Advances in Type Systems for Functional Logic Programming (Extended Version)*
Technical Report SIC-05-12

Francisco J. López-Fraguas
Enrique Martín-Martín
Juan Rodríguez-Hortalá

Departamento de Sistemas Informáticos y Computación
Universidad Complutense de Madrid, Spain
fraguas@sip.ucm.es, emartim@fdi.ucm.es, juanrh@fdi.ucm.es

Abstract. Type systems are widely used in programming languages as a powerful tool providing safety to programs, and forcing the programmers to write code in a clearer way. Functional-logic languages have inherited Damas & Milner type system from their functional part due to its simplicity and popularity. In this paper we address a couple of aspects that can be subject of improvement. One is related to a problematic feature of functional logic languages not taken under consideration by standard systems: it is known that the use of opaque HO patterns in left-hand sides of program rules may produce undesirable effects from the point of view of types. We re-examine the problem, and propose a Damas & Milner-like type system where certain uses of HO patterns (even opaque) are permitted while preserving type safety, as proved by a subject reduction result that uses HO-let-rewriting, a recently proposed operational semantics for HO functional logic programs. At the same time that we formalize the type system, we have made the effort of technically clarifying additional issues: one is the different ways in which polymorphism of local definitions can be handled, and the other is the overall process of type inference in a whole program.

1 Introduction

Type systems for programming languages are an active area of research [17], no matters which paradigm one considers. In the case of functional programming, most type systems have arisen as extensions of Damas & Milner’s [3], for its remarkable simplicity and good properties (decidability, existence of principal types, possibility of type inference). Functional logic languages [11]76, in their practical side, have inherited more or less directly Damas & Milner’s types.

* This paper is the extended version of “Advances in Type Systems for Functional Logic Programming” appeared in Pre-proceedings of the 18th International Workshop on Functional and (Constraint) Logic Programming (WFLP’09), June 28, 2009, Brasilia, Brazil.
In principle, most of the type extensions proposed for functional programming could be also incorporated to functional logic languages (this has been done, for instance, for type classes in \[14\]). However, if types are not only decoration but are to provide safety, one should be sure that the adopted system has indeed good properties. In this paper we tackle a couple of aspects of existing FLP systems that are problematic or not well covered by standard Damas & Milner systems. One is the presence of so called \textit{HO patterns} in programs, an expressive feature for which a sensible semantics exists \[4\]; however, it is known that unrestricted use of HO patterns leads to type unsafety, as recalled below. The second is the degree of polymorphism assumed for local pattern bindings, a matter with respect to which existing FP or FLP systems vary greatly.

The rest of the paper is organized as follows. The next two subsections further discuss the two mentioned aspects. Section 2 contains some preliminaries about FL programs and types. In Section 3 we expose the type system and prove its soundness wrt. the \textit{let rewriting} semantics of \[10\]. Section 4 contains a type inference relation, which let us find the most general type of expressions. Section 5 present a method to infer types for programs. Finally, Section 6 contains some conclusions and future work.

### 1.1 Higher order patterns

In our formalism patterns appear in the left-hand side of rules and in lambda or let expressions. Some of these patterns can be HO patterns, if they contain partial applications of function or constructor symbols. HO patterns can be a source of problems from the point of view of the types. In particular, it was shown in \[5\] that unrestricted use of HO patterns leads to loss of expected property of \textit{subject reduction} (i.e., evaluation does not change types), an essential property for a type system. The following is a crisp example of the problem.

\textbf{Example 1 (Polymorphic Casting \[2\]).} Consider the program consisting of the rules \(\text{snd X Y} \rightarrow Y\), \(\text{true X} \rightarrow X\), \(\text{false X} \rightarrow \text{false}\), \(\text{id X} \rightarrow X\), with the usual types inferred by a classical Damas & Milner algorithm. Then we can write the functions \(\text{co (snd X)} \rightarrow X\) and \(\text{cast X} \rightarrow \text{co (snd X)}\), whose inferred types will be \(\forall \alpha. \forall \beta. (\alpha \rightarrow \alpha) \rightarrow \beta\) and \(\forall \alpha. \forall \beta. \alpha \rightarrow \beta\) respectively. It is clear that \(\text{and (cast 0) true}\) is well-typed, because \(\text{cast 0}\) has type \text{bool} (in fact it has any type), but if we reduce the expression to \text{and 0 true} using the rule of \text{cast} the resulting expression is bad-typed.

The problem arises when dealing with HO patterns, because unlike FO patterns, knowing the type of a pattern does not always permit us to know the type of its subpatterns. In the previous example the cause is function \text{co}, because its pattern \text{snd X} is \textit{opaque} and shadows the type of its subpattern \text{X}. Usual inference algorithms treat this opacity as polymorphism, and that is the reason why it is inferred a completely polymorphic type for the the result of the function \text{co}.

In \[5\] the appearance of any opaque pattern in the left-hand side of the rules is prohibited, but we will see that it is possible to be less restrictive. The key is
making a distinction between \textbf{opaque} and \textbf{transparent} variables of a pattern: a variable is opaque if its type is not univocally fixed by the type of the pattern, and is transparent otherwise. We call a variable of a pattern \textbf{critical} if it is opaque in the pattern and also appears elsewhere in the expression. The formal definition of opaque and critical variables will be given in Sect. 3. With these notions we can relax the situation in \cite{5}, prohibiting only those patterns having critical variables.

1.2 Local definitions

Functional and functional logic languages provide syntax to introduce local definitions inside an expression. But in spite of the popularity of let-expressions, different implementations treat them differently because of the polymorphism they give to bound variables. This differences can be observed in Example \ref{example2} being $(e_1, \ldots, e_n)$ and $[e_1, \ldots, e_n]$ the usual tuple and list notation respectively.

\begin{example}[let expressions] Let $e_1$ be $\text{let } F = \text{id in } (F \text{ true, } F \ 0)$, and $e_2$ be $\text{let } [F, G] = [\text{id, id} \text{ in } (F \text{ true, } F \ 0, G \ 0, G \ false)$

Intuitively, $e_1$ gives a new name to the identity function and uses it twice with arguments of different types. Surprisingly, not all the implementations consider this expression as well-typed, and the reason is that $F$ is used with different types in each appearance: $\text{bool} \rightarrow \text{bool}$ and $\text{int} \rightarrow \text{int}$. Some implementations as Clean 2.2, PAKCS 1.9.1 or KICS 0.81893 consider that a variable bound by a let-expression must be used with the same type in all the appearances in the body of the expression. In this situation we say that lets are completely monomorphic, and write $\text{let}_m$ for it.

On the other hand, we can consider that all the variables bound by the let-expression may have different but coherent types, i.e., are treated polymorphically. Then expressions like $e_1$ or $e_2$ would be well-typed. This is the decision adopted by Hugs Sept 2006 or OCaml 3.10.2. In this case, we will say that lets are completely polymorphic, and write $\text{let}_p$.

Finally, we can treat the bound variables monomorphically or polymorphically depending on the form of the pattern. If the pattern is a variable, the let treats it polymorphically, but if it is compound the let treats all the variables monomorphically. This is the case of GHC 6.8.2, SML of New Jersey v110.67 or Curry Münster 0.9.11. In this implementations $e_1$ is well-typed, while $e_2$ not. We call this kind of let-expression $\text{let}_{pm}$.

