamma_\circ \vdash_\mathcal{I} \boldsymbol{e}_2 : t'_\circ \leq t_\circ$).
(4) By monotonicity (D.19), we can propagate the changes on the resulting type and we get a derivation for $\Gamma' \vdash_\mathcal{I} C[\boldsymbol{e}_2] : t'$ with $t' \leq t$.

□

Property D.27. *If $\Gamma \vdash_\mathcal{I} \boldsymbol{\kappa} : t$ and $\boldsymbol{\kappa} \equiv_\kappa \boldsymbol{\kappa}'$, then $\exists t' \leq t$ such that $\Gamma \vdash_\mathcal{I} \boldsymbol{\kappa}' : t'$.*

Proof. First, let's assume the equivalence rule of $\equiv_\kappa$ only applies at top-level (i.e. not under an arbitrary context). We have a case for each rule:

22 (→) If the derivation $\Gamma \vdash_\mathcal{I} \texttt{bind}\, x_1 = \boldsymbol{a}_1\, \texttt{in}\, \texttt{bind}\, x_2 = \boldsymbol{a}_2\, \texttt{in}\, \boldsymbol{\kappa} : t$ uses the rule [$\vee_1$-Int] for at least one of the two bindings, then the transformation into a derivation for $\Gamma \vdash_\mathcal{I} \texttt{bind}\, x_2 = \boldsymbol{a}_2\, \texttt{in}\, \texttt{bind}\, x_1 = \boldsymbol{a}_1\, \texttt{in}\, \boldsymbol{\kappa} : t'$ is trivial.

Otherwise, we can use the following transformation:

$$[\vee_2\text{-Int}]\ \dfrac{[\vee_2\text{-Int}]\ \dfrac{\dfrac{A}{\Gamma \vdash_{\mathcal{I}} \boldsymbol{a}_1 : \bigvee_{j\in J} t_j} \qquad [\vee_2\text{-Int}]\ \dfrac{\dfrac{B_j}{\Gamma, x_1 : t_j \vdash_{\mathcal{I}} \boldsymbol{a}_2 : \bigvee_{k\in K_j} t'_{j,k}} \qquad \dfrac{C_{j,k}}{\Gamma, x_1 : t_j, x_2 : t'_{j,k} \vdash_{\mathcal{I}} \boldsymbol{\kappa} : s'_{j,k}}}{\Gamma, x_1 : t_j \vdash_{\mathcal{I}} \mathtt{bind}\, x_2 = \boldsymbol{a}_2\, \mathtt{in}\, \boldsymbol{\kappa} \ : \bigvee_{k\in K_j} s'_{j,k} \simeq s_j}}{\Gamma \vdash_{\mathcal{I}} \mathtt{bind}\, x_1 = \boldsymbol{a}_1\, \mathtt{in}\, \mathtt{bind}\, x_2 = \boldsymbol{a}_2\, \mathtt{in}\, \boldsymbol{\kappa} \ : \bigvee_{j\in J} s_j \simeq t}$$

$$\downarrow$$

$$[\vee_2\text{-Int}]\ \dfrac{[\vee_2\text{-Int}]\ \dfrac{\dfrac{\text{Easily derived from any of the } B_j}{\Gamma \vdash_{\mathcal{I}} \boldsymbol{a}_2 : \bigvee_{i\in I} u_i} \qquad \dfrac{\dfrac{\text{Easily derived from } A}{\Gamma, x_2 : u_i \vdash_{\mathcal{I}} \boldsymbol{a}_1 : \bigvee_{j\in J} t_j} \qquad \dfrac{\text{Easily derived by monotonicity from one of the } C_{j,k}}{\Gamma, x_2 : u_i, x_1 : t_j \vdash_{\mathcal{I}} \boldsymbol{\kappa} : v_{i,j} \le s_j}}{\Gamma, x_2 : u_i \vdash_{\mathcal{I}} \mathtt{bind}\, x_1 = \boldsymbol{a}_1\, \mathtt{in}\, \boldsymbol{\kappa} \ : \bigvee_{j\in J} v_{i,j} \le t}}{\Gamma \vdash_{\mathcal{I}} \mathtt{bind}\, x_2 = \boldsymbol{a}_2\, \mathtt{in}\, \mathtt{bind}\, x_1 = \boldsymbol{a}_1\, \mathtt{in}\, \boldsymbol{\kappa} \ : \bigvee_{i\in I} \bigvee_{j\in J} v_{i,j} \le t}$$

$$\text{with } \{u_i\}_{i\in I} = \mathtt{partition}(\{t'_{j,k} \mid j \in J, k \in K_j\})$$

22 (←) Similar to the other direction (the rule is symmetric).

The general case (where the equivalence rule can apply under an arbitrary context) can be deduced by an immediate application of the lemma D.26. □

Property D.28. *If* $\boldsymbol{\kappa} \equiv_\kappa \boldsymbol{\kappa}'$, *then* $\lceil \boldsymbol{\kappa} \rceil \equiv_\alpha \lceil \boldsymbol{\kappa}' \rceil$.

Proof. First, let's assume the rule 22 applies at top-level on the expression $\mathtt{bind}\, x_1 = \boldsymbol{a}_1\, \mathtt{in}\, \mathtt{bind}\, x_2 = \boldsymbol{a}_2\, \mathtt{in}\, \boldsymbol{\kappa}$. As $x_1 \notin \mathrm{fv}(\boldsymbol{a}_2)$ and $x_2 \notin \mathrm{fv}(\boldsymbol{a}_1)$, we have $\boldsymbol{\kappa}\{\boldsymbol{a}_1/x_1\}\{\boldsymbol{a}_2/x_2\} = \boldsymbol{\kappa}\{\boldsymbol{a}_2/x_2\}\{\boldsymbol{a}_1/x_1\}$ and thus the unwinding remains unchanged.