Fig. 1 summarizes the decisions of various implementations of functional and functional logic languages. The exact behavior wrt. types of local definitions is usually not well documented, not to say formalized, in those system. One of our contributions is this paper is to technically clarify this question by adopting a neutral position, and formalizing the different possibilities for the polymorphism of local definitions.

3
2 Preliminaries

Let expressions in different programming languages.

Fig. 1. Let expressions in different programming languages.

<table>
<thead>
<tr>
<th>Programming language and version</th>
<th>let_m</th>
<th>let_pmn</th>
<th>let_p</th>
</tr>
</thead>
<tbody>
<tr>
<td>GHC 6.8.2</td>
<td>×</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hugs Sept. 2006</td>
<td></td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Standard ML of New Jersey 110.67</td>
<td></td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>Ocaml 3.10.2</td>
<td></td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>Clean 2.0</td>
<td>×</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOY 2.3.1*</td>
<td></td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Curry PAKCS 1.9.1</td>
<td></td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>Curry Münster 0.9.11</td>
<td></td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>KICS 0.81893</td>
<td>×</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(*) we use where instead of let, not supported by TOY.
we write $\mathcal{A}(s_i) = \sigma_i$. A type substitution $\pi \in \mathcal{TSub}$ is a finite mapping from type variables to simple types $[(\alpha_i/\tau_i)]$. For sets of assumptions $FTV(\{\stackrel{\tau}{\alpha_i};\sigma_i\}) = \bigcup FTV(\sigma_i)$. We will say a type-scheme $\sigma$ is closed if $FTV(\sigma) = \emptyset$. The notion of applying a type substitution to a type variable or simple type is the natural, and for type-schemes consists in applying the substitution only to their free variables. This notion is extended to set of assumptions in the obvious way. We will say $\sigma$ is an instance of $\sigma'$ if $\sigma = \sigma' \pi$ for some $\pi$. $\tau'$ is a generic instance of $\sigma \equiv \forall \alpha_i.\tau$ if $\tau' = \tau[\alpha_i/\tau_i]$ for some $\tau_i$, and we write it $\sigma \triangleright \tau'$. We extend $\triangleright$ to a relation between type-schemes by saying that $\sigma \triangleright \sigma'$ iff every simple type such that is a generic instance of $\sigma'$ is also a generic instance of $\sigma$. Then $\forall \alpha_i.\tau \triangleright \forall \beta_i.\tau[\alpha_i/\tau_i]$ iff $\{\beta_i\} \cap FTV(\forall \alpha_i.\tau) = \emptyset$ [12]. Finally, $\tau'$ is a variant of $\sigma \equiv \forall \alpha_i.\tau (\sigma \triangleright_{var} \tau')$ if $\tau' = \tau[\alpha_i/\beta_i]$ and $\beta_i$ are fresh type variables.

3 Type derivation

We propose a modification of Damas & Milner type system [3] with some differences. We have found convenient to separate the task of giving a regular Damas & Milner type and the task of checking critical variables. To do that we have defined two different type relations: $\vdash$ and $\vdash^\ast$.

The basic typing relation $\vdash$ in the upper part of Fig. 2 is like the classical Damas & Milner’s system but extended to handle the three different kinds of let expressions and the occurrence of patterns instead of variables in lambda and let expressions. We have also made the rules more syntax-directed so that the form of type derivations depends only on the form of the expression to be typed. $Gen(\tau, \mathcal{A})$ is the closure or generalization of $\tau$ wrt. $\mathcal{A}$ [6][12][18], which generalizes all the type variables of $\tau$ that do not appear free in $\mathcal{A}$. Formally: $Gen(\tau, \mathcal{A}) = \forall \alpha_i.\tau$ where $\{\alpha_i\} = FTV(\tau) \setminus FTV(\mathcal{A})$. As can be seen, $[LET_m]$ and $[LET^A_{pm}]$ behave the same, and do not generalize any of the types $\tau_i$ for the variables $X_i$ to give a type for the body. On the contrary, $[LET^X_{pm}]$ and $[LET_p]$ generalize the types given to the variables. Notice that if two variables share the same type in the set of assumptions $\mathcal{A}$, generalization will lose the connection between them. This fact can be seen with $e_2$ in Ex. 2. Although the type for both $F$ and $G$ can be $\alpha \rightarrow \alpha$ (with $\alpha$ a variable not appearing in $\mathcal{A}$) the generalization step will assign both the type-scheme $\forall \alpha.\alpha \rightarrow \alpha$, losing the connection between them.

The $\vdash^\ast$ relation (lower part of Fig. 2) uses $\vdash$ but enforces also the absence of critical variables. The characterization of an opaque variable is defined as follows. It states that a variable $X_i$ is opaque in $t$ when it is possible to build a type derivation for $t$ where the type assumed for $X_i$ contains type variables which do not occur in the type derived for the pattern.

Definition 1 (Opaque variable of $t$ wrt. $\mathcal{A}$). Let $t$ be a pattern that admits type wrt. a given set of assumptions $\mathcal{A}$. We say that $X_i \in \mathcal{X}_i = \text{var}(t)$ is opaque wrt. $\mathcal{A}$ iff $\exists \tau_i, \tau$ s.t. $\mathcal{A} \oplus \{X_i; \tau_i\} \vdash \tau$ and $FTV(\tau_i) \nsubseteq FTV(\tau)$. 

5
The previous definition is based on the existence of a certain type derivation, and therefore cannot be used as an effective check for the opacity of variables. An equivalent characterization can be formulated exploiting the close relationship between $\vdash$ an type inference $\triangleright$ that will be presented in Sect. 4. Since $\triangleright$ can be viewed as an algorithm, Prop. 1 provides a more operational definition which is useful when implementing the type system.

Proposition 1. $X_i \in X_i = \text{var}(t)$ is opaque wrt. $\mathcal{A}$ iff $\mathcal{A} \vdash \{X_i : \alpha_i\} \triangleright t : \tau_g$ and $\text{FTV}(\alpha_i, \tau_g) \not\subseteq \text{FTV}(\tau_g)$.
We write $\text{opaqueVar}_A(t)$ for set of opaque variables of $t$ wrt. $A$. Now, we can define the critical variables of an expression $e$ wrt. $A$ as those variables that, being opaque in a let or lambda pattern of $e$, are indeed used in $e$. Formally:

**Definition 2 (Critical variables).**

$critVar_A(s) = \emptyset$
$critVar_A(e_1; e_2) = critVar_A(e_1) \cup critVar_A(e_2)$
$critVar_A(\lambda t. e) = (\text{opaqueVar}_A(t) \cap FV(e)) \cup critVar_A(e)$
$critVar_A(\text{let}_t^* t = e_1 in e_2) = (\text{opaqueVar}_A(t) \cap FV(e_2)) \cup critVar_A(e_1) \cup critVar_A(e_2)$

The typing relation $\vdash^\cdot$ has been defined in a modular way in the sense that the opacity check is kept separated from the regular Damas & Milner typing. Therefore it is easy to see that if every constructor and function symbol in program has a transparent assumption, then all the variables in patterns will be transparent, and so $\vdash^\cdot$ will be equivalent to $\vdash$. This happens in particular for those programs using only first order patterns and whose constructor symbols come from a Haskell (or Toy, Curry)-like data declaration.

### 3.1 Properties of the typing relations

The typing relations fulfill a set of useful properties. Here we use $\vdash^?$ for any of the two typing relations; $\vdash$ or $\vdash^\cdot$.

**Theorem 1 (Properties of the typing relations).**

a) If $A \vdash^? e : \tau$ then $A\pi \vdash^? e : \tau\pi$

b) Let $s$ be a symbol which does not appear in $e$. Then $A \vdash^? e : \tau \iff A \oplus \{ s : \sigma_s \} \vdash^? e : \tau$.

c) If $A \oplus \{ X : \tau_x \} \vdash^? e : \tau$ and $A \oplus \{ X : \tau_x \} \vdash^? e' : \tau_x$ then $A \oplus \{ X : \tau_x \} \vdash^? e[X/e'] : \tau$.

d) If $A \oplus \{ s : \sigma \} \vdash e : \tau$ and $\sigma' \succ \sigma$, then $A \oplus \{ s : \sigma' \} \vdash e : \tau$.

Part a) states that type derivations are closed under type substitutions. b) shows that type derivations for $e$ depend only on the assumptions for the symbols in $e$. c) is a substitution lemma stating that in a type derivation we can replace a variable by an expression with the same type. Finally, d) establishes that from a valid type derivation we can change the assumption of a symbol for a more general type-scheme, and we still have a correct type derivation for the same type. Notice that this is not true wrt. the typing relation $\vdash^\cdot$ because a more general type can introduce opacity. For example the variable $X$ is opaque in $\text{snd} X$ with the usual type for $\text{snd}$, but with a more specific type such as $\text{bool} \to \text{bool} \to \text{bool}$ it is no longer opaque.

### 3.2 Subject Reduction

Subject reduction is a key property for type systems, meaning that evaluation does not change the type of an expression. This ensures that run-time type errors will not occur. Subject reduction is only guaranteed for well-typed programs, a notion that we formally define now.
Definition 3 (Well-typed program). A program rule \( f \ t_1 \ldots t_n \rightarrow e \) is well-typed wrt. \( A \) if \( A \vdash \lambda \tau_1 \ldots \lambda \tau_n.e : \tau \) and \( \tau \) is a variant of \( A(f) \). A program \( P \) is well-typed wrt. \( A \) if all its rules are well-typed wrt. \( A \). If \( P \) is well-typed wrt. \( A \) we write \( \text{wt}_A(P) \).

Notice the use of the extended typing relation \( \vdash \) in the previous definition. This is essential, as we will explain later.

Although the restriction that the type of the lambda abstraction associated to a rule must be a variant of the type of the function symbol (and not an instance) may be strange, it is necessary. If not, the fact that a program is well-typed will not give us important information about the functions like the type of their arguments, and will make us to consider as well-typed undesirable programs like \( P \equiv \{ f \text{ true} \rightarrow \text{true}; f \text{ 2} \rightarrow \text{false} \} \) with the assumptions \( A \equiv \{ f :: \forall \alpha.\alpha \rightarrow \text{bool} \} \). Besides, this restriction is implicitly considered in \([6]\).

\[
\begin{array}{l}
\text{TRL}(s) = s, \text{ if } s \in DC \cup FS \cup DV \\
\text{TRL}(e_1, e_2) = \text{TRL}(e_1) \cdot \text{TRL}(e_2) \\
\text{TRL}({\text{let}}_K X = e_1 \text{ in } e_2) = \text{let}_K X = \text{TRL}(e_1) \text{ in } \text{TRL}(e_2), \text{ with } K \in \{m,p\} \\
\text{TRL}({\text{let}}_p X = e_1 \text{ in } e_2) = \text{let}_p X = \text{TRL}(e_1) \text{ in } \text{TRL}(e_2) \\
\text{TRL}({\text{let}}_m t = e_1 \text{ in } e_2) = \text{let}_m Y = \text{TRL}(e_1) \text{ in } \text{let}_m X_i = f_{X_i} Y \text{ in } \text{TRL}(e_2) \\
\text{TRL}({\text{let}}_p t = e_1 \text{ in } e_2) = \text{let}_p Y = \text{TRL}(e_1) \text{ in } \text{let}_p X_i = f_{X_i} Y \text{ in } \text{TRL}(e_2) \\
\end{array}
\]

for \( \{X_i\} = \text{var}(t) \cap \text{var}(e_2) \), \( f_{X_i} \in FS^1 \) fresh defined by the rule \( f_{X_i} t \rightarrow X_i \), \( Y \in DV \) fresh, \( t \) a non variable pattern and \( t' \) any pattern.

Fig. 3. Transformation rules of let expressions with patterns

For subject reduction to be meaningful, a notion of evaluation is needed. In this paper we consider the \textit{let-rewriting} relation of \([10]\). As can be seen, \textit{let-rewriting} does not support let expressions with compound patterns. Instead of extending the semantics with this feature we propose a transformation from let-expressions with patterns to let-expressions with only variables (Fig. 3). There are various ways to perform this transformation, which differ in the strictness of the pattern matching. We have chosen the alternative explained in \([10]\) that does not demand the matching if no variable of the pattern is needed, but otherwise forces the matching of the whole pattern. This transformation has been enriched with the different kinds of let expressions in order to preserve the types, as is stated in Th. 2. Notice that the result of the transformation and the expressions accepted by \textit{let-rewriting} only has \textit{let}_m or \textit{let}_p expressions, since without compound patterns \textit{let}_{pm} is the same as \textit{let}_p. Finally, we have added polymorphism annotations to let expressions (Fig. 4). Original (Flat) rule has been split into two, one for each kind of polymorphism. Although both behave the same from the point of view of values, the splitting is needed to guarantee type preservation. \( \lambda \)-abstractions have been omitted, since they are not supported by \textit{let-rewriting}. 
Fig. 4. Higher order let-rewriting relation $\rightarrow^l$

**Theorem 2 (Type preservation of the let transformation).** Assume $\mathcal{A} \vdash^* e : \tau$ and let $\mathcal{P} = \{ f_{X_i} : t_i \rightarrow X_i \}$ be the rules of the projection functions needed in the transformation of $e$ according to Fig. 3. Let also $\mathcal{A}'$ be the set of assumptions over that functions, defined as $\mathcal{A}' = \{ f_{X_i} : \text{Gen}(\pi_{X_i}, \mathcal{A}) \}$, where $\mathcal{A} \vdash^* \lambda t_i. X_i : \tau_{X_i} | \pi_{X_i}$. Then $\mathcal{A} \uplus \mathcal{A}' \vdash^* \text{TRL}(e) : \tau$ and $\text{wt}_{\mathcal{A} \uplus \mathcal{A}'}(\mathcal{P})$.

Th. 2 also states that the projection functions are well-typed. Then if we start from a well-typed program $\mathcal{P}$ wrt. $\mathcal{A}$ and apply the transformation to all its rules, the program extended with the projections rules will be well-typed wrt. the extended assumptions: $\text{wt}_{\mathcal{A} \uplus \mathcal{A}'}(\mathcal{P} \uplus \mathcal{P}')$. This result is straightforward, because $\mathcal{A}'$ does not contain any assumption for the symbols in $\mathcal{P}$, so $\text{wt}_{\mathcal{A}}(\mathcal{P})$ implies $\text{wt}_{\mathcal{A} \uplus \mathcal{A}'}(\mathcal{P})$.