The general case can easily be deduced with the observation that $\forall C, \boldsymbol{\kappa}_1, \boldsymbol{\kappa}_2.\ \lceil \boldsymbol{\kappa}_1 \rceil \equiv_\alpha \lceil \boldsymbol{\kappa}_2 \rceil \Rightarrow \lceil C[\boldsymbol{\kappa}_1] \rceil \equiv_\alpha \lceil C[\boldsymbol{\kappa}_2] \rceil$ □

In the following, we use the notation $\boldsymbol{\varphi}$ to designate either an atom $\boldsymbol{a}$ or a canonical expression $\boldsymbol{\kappa}$.

Lemma D.29. *If* $\Gamma \vdash_{\mathcal{I}} \boldsymbol{\varphi} : t$ *and* $\boldsymbol{\varphi} \dashrightarrow \boldsymbol{\varphi}'$, *then* $\exists t' \le t$ *such that* $\Gamma \vdash_{\mathcal{I}} \boldsymbol{\varphi}' : t'$.

Proof. First, let's assume that the $\dashrightarrow$ rule applies at top-level (i.e. not under an arbitrary context). We have a case for each rewriting rule:

23 If the derivation $\Gamma \vdash_{\mathcal{I}} \mathtt{bind}\, x_1 = \boldsymbol{a}_1\, \mathtt{in}\, \mathtt{bind}\, x_2 = \boldsymbol{a}_2\, \mathtt{in}\, \boldsymbol{\kappa} \ : t$ uses the rule [$\vee_1$-Int] for at least one of the two bindings, then the transformation into a derivation for $\Gamma \vdash_{\mathcal{I}} \mathtt{bind}\, x_1 = \boldsymbol{a}_1\, \mathtt{in}\, \boldsymbol{\kappa}\{x_1/x_2\} \ : t'$ is trivial.

Otherwise, we can use the following transformation:

$$[\vee_2\text{-Int}]\ \dfrac{[\vee_2\text{-Int}]\ \dfrac{\dfrac{A}{\Gamma \vdash_{\mathcal{I}} \boldsymbol{a}_1 : \bigvee_{j\in J} t_j}\qquad \dfrac{\dfrac{B_j}{\Gamma, x_1 : t_j \vdash_{\mathcal{I}} \boldsymbol{a}_2 : \bigvee_{k\in K_j} t'_{j,k}}\qquad \dfrac{C_{j,k}}{\Gamma, x_1 : t_j, x_2 : t'_{j,k} \vdash_{\mathcal{I}} \boldsymbol{\kappa} : s'_{j,k}}}{\Gamma, x_1 : t_j \vdash_{\mathcal{I}} \mathtt{bind}\, x_2 = \boldsymbol{a}_2 \,\mathtt{in}\, \boldsymbol{\kappa} \ : \bigvee_{k\in K_j} s'_{j,k} \simeq s_j}}{\Gamma \vdash_{\mathcal{I}} \mathtt{bind}\, x_1 = \boldsymbol{a}_1 \,\mathtt{in}\, \mathtt{bind}\, x_2 = \boldsymbol{a}_2 \,\mathtt{in}\, \boldsymbol{\kappa} \ : \bigvee_{j\in J} s_j \simeq t}$$

$$\downarrow$$

$$[\vee_2\text{-Int}]\ \dfrac{\dfrac{A}{\Gamma \vdash_{\mathcal{I}} \boldsymbol{a}_1 : \bigvee_{i\in I} u_i}\qquad \dfrac{\text{Easily derived by monotonicity from one of the } C_{j,k}}{\Gamma, x_1 : u_i \vdash_{\mathcal{I}} \boldsymbol{\kappa}\{x_1/x_2\} : v_i \le t}}{\Gamma \vdash_{\mathcal{I}} \mathtt{bind}\, x_1 = \boldsymbol{a}_1 \,\mathtt{in}\, \boldsymbol{\kappa}\{x_1/x_2\} \ : \bigvee_{i\in I} v_i \le t}$$

$$\text{with } \{u_i\}_{i\in I} = \mathtt{partition}(\{t_j\}_{j\in J} \cup \{t'_{j,k} \mid j \in J, k \in K_j\})$$

24 If the derivation $\Gamma \vdash_{\mathcal{I}} \mathtt{bind}\, x = \boldsymbol{a} \,\mathtt{in}\, \boldsymbol{\kappa} : t$ uses the rule [$\vee_1$-Int] for the bind, then the transformation into a derivation for $\Gamma \vdash_{\mathcal{I}} \boldsymbol{\kappa} : t$ is trivial.
Otherwise, let us consider one of the premise $\Gamma, x : t_j \vdash_{\mathcal{I}} \boldsymbol{\kappa} : s_j$. As $x \notin \mathrm{fv}(\boldsymbol{\kappa})$, this derivation does not use the rule [Ax-Int] on x. Thus, we can easily transform it into a derivation of $\Gamma \vdash_{\mathcal{I}} \boldsymbol{\kappa} : s_j$.

25 If the derivation $\Gamma \vdash_{\mathcal{I}} \lambda x.(\mathtt{bind}\, y = x \,\mathtt{in}\, \boldsymbol{\kappa}) : t$ uses the rule [$\vee_1$-Int] for the bind, then the transformation into a derivation for $\Gamma \vdash_{\mathcal{I}} \lambda x.(\boldsymbol{\kappa}\{x/y\}) : t'$ is trivial.
Otherwise, we can use the following transformation:

$$[\to\text{I-Int}]\ \dfrac{[\vee_2\text{-Int}]\ \dfrac{[\text{Ax-Int}]\ \dfrac{}{\Gamma, x : t_j \vdash_{\mathcal{I}} x : \bigvee_{k\in K_j} t'_{j,k}}\qquad \dfrac{(\forall j \in J)\quad \dfrac{A_{j,k}}{\Gamma, x : t_j, y : t'_{j,k} \vdash_{\mathcal{I}} \boldsymbol{\kappa} : s'_{j,k}}}{\Gamma, x : t_j \vdash_{\mathcal{I}} \mathtt{bind}\, y = x \,\mathtt{in}\, \boldsymbol{\kappa} \ : \bigvee_{k\in K_j} s'_{j,k} \simeq s_j}}{\Gamma \vdash_{\mathcal{I}} \lambda x.(\mathtt{bind}\, y = x \,\mathtt{in}\, \boldsymbol{\kappa}) : \bigwedge_{j\in J} t_j \to s_j \simeq t}$$