Th. 3 states the subject reduction property for a let-rewriting step, but its extension to any number of steps is trivial.

**Theorem 3 (Subject Reduction).** If $\mathcal{A} \vdash^* e : \tau$ and $\text{wt}_{\mathcal{A}}(\mathcal{P})$ and $\mathcal{P} \vdash e \rightarrow^l e'$ then $\mathcal{A} \vdash^* e' : \tau$.

For this result to hold it is essential that the definition of well-typed program relies on $\vdash^*$. A counterexample can be found in Ex. 4 where the program would be well-typed wrt. $\vdash$ but the subject reduction property fails for $\text{and} (\text{cast 0}) \text{true}$ because of the rule for $\text{co}$.

The proof of the subject reduction property is based on the following Lemma, an important auxiliary result about the instantiation of transparent variables. Intuitively it states that if we have a pattern $t$ with type $\tau$ and we change its variables by other expressions, the only way to obtain the same type $\tau$ for the substituted pattern is by changing the transparent variables for expressions with the same type. This is not guaranteed with opaque variables, and that is why we forbid their use in expressions.
Lemma 1. Assume $A \perp \{X_i : \tau_i\} \vdash t : \tau$, where $\text{var}(t) \subseteq \{X_i\}$. If $A \vdash t[X_i/s_i] : \tau$ and $X_j$ is a transparent variable of $t$ wrt. $A$ then $A \vdash s_j : \tau_j$.

4 Type inference for expressions

The typing relation $\vdash \cdot$ lacks some properties that prevent its usage as a type-checker mechanism in a compiler for a functional logic language. First, in spite of the syntax-directed style, the rules for $\vdash \cdot$ have a bad operational behavior: at some steps they need to guess a type. Second, the types related to an expression can be infinite due to polymorphism. Finally, the typing relation needs all the assumptions for the symbols in order to work. To overcome this problems, type systems usually are accompanied with a type inference algorithm which returns a valid type for an expression and also establish the types for some symbols in the expression.

In this work we have given the type inference in Fig. 5 a relational style to show the similarities with the typing relation. But in essence, the inference rules represent an algorithm (similar to algorithm $W [3,12]$) which fails if any of the rules cannot be applied. This algorithm accepts a set of assumptions $A$ and an expression $e$, and returns a simple type $\tau$ and a type substitution $\pi$. Intuitively, $\tau$ will be the “most general” type which can be given to $e$, and $\pi$ the “minimum” substitution we have to apply to $A$ in order to able to derive a type for $e$.

Th. 4 shows that the type and substitution found by the inference are correct, i.e., we can build a type derivation for the same type if we apply the substitution to the assumptions.

Theorem 4 (Soundness of $\vdash \cdot$). $A \vdash \cdot e : \tau \models \Rightarrow A\pi \vdash \cdot e : \tau$

Th. 5 expresses the completeness of the inference process. If we can derive a type for an expression applying a substitution to the assumptions, then inference will succeed and will find a type and a substitution which are more general.

Theorem 5 (Completeness of $\vdash \cdot$ wrt $\vdash \cdot$). If $A\pi' \vdash \cdot e : \tau'$ then $\exists \tau, \pi, \pi''$. $A \vdash \cdot e : \tau | \pi \land A\pi\pi'' = A\pi' \land \tau\pi'' = \tau'$.

A result similar to Th. 5 cannot be obtained for $\vdash \cdot \cdot$ because of critical variables, as Example 3 shows.

Example 3 (Inexistence of a more general typing substitution). Let $A \equiv \{\text{snd}' :: \alpha \rightarrow \text{bool} \rightarrow \text{bool}\}$ and consider the following two valid derivations $D_1 \equiv A[\alpha/\text{bool}] \vdash \cdot \lambda(\text{snd'} X).X : (\text{bool} \rightarrow \text{bool}) \rightarrow \text{bool}$ and $D_2 \equiv A[\alpha/\text{int}] \vdash \cdot \lambda(\text{snd'} X).X : (\text{bool} \rightarrow \text{bool}) \rightarrow \text{int}$. It is clear that there is not a substitution more general than $[\alpha/\text{bool}]$ and $[\alpha/\text{int}]$ which makes possible a type derivation for $\lambda(\text{snd'} X).X$. The only substitution more general than these two will be $[\alpha/\beta]$ (for some $\beta$), converting $X$ in a critical variable.

In spite of this, we will see that $\vdash \cdot \cdot$ is still able to find a more general substitution when it exists. To formalize that, we will use the notion of $H^*_A,e$, which denotes the set collecting all type substitution $\pi$ such that $A\pi$ gives some type to $e$. 

10
\[
\begin{align*}
\text{[ID]} & \quad A \vdash s : \tau | id \quad \text{if } s \in DC \cup FS \cup DV \\
& \quad \land (s : \sigma) \in A \land \sigma \succ var \tau \\
\text{[APP]} & \quad A \Gamma, \alpha \vdash e_1 : \tau_1 | \pi_1 \\
& \quad A \Gamma, \alpha, \pi_1 \vdash e_2 : \tau_2 | \pi_2 \\
& \quad A \Gamma \vdash e_1 e_2 : \alpha | \pi_1 \pi_2 \pi \quad \text{if } \alpha \text{ fresh type variable} \\
& \quad \land \pi = \text{mgu}(\tau_1 \pi_2, \tau_2 \alpha) \\
\text{[LET]} & \quad A \oplus \{X : \alpha\} \vdash \lambda t : \tau_1 | \pi_1 \\
& \quad (A \oplus \{X : \alpha\}) \Gamma, \alpha \vdash e : \tau | \pi \\
& \quad A \Gamma, \lambda\.e : \tau_1 \pi \rightarrow \tau | \pi_1 \pi \\
& \quad \quad \quad \quad \text{if } \{X\} = \text{var}(t) \\
& \quad \quad \quad \quad \land \alpha \text{ fresh type variables} \\
\text{[LET]} & \quad A \oplus \{X : \alpha\} \vdash \text{let } t = e_1 \text{ in } e_2 : \tau_2 | \pi_1 \pi_2 \\
& \quad A \Gamma, \alpha, \tau_1 \pi_1 \pi \vdash e_1 : \tau_1 | \pi_1 \\
& \quad A \Gamma, \alpha, \tau_1 \pi_1 \pi \vdash e_2 : \tau_2 | \pi_2 \\
& \quad A \Gamma \vdash \text{let } t = e_1 \text{ in } e_2 : \tau_2 | \pi_1 \pi_2 \\
& \quad \quad \quad \quad \text{if } \{X\} = \text{var}(t) \land \alpha \text{ fresh type variables} \\
& \quad \quad \quad \quad \land \pi = \text{mgu}(\tau_1 \pi_1, \tau_1) \\
\text{[LET]} & \quad A \oplus \{X : \alpha\} \vdash \text{let } t_1 \ldots t_n = e_1 \text{ in } e_2 : \tau_2 | \pi_1 \pi_2 \\
& \quad A \Gamma, \alpha, \tau_1 \pi_1 \pi \vdash e_1 : \tau_1 | \pi_1 \\
& \quad A \Gamma, \alpha, \tau_1 \pi_1 \pi \vdash e_2 : \tau_2 | \pi_2 \\
& \quad A \Gamma \vdash \text{let } t_1 \ldots t_n = e_1 \text{ in } e_2 : \tau_2 | \pi_1 \pi_2 \\
& \quad \quad \quad \quad \text{if } h \in DC \cup FS \land \{X_n\} = \text{var}(h t_1 \ldots t_n) \\
& \quad \quad \quad \quad \land \alpha \text{ fresh type variables} \land \pi = \text{mgu}(\tau_0 \pi_1, \tau_1) \\
\text{[LET]} & \quad A \oplus \{X : \alpha\} \vdash \text{let } t = e_1 \text{ in } e_2 : \tau_2 | \pi_1 \pi_2 \\
& \quad A \Gamma, \alpha, \tau_1 \pi_1 \pi \vdash e_1 : \tau_1 | \pi_1 \\
& \quad A \Gamma, \alpha, \tau_1 \pi_1 \pi \vdash e_2 : \tau_2 | \pi_2 \\
& \quad A \Gamma \vdash \text{let } t = e_1 \text{ in } e_2 : \tau_2 | \pi_1 \pi_2 \\
& \quad \quad \quad \quad \text{if } \{X\} = \text{var}(t) \land \alpha \text{ fresh type variables} \\
& \quad \quad \quad \quad \land \pi = \text{mgu}(\tau_1 \pi_1, \tau_1) \\
\text{[IP]} & \quad A \vdash e : \tau | \pi \\
& \quad A \vdash e : \tau | \pi \\
& \quad \quad \quad \quad \quad \text{if } \text{critVar}_A(e) = \emptyset
\end{align*}
\]

Fig. 5. Inference rules
Definition 4 (Typing substitutions of $e$).
$$\Pi_{A,e} = \{ \pi \in TSubst \mid \exists \tau \in SType. A \pi \vdash \bullet e : \tau \}$$

Now we are ready to formulate our result regarding the maximality of $\vdash \bullet$.

Theorem 6 (Maximality of $\vdash \bullet$).

a) $\Pi_{A,e}$ has a maximum element $\iff \exists \tau_g \in SType, \pi_g \in TSubst. A \vdash \bullet e : \tau | \pi_g$.

b) If $A \pi' \vdash \bullet e : \tau'$ and $A \vdash \bullet e : \tau | \pi$ then exists a type substitution $\pi''$ such that $A \pi' = A \pi \pi''$ and $\tau' = \tau \pi''$.

5 Type inference for programs

In the functional programming setting, type inference does not need to distinguish between programs and expressions, because the program can be incorporated in the expression by means of let expressions and $\lambda$-abstractions. This way, the results given for expressions are also valid for programs. But in our framework it is different, because our semantics (let-rewriting) does not support $\lambda$-abstractions and our let expressions do not define new functions but only perform pattern matching. Thereby in our case we need to provide an explicit method for inferring the types of a whole program. By doing so, we will also provide a specification closer to implementations.

The type inference procedure for a program takes a set of assumptions $A$ and a program $P$ and returns a type substitution $\pi$. The set $A$ must contain assumptions for all the symbols in the program, even for the functions defined in $P$. We want to reflect the fact that in practice some defined functions may come with an explicit type declaration. Indeed this is a frequent way of documenting a program. Furthermore, type declarations are sometimes a real need, for instance if we want the language to support polymorphic recursion. Therefore, for some of the functions –those for which we want to infer types– the assumption will be simply a fresh type variable, to be instantiated by the inference process. For the rest, the assumption will be a closed type-scheme, to be checked by the procedure.

Definition 5 (Type Inference of a Program). The procedure $B$ for type inference of a program $\{rule_1, \ldots, rule_m\}$ is defined as:

$$B(A, \{rule_1, \ldots, rule_m\}) = \pi,$$ if

1. $A \vdash \bullet (\varphi(rule_1), \ldots, \varphi(rule_m)) : (\tau_1, \ldots, \tau_m) | \pi$.

2. Let $f^1 \ldots f^k$ be the function symbols of the rules $rule_i$ in $P$ such that $A(f^i)$ is a closed type-scheme, and $\tau^i$ the type obtained for $rule_i$ in step 1. Then $\tau^i$ must be a variant of $A(f^i)$.

$\varphi$ is a transformation from rules to expressions defined as:

$$\varphi(f t_1 \ldots t_n \to e) = \text{pair } \lambda t_1 \ldots \lambda t_n. e f$$
where () is the usual tuple constructor, with type () : ∀α1,α → ...αm → (α1,...,αm); and pair is a special constructor of tuples of two elements of the same type, with type pair :: ∀α.α → α → α.

The procedure B has two important properties. It is sound: if the procedure B finds a substitution π then the program P is well typed with respect to the assumptions Aπ (Th. 7). And second, if the procedure B succeeds it finds a more general typing substitution (Th. 8). It is not true in general that the existence of a well-typing substitution π ′ implies the existence of a more general one. A counterexample of this fact is very similar to Ex. 3.

**Theorem 7 (Soundness of B).** If B(A, P) = π then wt Aπ(P).

**Theorem 8 (Maximality of B).** If wt Aπ′(P) and B(A, P) = π then ∃π″ such that Aπ′ = Aππ″.

Notice that types inferred for the functions are simple types. In order to obtain type-schemes we need and extra step of generalization, as discussed in the next section.

### 5.1 Stratified Inference of a Program

It is known that splitting a program into blocks of mutually recursive functions and inferring the types in order may reduce the need of providing explicit type-schemes. This situation is shown in Example 4.

**Example 4 (Program Inference vs Stratified Inference).**

\[ A ≡ \{\text{true} : \text{bool}, 0 : \text{int}, \text{id} : \alpha, f : \beta, g : \gamma\} \]

\[ P ≡ \{\text{id} X → X; f → \text{id} \text{true}; g → \text{id} 0\} \]

\[ P_1 ≡ \{\text{id} X → X\}, P_2 ≡ \{f → \text{id} \text{true}\}, P_3 ≡ \{g → \text{id} 0\} \]

An attempt to apply the procedure B to infer types for the whole program fails because it is not possible for id to have types bool → bool and int → int at the same time. We will need to provide explicitly the type-scheme for id : ∀α.α → α in order to the type inference to succeed, yielding types f : bool → bool and g : int → int. But this is not necessary if we first infer types for P_1, obtaining δ → δ for id which will be generalized to ∀δ.δ → δ. With this assumption the type inference for both programs P_2 and P_3 will succeed with the expected types.

A general stratified inference procedure can be defined in terms of the basic inference B. First, it calculates the graph of strongly connected components from the dependency graph of the program, using e.g. Kosaraju or Tarjan’s algorithm [20]. Each strongly connected component will contain mutually dependent functions. Then it will infer types for every component (using B) in topological order, generalizing the obtained types before following with the next component.