$$\downarrow$$

$$[\to\text{I-Int}]\ \dfrac{(\forall i \in I)\qquad \dfrac{\text{Easily derived by D.20 from some of the } A_{j,k}}{\Gamma, x : u_i \vdash_{\mathcal{I}} \boldsymbol{\kappa}\{x/y\} : v_i \le \bigwedge\{s_j \mid j \in J \text{ s.t. } u_i \le t_j\}}}{\Gamma \vdash_{\mathcal{I}} \lambda x.(\boldsymbol{\kappa}\{x/y\}) : \bigwedge_{i\in I} u_i \to v_i \le t}$$

$$\text{with } \{u_i\}_{i\in I} = \mathtt{partition}(\{t_j\}_{j\in J} \cup \{t'_{j,k} \mid j \in J, k \in K_j\})$$

26 This case is similar to the case 23.

27 For the sake of simplicity, we will consider a simplified version of this rule: $\lambda x.(\mathtt{bind}\, y = \boldsymbol{a} \,\mathtt{in}\, \boldsymbol{\kappa}) \dashrightarrow \mathtt{bind}\, y = \boldsymbol{a} \,\mathtt{in}\, \lambda x.\boldsymbol{\kappa}$. The regular rule can then easily be deducted from that by adding a top-level binding on both sides:
$\mathtt{bind}\, x_\circ = \lambda x.(\mathtt{bind}\, y = \boldsymbol{a} \,\mathtt{in}\, \boldsymbol{\kappa}) \,\mathtt{in}\, \boldsymbol{\kappa}_\circ \dashrightarrow \mathtt{bind}\, x_\circ = (\mathtt{bind}\, y = \boldsymbol{a} \,\mathtt{in}\, \lambda x.\boldsymbol{\kappa}) \,\mathtt{in}\, \boldsymbol{\kappa}_\circ$
and then applying the property D.24 on the right side.

If the derivation $\Gamma \vdash_I \lambda x.(\mathtt{bind}\, y = \boldsymbol{a}\, \mathtt{in}\, \boldsymbol{\kappa}) : t$ uses the rule [$\vee_1$-Int] for the bind, then the transformation into a derivation for $\Gamma \vdash_I \mathtt{bind}\, y = \boldsymbol{a}\, \mathtt{in}\, \lambda x.\boldsymbol{\kappa} : t'$ is trivial.
Otherwise, we can use the following transformation:

$$
\dfrac{\dfrac{\dfrac{(\forall j \in J)\quad \dfrac{A_j}{\Gamma, x : t_j \vdash_I \boldsymbol{a} : \bigvee_{k\in K_j} t'_{j,k}} \qquad \dfrac{B_{j,k}}{\Gamma, x : t_j, y : t'_{j,k} \vdash_I \boldsymbol{\kappa} : s'_{j,k}}}{\Gamma, x : t_j \vdash_I \mathtt{bind}\, y = \boldsymbol{a}\, \mathtt{in}\, \boldsymbol{\kappa} : \bigvee_{k\in K_j} s'_{j,k} \simeq s_j}\,[\vee_2\text{-Int}]}{\Gamma \vdash_I \lambda x.(\mathtt{bind}\, y = \boldsymbol{a}\, \mathtt{in}\, \boldsymbol{\kappa}) : \bigwedge_{j\in J} t_j \to s_j \simeq t}\,[\to\text{I-Int}]
$$

$$
\downarrow
$$

$$
\dfrac{\text{Easily derived from any of the } A_j}{\Gamma \vdash_I \boldsymbol{a} : \bigvee_{i\in I} u_i}
$$

$$
\dfrac{\dfrac{(\forall j \in J)\quad \dfrac{\text{Easily derived by monotonicity from one of the } B_{j,k}}{\Gamma, y : u_i, x : t_j \vdash_I \boldsymbol{\kappa} : v_{i,j} \le s_j}}{\Gamma, y : u_i \vdash_I \lambda x.\boldsymbol{\kappa} : \bigwedge_{j\in J} t_j \to v_{i,j} \le t}\,[\to\text{I-Int}]}{\Gamma \vdash_I \mathtt{bind}\, y = \boldsymbol{a}\, \mathtt{in}\, \lambda x.\boldsymbol{\kappa} : \bigvee_{i\in I} \bigwedge_{j\in J} t_j \to v_{i,j} \le t}\,[\vee_2\text{-Int}]
$$

$$
\text{with } \{u_i\}_{i\in I} = \mathtt{partition}(\{t'_{j,k} \mid j \in J, k \in K_j\})
$$

The general case (where the rule can apply under an arbitrary context) can be deduced by an application of the lemma D.26. □

Property D.30. *Let $\boldsymbol{\kappa}_1, \boldsymbol{\kappa}_2$ such that $\boldsymbol{\kappa}_1 \dashrightarrow_\kappa \boldsymbol{\kappa}_2$. If $\Gamma \vdash_I \boldsymbol{\kappa}_1 : t$ then $\Gamma \vdash_I \boldsymbol{\kappa}_2 : t' \le t$.*

Proof. Immediate application of D.27 and D.29. □

Property D.31. *If $\boldsymbol{\kappa} \dashrightarrow_\kappa \boldsymbol{\kappa}'$, then $\lceil \boldsymbol{\kappa} \rceil \equiv_\alpha \lceil \boldsymbol{\kappa}' \rceil$.*

Proof. Straightforward: the proof is similar to the one of D.28. □

Property D.32 (Normalization). *There is no infinite chain $\boldsymbol{\kappa}_1 \dashrightarrow_\kappa \boldsymbol{\kappa}_2 \dashrightarrow_\kappa \cdots$*

Proof. Let's suppose such an infinite chain exists.
Let n be the maximal number of nested lambdas in $\boldsymbol{\kappa}_1$. We call depth of a binding the number of nested lambdas it is into (the depth of a binding of $\boldsymbol{\kappa}_1$ is at most n). Let $N_{\boldsymbol{\kappa}}(i)$ be the number of bindings of depth i in an expression $\boldsymbol{\kappa}$.
Let $S(\boldsymbol{\kappa})$ be the following n-uplet: $(N_{\boldsymbol{\kappa}}(n), N_{\boldsymbol{\kappa}}(n-1), \cdots, N_{\boldsymbol{\kappa}}(0))$. Then, the chain $S(\boldsymbol{\kappa}_1)$, $S(\boldsymbol{\kappa}_2)$, $\cdots$ is strictly decreasing with respects to the lexical order, which is impossible. □

Lemma D.33. *If $\boldsymbol{\kappa} \not\dashrightarrow_\kappa$, then $\boldsymbol{\kappa}$ satisfies the properties 1, 3 and 4 of MSC-forms, and satisfies this weaker version of property 2 (aliasing):*
if $\mathtt{bind}\, x = \boldsymbol{a}\, \mathtt{in}\, \boldsymbol{\kappa}'$ is a sub-expression of $\boldsymbol{\kappa}$, then $\boldsymbol{a}$ is either not a variable or a variable in $fv(\boldsymbol{\kappa})$.

Proof. Let us start with the property 3 (extrusion of bindings). We assume that there exists a subexpression $\lambda x.\, \boldsymbol{\kappa}_1$ of $\boldsymbol{\kappa}$ and a subexpression $\mathtt{bind}\, y = \boldsymbol{a}\, \mathtt{in}\, \boldsymbol{\kappa}_2$ of $\boldsymbol{\kappa}_1$ such that $\mathrm{fv}(\boldsymbol{a}) \subseteq \mathrm{fv}(\lambda x.\, \boldsymbol{\kappa}_1)$. Then, the definition $\boldsymbol{a}$ cannot depend on any variable defined inside $\lambda x.\, \boldsymbol{\kappa}_1$ (including x), otherwise this variable would be in $\mathrm{fv}(\boldsymbol{a})$ and not in $\mathrm{fv}(\lambda x.\, \boldsymbol{\kappa}_1)$. Thus, we can reorder the binding y in the first

position of its containing lambda-abstraction, and then apply the rule 27 on it, which contradicts $\boldsymbol{\kappa} \not\rightarrow_\kappa$.

Now let's assume that there are two bindings with the definitions $\boldsymbol{a}_1$ and $\boldsymbol{a}_2$ such that $\lceil \boldsymbol{a}_1 \rceil \equiv_\alpha \lceil \boldsymbol{a}_2 \rceil$. By structural induction on the context of these two bindings, we can easily find two bindings with the definitions $\boldsymbol{a}'_1$ and $\boldsymbol{a}'_2$ such that $\boldsymbol{a}'_1 \equiv_\alpha \boldsymbol{a}'_2$. As we know that the property 3 is satisfied, we know that every binding is located in the body of the outermost lambda-abstraction possible (or at top-level), depending on the free variables of its definition. This means that our two definitions of $\boldsymbol{a}'_1$ and $\boldsymbol{a}'_2$ are not separated by a lambda-abstraction. Thus, we can reorder them to be the one next to the other, and then we can apply the rule 23 on them, which contradicts $\boldsymbol{\kappa} \not\rightarrow_\kappa$. Thus, the property 1 is also satisfied.

The property 4 is trivial: any binding that does not satisfy this property can directly be eliminated with the rule 24.

We finish with the weaker version of the property 2. Let us assume that there is a binding $\texttt{bind}\, x = y \,\texttt{in}\, \boldsymbol{\kappa}'$ with $y \notin \text{fv}(\boldsymbol{\kappa})$. It means that there exists a lambda abstraction or a binding that introduce the variable y. As the property 3 is satisfied, we know that these two variables are not separated by a lambda-abstraction, and thus we can reorder them to be the one next to the other. We can then apply the rule 26 or 25 depending whether y is introduced by a binding or a lambda-abstraction, which contradicts $\boldsymbol{\kappa} \not\rightarrow_\kappa$. □

Corollary D.34. *If $\boldsymbol{\kappa} \not\rightarrow_\kappa$ and $\boldsymbol{\kappa}$ is closed ($fv(\boldsymbol{\kappa}) = \varnothing$), then $\boldsymbol{\kappa}$ is in MSC form.*

Proof. Direct application of D.33. □

Property D.35 (Confluence). *Let $\boldsymbol{\kappa}_1, \boldsymbol{\kappa}'_1, \boldsymbol{\kappa}_2$ and $\boldsymbol{\kappa}'_2$ such that $\boldsymbol{\kappa}_1 \equiv_\kappa \boldsymbol{\kappa}'_1$, $\boldsymbol{\kappa}_1 \dashrightarrow_\kappa \boldsymbol{\kappa}_2$ and $\boldsymbol{\kappa}'_1 \dashrightarrow_\kappa \boldsymbol{\kappa}'_2$. Then, there exists $\boldsymbol{\kappa}_3$ and $\boldsymbol{\kappa}'_3$ such that $\boldsymbol{\kappa}_3 \equiv_\kappa \boldsymbol{\kappa}'_3$, $\boldsymbol{\kappa}_2 \dashrightarrow^*_\kappa \boldsymbol{\kappa}_3$ and $\boldsymbol{\kappa}'_2 \dashrightarrow^*_\kappa \boldsymbol{\kappa}'_3$.*

Proof. Immediate application of D.32 (normalization), D.33 (terms that cannot be rewritten using $\dashrightarrow_\kappa$ are in MSC-form) and D.25 (equivalence of MSC-forms). □