Although stratified inference needs less explicit type-schemes, programs involving polymorphic recursion still require explicit type-schemes in order to infer their types.
6 Conclusions and Future Work

In this paper we have proposed a type system for functional logic languages based on Damas & Milner type system. As far as we know, prior to our work only [5] treats with technical detail a type system for functional logic programming. Our paper makes clear contributions when compared to [5]:

- By introducing the notion critical variables, we are more liberal in the treatment of opaque variables, but still preserving the essential property of subject reduction; moreover, this liberality extends also to data constructors, dropping the traditional restriction of transparency required to them. This is somehow similar to what happens with existential types [13] or generalized abstract datatypes [8], a connection that we plan to further investigate in the future.
- Our type system considers local pattern bindings and $\lambda$-abstractions (also with patterns), that were missing in [5]. In addition to that, we have made a rather exhaustive analysis and formalization of different possibilities for polymorphism in local bindings.
- Subject reduction was proved in [5] wrt. a narrowing calculus. Here we do it wrt. an small-step operational semantics closer to real computations.
- In [5] programs came with explicit type declarations. Here we provide type inference algorithms where type declarations are optional.

We have in mind several lines for future work: apart from the relation to existential types mentioned above, we are interested in other known extensions of type system, like type classes or generic programming. We also want to generalize the subject reduction property to narrowing, using let narrowing reductions of [10], and taking into account known problems [5,1] in the interaction of HO narrowing and types. Handling extra variables (variables occurring only in right hand sides of rules) is another challenge from the viewpoint of types.

References

A Proofs

Definition 6.
\[ \Pi_{A,e} = \{ \pi \in TSubst \mid \exists \tau \in SType. \ A\pi \vdash e : \tau \} \]

Observation 1
Note that \( \forall \alpha_i.\tau = \forall\beta_i.\tau[\alpha_i/\beta_i] \) if \( \{ \beta_i\} \cap FTV(\tau) = \emptyset \). In other words, two different type-schemes are the same if we change the bounded variables for other variables which do not appear free in \( \tau \). For example, \( \forall \alpha,\beta.(\alpha,\beta) \rightarrow \alpha \) is equal to \( \forall \gamma,\delta.(\gamma,\delta) \rightarrow \gamma \).
Observation 2
If \(\sigma \succ \sigma'\) then \(\text{FTV}(\sigma) \subseteq \text{FTV}(\sigma')\). It is clear from the definition of \(\succ\). If \(\alpha\) is a type variable in \(\text{FTV}(\sigma)\) then it will not be affected by the substitution. Besides, \(\alpha\) will be different from the generalized variables in \(\sigma'\). Therefore \(\alpha \in \text{FTV}(\sigma) \implies \alpha \in \text{FTV}(\sigma')\), so \(\text{FTV}(\sigma) \subseteq \text{FTV}(\sigma')\).

Observation 3
If \(s \neq s'\) then \(A \oplus \{s : \sigma\} \oplus \{s' : \sigma'\}\) is the same as \(A \oplus \{s' : \sigma'\} \oplus \{s : \sigma\}\). This observation can be extended to sets of assumptions, in the sense that \(A \oplus \{X_i : \sigma_i\} \oplus \{X'_j : \sigma'_j\} = A \oplus \{X'_j : \sigma'_j\} \oplus \{X_i : \sigma_i\}\) if \(X_i \neq X'_j\) for all \(i\) and \(j\).

Observation 4
If \(A \oplus \{X_i : \tau_i\} \vdash e : \tau\) then we can assume that \(A \oplus \{X_i : \alpha_i\} \parallel e : \tau' | \pi\) such that \(A\pi = A\).

Proof (Explantation). Intuitively, the inference finds a type which is more general than all the possible types for an expression, and also a type substitution which is necessary applying to the set of assumptions in order to derive a type for the expression. In this case it is possible from the original set of assumptions \(A\) to derive a type, so we do not need to change \(A\). Therefore the type substitution \(\pi\) from the inference would not need to affect \(A\), just only \(\alpha_i\) and the fresh variables generated during inference.

By Theorem 5 we know that there exists a type substitution \(\pi''\) such that \(A\pi\pi'' = A\) and \(\tau\pi'' = \tau\). This means that \(A\pi\) is just a renaming of some free type variables of \(A\), which are restored with the type substitution \(\pi''\). Being \(A\pi\) a renaming of \(A\) is a consequence of the \(mgu\) algorithm used. In this case, during inference there will be some unifying steps between a free type variable \(\alpha\) from \(A\) and a fresh one \(\beta\). Clearly, both \([\alpha/\beta]\) and \([\beta/\alpha]\) are more general unifiers. In this cases if we choose the first, we will compute a substitution which will make \(A\pi\) a renaming of \(A\); but if we choose always to substitute the fresh type variables the set of assumption \(A\pi\) will remain the same as \(A\).

Observation 5
If \(\text{FTV}(A) = \text{FTV}(A')\) then \(\text{Gen}(\tau, A) = \text{Gen}(\tau, A')\)

Observation 6 (Uniqueness of the type inference)
The result of a type inference is unique upon renaming of fresh type variables. In a type inference \(A \parallel e : \tau | \pi\) the variables in \(\text{FTV}(\tau)\), \(\text{Dom}(\pi)\) or \(\text{Rng}(\pi)\) which do not occur in \(\text{FTV}(A)\) are fresh variables generated by the inference process, so the result will remain valid if we replace them with different fresh type variables.

Observation 7
In a type derivation \(A \vdash e : \tau\) will appear a type derivation for every subexpression \(e'\) of \(e\). That is, the derivation will have a part of the tree rooted by \(A \oplus \{X_i : \tau_i\} \vdash e' : \tau'\), being \(\tau'\) a suitable type for \(e'\), and being \(\{X_i : \tau_i\}\) a set
of assumptions over variables of the expression e which have been introduced by
the rules $[A]$, $[LET]$, $[LET^{\text{psn}}]$, $[LET^{\text{th}}]$ or $[LET^{\text{p}}]$.
If the expression is a pattern, the set of assumptions $\{X_i : \pi_i\}$ will be empty
because the only rules used to type a pattern are $[ID]$ and $[APP]$.

Observation 8
If $wt_A(P)$ and $A'$ is a set of assumptions for variables, then $wt_{A \oplus A'}(P)$.
The reason is that $A'$ does not change the assumptions for the function and
constructor symbols in $A$. Since there are not extra variables in the right hand
sides, for every function rule in $P$ the typing rule for the lambda expression will
add assumptions for all the variables, shadowing the provided ones.

Lemma 1
Assume $A \oplus \{X_i : \pi_i\} \vdash t : \tau$, where $\text{var}(t) \subseteq \{X_i\}$. If $A \vdash t[X_i/s_i] : \tau$ and $X_j$
is a transparent variable of $t$ wrt. $A$ then $A \vdash s_j : \tau_j$.