Lemma D.36. *Let Γ, $\boldsymbol{e}$ and t such that $\Gamma \vdash_\mathcal{I} \boldsymbol{e} : t$. Let ρ be a substitution that associates to each variable in $fv(\boldsymbol{e})$ a new (unique) name. Let C be a context that defines, for each variable x in $fv(\boldsymbol{e})$, the binding $\texttt{bind}\, \rho(x) = x \,\texttt{in}\, \cdots$ (it defines an alias for all variables in $fv(\boldsymbol{e})$).*

Then, there exists $\boldsymbol{\kappa}$ an expression in MSC-form and t' a type such that $\lceil C[\boldsymbol{\kappa}] \rceil \equiv_\alpha \lceil \boldsymbol{e} \rceil$, $\Gamma \vdash_\mathcal{I} C[\boldsymbol{\kappa}\rho] : t'$ and $t' \leq t$. Note that all possible such expressions $C[\boldsymbol{\kappa}\rho]$ are equivalent with respect to $\equiv_\kappa$.

Proof. From $\Gamma \vdash_\mathcal{I} \boldsymbol{e} : t$, we apply D.24 and D.21 so that we get $\boldsymbol{\kappa}$ such that $\lceil \boldsymbol{\kappa} \rceil = \lceil \boldsymbol{e} \rceil$ and $\Gamma \vdash_\mathcal{I} \boldsymbol{\kappa} : t' \leq t$.

Then we apply D.30, D.31 and D.33 to get C' and $\boldsymbol{\kappa}'$ such that $\lceil C'[\boldsymbol{\kappa}'] \rceil = \lceil \boldsymbol{e} \rceil$ and $\Gamma \vdash_\mathcal{I} C'[\boldsymbol{\kappa}'] : t'' \leq t$, with $\boldsymbol{\kappa}'$ an MSC-form and C' a context that optionally defines an alias for some variables in $\text{fv}(\boldsymbol{e})$.

We can easily derive $\Gamma \vdash_\mathcal{I} C[(C'[\boldsymbol{\kappa}'])\rho] : t'' \leq t$ from that just by applying ρ to the derivation tree and by adding additional aliases at top-level for the new variables in ρ (these additional bindings can be typed using $[\vee_1\text{-Int}]$ when the aliased variable is not in Γ, and otherwise using $[\vee_2\text{-Int}]$ with J a singleton).

Now, we can derive $\Gamma \vdash_\mathcal{I} C[\boldsymbol{\kappa}'\rho] : t''' \leq t$ by merging the aliases defined by C' and those defined by C using the rule 26 (see lemma D.29).

Finally, note that for a given C such as in the statement of the lemma, all the expressions $C[\boldsymbol{\kappa}'\rho]$ with $\boldsymbol{\kappa}'$ a MSC-form such that $\lceil C[\boldsymbol{\kappa}'\rho] \rceil = \lceil \boldsymbol{e} \rceil$ are equivalent with respect to $\equiv_\kappa$ (quite straightforward by using D.25). □

Theorem D.37 (Completeness of the MSC form). *If $\vdash_\mathcal{I} \boldsymbol{e} : t$ and if $\boldsymbol{\kappa}$ is a maximal sharing canonical form such that $\lceil \boldsymbol{\kappa} \rceil \equiv_\alpha \lceil \boldsymbol{e} \rceil$, then $\exists t'$ such that $t' \leq t$ and $\vdash_\mathcal{I} \boldsymbol{\kappa} : t'$.*

Proof. Direct application of D.36. □

Theorem D.38 (Completeness of the intermediate type system). *If* $\Gamma \vdash e : t$ *then* $\exists \boldsymbol{e}', t'$ *such that* $\lceil \boldsymbol{e}' \rceil \equiv_\alpha e$, $t' \leq t$, *and* $\Gamma \vdash_\mathcal{I} \boldsymbol{e}' : t'$

Proof. We apply all the normalization lemmas D.5, D.6, D.7 and D.8 to the derivation of the judgement $\Gamma \vdash e : t$, and we proceed by structural induction on it.

Depending on the last rule used (we use the variable names defined in this rule):

[Const] Trivial.

[Ax] Trivial.

[≤] Trivial (by induction on the premise).

[→I] By induction (application of the rule [→I-Int] with $J = \{t_1\}$).

[→E] By induction on the premises, we get $\Gamma \vdash_\mathcal{I} \boldsymbol{e}_1 : s_1 \leq t_1 \to t_2$ and $\Gamma \vdash_\mathcal{I} \boldsymbol{e}_2 : s_2 \leq t_1$ with $\lceil \boldsymbol{e}_1 \rceil \equiv_\alpha e_1$ and $\lceil \boldsymbol{e}_2 \rceil \equiv_\alpha e_2$. According to the definition of $\circ$ (and by monotonicity), we have $s_1 \circ s_2 \leq (t_1 \to t_2) \circ t_1 \leq t_2$. Thus, we can conclude with an application of the rule [→E-Int].

[×I] By induction (application of the rule [×I-Int]).

[×E$_1$] By induction on the premise, we get $\Gamma \vdash_\mathcal{I} \boldsymbol{e} : s \leq t_1 \times t_2$ with $\lceil \boldsymbol{e} \rceil \equiv_\alpha e$. According to the definition of π_1 (and by monotonicity), we have $\pi_1 s \leq \pi_1(t_1 \times t_2) \leq t_1$. Thus, we can conclude with an application of the rule [×E-Int].

[×E$_2$] Similar to the previous case.

[∧+] Thanks to the lemma D.6, we know that the premises of this rule are applications of [→I]. Moreover, by induction, we have $\forall i \in I.\ \Gamma \vdash_\mathcal{I} \boldsymbol{e}_i : t'_i \leq t_i$ with $\lceil \boldsymbol{e}_i \rceil \equiv_\alpha e$.
By applying the lemma D.36, we can derive $\forall i \in I. \Gamma \vdash_\mathcal{I} \boldsymbol{\kappa} : t'_i \leq t_i$ with $\lceil \boldsymbol{\kappa} \rceil \equiv_\alpha e$ and $\boldsymbol{\kappa}$ being a MSC-form preceded by some aliasing. We can conclude with an application of the rule [→I-Int] with $J = I$.