Proof. According to Observation 7, in the derivation of $A \vdash t[X_i/s_i] : \tau$ appear
derivations for every subpattern $s_i$, and they have the form $A \vdash s_i : \tau'_i$ for some
$\tau'_i$. We will prove that if $X_j$ is a particular transparent variable of $t$, then $\tau_j = \tau'_j$.
It is easy to see that taking the types $\tau'_i$ as assumptions for the original variables
$X_i$ we can construct a derivation of $A \oplus \{X_i : \tau'_i\} \vdash t : \tau$, simply replacing
the derivations for the subpatterns $A \vdash s_i : \tau'_i$ with derivations for the variables
$A \oplus \{X_i : \tau'_i\} \vdash X_i : \tau'_i$ in the original derivation for $A \vdash t[X_i/s_i] : \tau$. Since $X_j$
is a transparent variable of $t$ wrt $A$, by definition $A \oplus \{X_i : \alpha_i\} \vdash t : \tau_g|\pi_g$ and
$FTV(\alpha_j|\pi_g) \subseteq FTV(\tau_g)$. By Theorem 5, if any type for $t$ can be derived from
$A \oplus \{X_i : \alpha_i\}\pi_s$ then $\pi_g$ must be more general than $\pi_s$. We know that there
are (at least) two substitutions $\pi^1$ and $\pi^2$ which can type $t : \pi^1 = \{\alpha_i \mapsto \tau_i\}$
and $\pi^2 = \{\alpha_i \mapsto \tau'_i\}$, so they must be more specific than $\pi_g$ (i.e. there exist
$\pi, \pi'$ such that $\pi^1 = \pi_g|\pi$ and $\pi^2 = \pi_g|\pi'$). We also know (by Theorem 4) that
$A \oplus \{X_i : \alpha_i\} \vdash t : \tau_g|\pi_g$ implies $(A \oplus \{X_i : \alpha_i\})|\pi_g \vdash t : \tau_g$, and by Theorem 1,
this implies that $(A \oplus \{X_i : \alpha_i\})|\pi_g \vdash t : \tau_g|\pi; \text{ so } \tau_g|\pi = \tau$ (the same thing
happens with $\pi' : \tau_g|\pi' = \tau$).

At this point we can distinguish two cases:

A) $X_j$ is transparent because of $FTV(\alpha_j|\pi_g) = \emptyset$. Then $\tau_j = (\alpha_j|\pi_g)\pi = (\alpha_j|\pi_g)\pi' = \tau'_j$, because if $\alpha_j|\pi_g$ does not have any free variable, it cannot be
affected by any substitution.

B) $X_j$ is transparent because of $FTV(\alpha_j|\pi_g) \subseteq FTV(\tau_g)$. As $\tau_g|\pi = \tau$ and
$\tau_g|\pi' = \tau$, then for every type variable $\beta$ in $FTV(\tau_g)$ then $\beta\pi = \beta\pi'$. As every
type variable $\beta$ in $FTV(\alpha_j|\pi_g)$ is also in $FTV(\tau_g)$ then as $\tau_j = (\alpha_j|\pi_g)\pi = (\alpha_j|\pi_g)\pi' = \tau'_j$. 

\[ \square \]

Lemma 2.
If $A \vdash e : \tau_1|\pi_1$ then $\exists \tau_2 \in SType, \pi_2, \pi'' \in TSubst$ s.t. $A \vdash e : \tau_2|\pi_2$ and
$\tau_2|\pi'' = \tau_1$ and $A\pi_2|\pi'' = A\pi_1$. 

17
Proof. By Theorem 1, \( \mathcal{A}(\pi \pi_1) \vDash e : \tau_1 \). Then applying Theorem 5, \( \mathcal{A} \vDash e : \tau_2 | \pi_2 \) and there exists a type substitution \( \pi'' \in \mathcal{TSubst} \) such that \( \tau_2 \pi'' = \tau_1 \) and \( \mathcal{A} \pi_2 \pi'' = \mathcal{A} \pi_1 \).

**Lemma 3 (Equivalence of the two characterizations of opaque variable).**

Let \( t \) be a pattern that admits type wrt. a given set of assumptions \( \mathcal{A} \). Then

\[
\exists \pi, \tau \text{ s.t. } \mathcal{A} \oplus \{ X_i : \alpha_i \} \vdash t : \tau \text{ and } \text{FTV}(\tau_i) \not\subseteq \text{FTV}(\tau) \\
\iff \mathcal{A} \oplus \{ X_i : \alpha_i \} \vDash t : \tau_g | \pi_g \text{ and } \text{FTV}(\alpha_i \pi_g) \not\subseteq \text{FTV}(\tau_g)
\]

**Proof.**

\(- \implies \) The type derivation can be written as \( (\mathcal{A} \oplus \{ X_i : \alpha_i \})[\alpha_i/\tau_i] \vdash t : \tau \), so by Theorem 5, \( \mathcal{A} \oplus \{ X_i : \alpha_i \} \vDash t : \tau_g | \pi_g \) and there exists some \( \pi'' \in \mathcal{TSubst} \) s.t. \( \tau_g \pi'' = \tau \), \( \mathcal{A} \pi_2 \pi'' = \mathcal{A} \) and \( \alpha_i \pi_g \pi'' = \tau_i \). We only need to prove that

\[
\text{FTV}(\tau_i) \not\subseteq \text{FTV}(\tau) \implies \text{FTV}(\alpha_i \pi_g) \not\subseteq \text{FTV}(\tau_g)
\]

It is equivalent to prove

\[
\text{FTV}(\alpha_i \pi_g) \subseteq \text{FTV}(\tau_g) \implies \text{FTV}(\tau_i) \subseteq \text{FTV}(\tau)
\]

which is trivial since \( \alpha_i \pi_g \pi'' = \tau_i \) and \( \tau_g \pi'' = \tau \), so

\[
\text{FTV}(\alpha_i \pi_g \pi'') \subseteq \text{FTV}(\tau_g \pi'')
\]

\(- \iff \) By Theorem 5, \( (\mathcal{A} \oplus \{ X_i : \alpha_i \})[\alpha_i/\tau_i] \vdash t : \tau_g \), and \( \text{FTV}(\alpha_i \pi_g) \not\subseteq \text{FTV}(\tau_g) \). Since \( t \) admits type by Observation 4, \( \mathcal{A} \pi_g = \mathcal{A} \), so \( \mathcal{A} \oplus \{ X_i : \alpha_i \pi_g \} \vDash t : \tau_g \).

**Lemma 4 (Decrease of opaque variables).**

If \( \mathcal{A} \oplus \{ X_i : \tau_i \} \vdash t : \tau \) and \( \mathcal{A} \pi \oplus \{ X_i : \tau_i \} \vdash t : \tau' \) then \( \text{opaqueVar}_{\mathcal{A} \pi}(t) \subseteq \text{opaqueVar}_{\mathcal{A} \pi}(t) \).

**Proof.** Since \( \text{opaqueVar}_{\mathcal{A} \pi}(t) = \text{var}(t) \setminus \text{transpVar}_{\mathcal{A} \pi}(e) \), then \( \text{opaqueVar}_{\mathcal{A} \pi}(t) \subseteq \text{opaqueVar}_{\mathcal{A} \pi}(t) \) is the same as \( \text{transpVar}_{\mathcal{A} \pi}(t) \subseteq \text{transpVar}_{\mathcal{A} \pi}(t) \). Then we have to prove that if a variable \( X_i \) of \( t \) is transparent wrt. \( \mathcal{A} \), then it is also transparent wrt. \( \mathcal{A} \pi \).

\( \mathcal{A} \oplus \{ X_i : \tau_i \} \) is the same as \( \mathcal{A} \oplus \{ X_i : \alpha_i \} \), so by Theorem 5, we have that \( \mathcal{A} \oplus \{ X_i : \alpha_i \} \vDash t : \tau_1 | \pi_1 \). Then the transparent variables of \( t \) will be those \( X_i \) such that \( \text{FTV}(\alpha_i \pi_1) \subseteq \text{FTV}(\tau_1) \).