[∨+] We have $e = e_\circ\{e'/x\}$. By induction on the premises, we have $\Gamma \vdash_\mathcal{I} \boldsymbol{e}' : t' \leq \bigvee_{i \in I} t_i$ with $\lceil \boldsymbol{e}' \rceil \equiv_\alpha e'$ and $\forall i \in I.\ \Gamma, x : t_i \vdash_\mathcal{I} \boldsymbol{e}_i : s_i \leq t$ with $\forall i \in I.\ \lceil \boldsymbol{e}_i \rceil \equiv_\alpha e_\circ$.
By applying the lemma D.36, we can derive $\forall i \in I. \Gamma, x : t_i \vdash_\mathcal{I} \boldsymbol{\kappa} : s'_i \leq s_i \leq t$ with $\lceil \boldsymbol{\kappa} \rceil \equiv_\alpha e_\circ$ and $\boldsymbol{\kappa}$ being a MSC-form preceded by some aliasing.
By monotonicity (D.19), we have $\forall i \in I.\ \Gamma, x : (t_i \wedge t') \vdash_\mathcal{I} \boldsymbol{\kappa} : s''_i \leq t$.
Let us consider the intermediate expression $\boldsymbol{e} = \mathtt{bind}\, x = e' \,\mathtt{in}\, \boldsymbol{\kappa}$. We have $\lceil \boldsymbol{e}' \rceil \equiv_\alpha e$. Moreover, we can derive $\Gamma \vdash \boldsymbol{e} : \bigvee_{i \in I} s''_i \leq t$ by using the rule [∨$_2$-Int].

[𝟘] By induction (application of the rule [𝟘-Int]).

[∈$_1$] By induction (application of the rule [∈$_1$-Int]).

[∈$_2$] By induction (application of the rule [∈$_2$-Int]).

□

D.3 Algorithmic Type System

See 4 for the full intermediate system and A.9 for the full algorithmic system.

Theorem D.39 (Soundness of the algorithmic type system). *If* $\Gamma \vdash_{\mathcal{A}} \kappa : t$ *then* $\Gamma \vdash_{\mathcal{I}} \langle\kappa\rangle : t$.

Proof. This direction is trivial: all the rules of the algorithmic system have an equivalent in the intermediate system. For the rules [$\vee_2$-Int] and [$\to$I-Int], the splits $\{t_j\}_{j\in J}$ to choose correspond to the ones determined by the annotations in the corresponding rule [$\vee_2$-Alg] or [$\to$I-Alg]. □

Lemma D.40. *If* $\Gamma \vdash_{\mathcal{I}} \boldsymbol{e} : t$, *then there exists a derivation of* $\Gamma \vdash_{\mathcal{I}} \boldsymbol{e} : t' \leq t$ *such that, for every application of a rule [*$\to$*I-Int] or [*$\vee_2$*I-Int], the set of types* $\{t_j\}_{j\in J}$ *is disjoint* ($\forall j, j' \in J.\ j \neq j' \Rightarrow t_j \wedge t_j$).

Proof. Let us suppose there is an application of [$\to$I-Int] or [$\vee_2$-Int] that uses a set of types $\{t_j\}_{j\in J}$ that does not satisfy the property. We will transform the derivation so that a new set of disjoint types $\{t'_j\}_{j\in J'}$ will be used instead.

Let us consider $\{t'_j\}_{j\in J'} = \texttt{partition}(\{t_j\}_{j\in J})$. These types are disjoint and cover the same domain as before. Moreover, by monotonicity (D.19) and by using the lemma D.20, we can derive $\forall j' \in J'.\ \Gamma, x : t'_{j'} \vdash_{\mathcal{I}} \kappa : s'_{j'} \leq \bigwedge_{j\in J \text{ s.t. } s'_{j'}\leq s_j} s_j$ from all the derivations $\forall j \in J.\ \Gamma, x : t_j \vdash_{\mathcal{I}} \kappa : s_j$. Thus, we can update our application of [$\to$I-Int] or [$\vee_2$I-Int] so that it uses the set of types $\{t'_j\}_{j\in J'}$. It might give a smaller resulting type, but by monotonicity we will still be able to deduce $\Gamma \vdash_{\mathcal{I}} \boldsymbol{e} : t' \leq t$.

Note that this transformation does not compromise the disjointness of the types of the other applications of [$\to$I-Int] and [$\vee_2$I-Int], thus we can apply it multiple times until all the rules [$\to$I-Int] and [$\vee_2$I-Int] use disjoint types. □

Theorem D.41 (Completeness of the algorithmic type system). *If* $\boldsymbol{\kappa}$ *is a MSC-form and* $\Gamma \vdash_{\mathcal{I}} \boldsymbol{\kappa} : t$, *then* $\exists\kappa$ *such that* $\langle\kappa\rangle = \boldsymbol{\kappa}$ *and* $\Gamma \vdash_{\mathcal{A}} \kappa : t' \leq t$

Proof. Note that the only difference between the algorithmic system and the intermediate one is that the set of splits $\{t_j\}_{j\in J}$ in the rules [$\to$I-Alg] and [$\vee_2$-Alg] and the choice of whether to use the rule [$\vee_1$-Alg] or [$\vee_2$-Alg] are determined by the annotations contained in κ. Thus, the challenge here will be to annotate κ so that it allows to "replay" the derivation tree of $\Gamma \vdash_{\mathcal{I}} \boldsymbol{\kappa} : t$ with the algorithmic rules.

First, we apply the transformation of the lemma D.40 to the derivation of $\Gamma \vdash_{\mathcal{I}} \boldsymbol{\kappa} : t$ so that we get a derivation D of $\Gamma \vdash_{\mathcal{I}} \boldsymbol{\kappa} : t' \leq t$ that satisfies the property described in the statement of this lemma.

Now, we start from an algorithmic expression κ similar to $\boldsymbol{\kappa}$ but with every binding and lambda annotated by an empty annotation. Each time a rule [$\to$I-Int] is applied in the derivation D (with $\Gamma \vdash_{\mathcal{I}} \lambda x.(\boldsymbol{e}) : t_\circ$ as conclusion), we add to the annotations of x the splits $\{(\Gamma \triangleright t_j)\}_{j\in J}$ (with $\{t_j\}_{j\in J}$ being the set of types used by the rule). We proceed similarly for the applications of [$\vee_2$-Int] in order to annotate the bindings.

The term κ we obtain can be typed with the algorithmic type system: we obtain a derivation very similar to D (every rule application of the derivation D is replaced by a similar application of the corresponding rule of the algorithmic type system). The applications of [$\to$I-Alg] and [$\vee_2$-Alg] will use the same set of types $\{t_j\}_{j\in J}$ as in the derivation D, because:

- $\supseteq$ We have added the annotations $\{\Gamma \triangleright t_j\}_{j\in J}$ to the corresponding variable
- $\subseteq$ Only these annotations will be selected: the annotations we might have added to this variable because of the other applications of [$\vee_2$-Int] or [$\to$I-Int] require a disjoint environment. Indeed, the different applications of [$\vee_2$-Int] or [$\to$I-Int] for a given variable are in different branches and all branches use a disjoint environment Γ thanks to the lemma D.40.

□

D.4 Annotations Reconstruction Algorithm

See B.3 for the full annotations reconstruction algorithm.

We define the following function:

$$\texttt{filter}_\Gamma(A) = \{(\Gamma' \triangleright t') \mid (\Gamma' \triangleright t') \in A, \Gamma' \leq \Gamma\}$$

We extend this function so that it can take an algorithmic expression φ as argument and returns the same expression φ where every annotation A has been replaced by $\texttt{filter}_\Gamma(A)$.

Lemma D.42. *If* $\Gamma \vdash_{\mathcal{R}} \varphi : t \Rightarrow \{\texttt{filter}_\Gamma(\varphi), \{\Gamma\}\}$ *then* $\Gamma \vdash_{\mathcal{A}} \texttt{filter}_\Gamma(\varphi) : t' \leq t$.

Proof. For convenience, let us define $\varphi' = \texttt{filter}_\Gamma(\varphi)$. We proceed by induction on the derivation tree of $\Gamma \vdash_{\mathcal{R}} \varphi : t \Rightarrow \{\varphi', \{\Gamma\}\}$.

[Const] We trivially have $\Gamma \vdash_{\mathcal{A}} \varphi' : \boldsymbol{b}_c \leq t$.

[ConstUntypable] Impossible (it cannot return $\{\varphi', \{\Gamma\}\}$).

[ProjEmpty] We trivially have $\Gamma \vdash_{\mathcal{A}} \varphi' : \mathbb{0} \leq t$.

[Proj$_1$] We know that $\{\Gamma[x :\hat{=} t_i \times s_i]\}_{i\in I} = \{\Gamma\}$. In particular, it means that $\Gamma \in \{\Gamma[x :\hat{=} t_i \times s_i]\}_{i\in I}$ and thus $\exists i \in I.\ \Gamma(x) \leq t_i \times s_i$. As $\forall i \in I.\ t_i \times s_i \leq (t \times \mathbb{1})$, we can derive $\Gamma \vdash_{\mathcal{A}} \varphi' : t' \leq t$.

[Proj$_2$] Similar to the previous case.

[PairEmpty] We trivially have $\Gamma \vdash_{\mathcal{A}} \varphi' : \mathbb{0} \leq t$.

[Pair] We know that $\{\Gamma[x_1 :\hat{=} t_i][x_2 :\hat{=} s_i]\}_{i\in I} = \{\Gamma\}$. In particular, it means that $\Gamma \in \{\Gamma[x_1 :\hat{=} t_i][x_2 :\hat{=} s_i]\}_{i\in I}$ and thus $\exists i \in I.\ \Gamma(x_1) \leq t_i$ and $\Gamma(x_2) \leq s_i$. As $\forall i \in I.\ t_i \times s_i \leq t$, we can derive $\Gamma \vdash_{\mathcal{A}} \varphi' : t' \leq t$.

[CaseEmpty] We trivially have $\Gamma \vdash_{\mathcal{A}} \varphi' : \mathbb{0} \leq t$.

[Case] We know that $\{\Gamma[x :\hat{=} s][x_1 :\hat{=} t], \Gamma[x :\hat{=} \neg s][x_2 :\hat{=} t]\} = \{\Gamma\}$. In particular, it means that $\Gamma \in \{\Gamma[x :\hat{=} s][x_1 :\hat{=} t]\}$ or $\Gamma \in \{\Gamma[x :\hat{=} \neg s][x_2 :\hat{=} t]\}$. Let's consider the first case. We can deduce $\Gamma(x) \leq s$ and $\Gamma(x_1) \leq t$, and thus we have $\Gamma \vdash_{\mathcal{A}} \varphi' : t' \leq t$ (rule [$\in_1$-Alg]). The second case is similar (rule [$\in_2$-Alg]).

[AppREmpty] We trivially have $\Gamma \vdash_{\mathcal{A}} \varphi' : \mathbb{0} \leq t$.

[AppLEmpty] We trivially have $\Gamma \vdash_{\mathcal{A}} \varphi' : \mathbb{0} \leq t$.

[AppR] We know that $\{\Gamma[x_1 :\hat{=} (s_i \wedge \Gamma(x_2)) \to t][x_2 :\hat{=} s_i]\}_{i\in I} = \{\Gamma\}$. In particular, it means that $\Gamma \in \{\Gamma[x_1 :\hat{=} (s_i \wedge \Gamma(x_2)) \to t][x_2 :\hat{=} s_i]\}_{i\in I}$ and thus $\exists i \in I.\ \Gamma(x_1) \leq (s_i \wedge \Gamma(x_2)) \to t$ and $\Gamma(x_2) \leq s_i$. We can deduce that $\Gamma(x_1) \leq \Gamma(x_2) \to t$ and thus we can derive $\Gamma \vdash_{\mathcal{A}} \varphi' : t' \leq t$.

[AppL] If this rule apply, then we know that [AppR] cannot apply and thus either:

- $\Gamma(x_1) \not\leq \mathbb{0} \to \mathbb{1}$, in this every s_i is a strict refinement of $\Gamma(x_1)$ and thus the rule cannot return $\{\varphi', \{\Gamma\}\}$, or
- The DNF of $\Gamma(x_1)$ is a disjunction of at least 2 elements, in this case we know by minimality of the DNF that every s_i is a strict refinement of $\Gamma(x_1)$ and thus the rule cannot return $\{\varphi', \{\Gamma\}\}$, or
- The DNF of $\Gamma(x_1)$ is a disjunction of 0 element and thus the rule will return $\{\varphi', \{\}\}$

In any case it is impossible for the rule to return $\{\varphi', \{\Gamma\}\}$.

[Abs] In order for this rule to return $\{\varphi', \{\Gamma\}\}$, we must have:

- $A' = \texttt{filter}_\Gamma(A)$: We can deduce that $(\Gamma \triangleright A) = \{s_i\}_{i\in I}$ and that $\forall i \in I.\ \mathbb{\Gamma}_i = \{(\Gamma, x : s_i)\}$.
- $\texttt{merge}_\kappa(\{\kappa_i\}_{i\in I}) = \texttt{filter}_\Gamma(\kappa)$: We can deduce that $\forall i \in I.\ \kappa_i = \texttt{filter}_{(\Gamma, x:s_i)}(\kappa)\}$.
- $\bigcup_{i\in I} \mathbb{\Gamma}'_i = \{\Gamma\}$: (nothing more to deduce)

Thus, by induction, we can deduce $\forall i \in I.\ \Gamma, x : s_i \vdash_{\mathcal{A}} \kappa_i : t'_i \leq t \circ_{\mathbb{1}} s_i$. As $\mathsf{dom}(t) = \bigvee_{j\in J} s_j \leq \bigvee(\Gamma \triangleright A) \leq \bigvee_{i\in I} s_i$, we have $\bigwedge s_i \to (t \circ_{\mathbb{1}} s_i) \leq t$. Consequently, we can derive $\Gamma \vdash_{\mathcal{A}} \varphi' : t' \leq t$ (rule [→I-Alg]).

Note that the final check $\bigvee_{j\in J} s_j \leq \bigvee\{s' \mid (\Gamma' \triangleright s') \in A'\}$ of the [Abs] rule is not strictly needed for the soundness, but it helps to detect an impossibility to obtain the type t sooner by checking if its domain can possibily be covered with the new annotations.

[AbsUntypeable] Impossible (it cannot return $\{\varphi', \{\Gamma\}\}$).

[UndefinedVar] Impossible (it cannot return $\{\varphi', \{\Gamma\}\}$).

[BindArgSkip] In order for this rule to return $\{\varphi', \{\Gamma\}\}$, it is necessary to have $\kappa' = \mathtt{filter}_\Gamma(\kappa)$ as well as $\mathbb{\Gamma} = \{\Gamma\}$. Thus, by induction on the second premise, we get $\Gamma \vdash_{\mathcal{A}} \kappa' : t' \leq t$. With a simple application of the [$\vee_1$-Alg] rule, we can derive $\Gamma \vdash_{\mathcal{A}} \varphi' : t' \leq t$.

[BindArgUntyp] Similar to the previous case.

[BindArgRefEnv] Impossible (it cannot return $\{\varphi', \{\Gamma\}\}$ because $\mathbb{\Gamma} \neq \{\Gamma\}$).

[BindArgRefAnns] Impossible (it cannot return $\{\varphi', \{\Gamma\}\}$ because $a' \neq a$).

[Bind] In order for this rule to return $\{\varphi', \{\Gamma\}\}$, we must have:

- $\bigcup_{i\in I} A_i = \mathtt{filter}_\Gamma(A)$: We can deduce that $(\Gamma \triangleright A) = \{s_i\}_{i\in I}$ and that $\forall i \in I.\ \mathbb{\Gamma}'_i = \{(\Gamma, x : s_i)\}$. This implies $\forall i \in I.\ \mathbb{\Gamma}_i = \{(\Gamma, x : s_i)\}$ because `propagate` can only refine environments.
- $\mathtt{merge}_\kappa(\{\kappa_i\}_{i\in I}) = \mathtt{filter}_\Gamma(\kappa)$: We can deduce that $\forall i \in I.\ \kappa_i = \mathtt{filter}_{(\Gamma, x:s_i)}(\kappa)\}$.
- $\bigcup_{i\in I} \mathbb{\Gamma}'_i = \{\Gamma\}$: (nothing more to deduce)

Thus, by induction, we can deduce $\forall i \in I.\ \Gamma, x : s_i \vdash_{\mathcal{A}} \kappa_i : t'_i \leq t$. Consequently, we can derive $\Gamma \vdash_{\mathcal{A}} \varphi' : t' \leq t$ (rule [$\vee_2$-Alg]).

[Var] We know that $\{\Gamma[x :\hat{=} t]\} = \{\Gamma\}$. We can deduce $\Gamma(x) \leq t$ and thus we trivially have $\Gamma \vdash_{\mathcal{A}} \varphi' : t' \leq t$.

□

Theorem D.43 (Soundness of the reconstruction algorithm). *If κ is a closed MSC-form and $\mathcal{R}(\kappa) = \kappa'$, then $\varnothing \vdash_{\mathcal{A}} \kappa' : t$ for some t.*

Proof. Immediate corollary of the previous lemma D.42. □