\( \mathcal{A} \pi \oplus \{ X_i : \tau_i \} \) is the same as \( \mathcal{A} \oplus \{ X_i : \alpha_i \} \pi[\alpha_i/\tau_i] \), because we can assume that \( \text{var} \pi \) does not appear in \( \pi \). Then by Theorem 5, \( \mathcal{A} \oplus \{ X_i : \alpha_i \} \pi \vDash t : \tau_2 | \pi_2 \), and by Lemma 2, there exists a type substitution \( \pi'' \) such that \( \mathcal{A} \oplus \{ X_i : \alpha_i \} \pi \pi_2 = \mathcal{A} \oplus \{ X_i : \alpha_i \} \pi_1 \pi'' \) and \( \tau_2 = \tau_1 \pi'' \).

Therefore every data variable \( X_i \), which is transparent wrt. \( \mathcal{A} \), will be also transparent wrt. \( \mathcal{A} \pi \), because:

18
Let \( \mathcal{A} \vdash C[e] : \tau \) and in that derivation appear a derivation of the form \( \mathcal{A} \oplus \mathcal{A}' \vdash e : \tau' \), and \( \mathcal{A} \oplus \mathcal{A}' \vdash e' : \tau' \) then \( \mathcal{A} \vdash C[e'] : \tau \).

**Proof.** We proceed by induction over the structure of the contexts:

- Case \( \mathbf{[ \ ]} \): This case is straightforward because \( \| e = e \) and \( \| e' = e' \).
- Case \( \mathbf{e}_1 \mathbf{C} \): Since \( \mathbf{(e}_1 \mathbf{C)}[e] = e_1 \mathbf{C}[e] \), if we have a derivation for \( \mathcal{A} \vdash (e_1 \mathbf{C})[e] \) it must be of the form:
  
  \[
  \mathbf{[APP]} \quad \frac{\mathcal{A} \vdash e_1 : \tau_1 \rightarrow \tau \quad \mathcal{A} \vdash C[e] : \tau_1}{\mathcal{A} \vdash e_1, C[e] : \tau}
  \]
  
  A derivation of \( \mathcal{A} \oplus \mathcal{A}' \vdash e : \tau' \) must appear in the whole derivation, so it must appear in the derivation \( \mathcal{A} \vdash C[e] : \tau_1 \) (according to Observation 7). Since \( \mathcal{A} \oplus \mathcal{A}' \vdash e' : \tau' \) then by the Induction Hypothesis we can state that \( \mathcal{A} \vdash C[e'] : \tau_1 \), and we can construct a derivation for \( \mathcal{A} \vdash (e_1 \mathbf{C})[e'] \):
  
  \[
  \mathbf{[APP]} \quad \frac{\mathcal{A} \vdash e_1 : \tau_1 \rightarrow \tau \quad \mathcal{A} \vdash C[e'] : \tau_1}{\mathcal{A} \vdash e_1, C[e'] : \tau}
  \]

- Case \( \mathbf{let}_m \mathbf{X = C in e}_1 \) \( (\mathbf{let}_m \mathbf{X = C in e}_1)[e] \) is equal to \( \mathbf{let}_m \mathbf{X = C in e}_1 \) in \( \mathbf{e}_1 \), so a derivation of \( \mathcal{A} \vdash (\mathbf{let}_m \mathbf{X = C in e}_1)[e] : \tau \) must have the form:
  
  \[
  \mathbf{[LET}_m\mathbf{]} \quad \frac{\mathcal{A} \oplus \{X : \tau_1\} \vdash X : \tau_1 \quad \mathcal{A} \vdash C[e] : \tau_1 \quad \mathcal{A} \oplus \{X : \tau_1\} \vdash e_1 : \tau}{\mathcal{A} \vdash \mathbf{let}_m \mathbf{X = C in e}_1 \in \mathbf{e}_1 : \tau}
  \]
  
  Clearly, a derivation for \( \mathcal{A} \oplus \mathcal{A}' \vdash e : \tau' \) will appear in the derivation for \( \mathcal{A} \vdash C[e] : \tau_1 \) (Observation 7). Since \( \mathcal{A} \oplus \mathcal{A}' \vdash e' : \tau' \) then by the Induction Hypothesis we can state that \( \mathcal{A} \vdash C[e'] : \tau_1 \). With this information we can construct a derivation for \( \mathcal{A} \vdash \mathbf{let}_m \mathbf{X = C in e}_1 \)[e']:
  
  \[
  \mathbf{[LET}_m\mathbf{]} \quad \frac{\mathcal{A} \oplus \{X : \tau_1\} \vdash X : \tau_1 \quad \mathcal{A} \vdash C[e'] : \tau_1 \quad \mathcal{A} \oplus \{X : \tau_1\} \vdash e_1 : \tau}{\mathcal{A} \vdash \mathbf{let}_m \mathbf{X = C in e}_1 \in \mathbf{e}_1 : \tau}
  \]

- Case \( \mathbf{let}_m \mathbf{X = e}_1 \mathbf{ in C} \) A type derivation of \( \mathbf{(let}_m \mathbf{X = e}_1 \mathbf{ in C)}[e] \) will have the form:
  
  \[
  \mathbf{[LET}_m\mathbf{]} \quad \frac{\mathcal{A} \oplus \{X : \tau_1\} \vdash X : \tau_1 \quad \mathcal{A} \vdash e_1 : \tau_1 \quad \mathcal{A} \oplus \{X : \tau_1\} \vdash C[e] : \tau}{\mathcal{A} \vdash \mathbf{let}_m \mathbf{X = e}_1 \in \mathbf{C in e}_1 : \tau}
  \]
  
  By Observation 7 the derivation \( \mathcal{A} \oplus \{X : \tau_1\} \vdash C[e] \) will contain a derivation \( (\mathcal{A} \oplus \{X : \tau_1\}) \oplus \mathcal{A}' \vdash e : \tau' \). It is a premise that \( (\mathcal{A} \oplus \{X : \tau_1\}) \oplus \mathcal{A}' \vdash e' : \tau' \) (in this case \( \mathcal{A}' = \{X : \tau_1\} \oplus \mathcal{A}' \)), so by the Induction Hypothesis \( \mathcal{A} \vdash C[e'] : \tau \) and we can construct a derivation \( \mathcal{A} \vdash \mathbf{let}_m \mathbf{X = e}_1 \in \mathbf{C in e}_1 \)[e'].
Lemma 6.
If \( \text{critVar}_A(e) = \emptyset \) and \( \text{critVar}_A(e') = \emptyset \) then \( \text{critVar}_A(e[X/e']) = \emptyset \).

Proof. We will proceed by induction over the structure of \( e \).

Base Case
- \( c \) Straightforward because \( e[X/e'] = c \), so \( \text{critVar}_A(e[X/e']) = \emptyset \).
- \( f \) The same as \( c \).
- \( X \) In this case \( X[X/e'] = e' \), and \( \text{critVar}_A(e') = \emptyset \) from the premises.
- \( Y \) \( Y \) is a variable distinct from \( X \). Then \( Y[X/e'] = Y \), so \( \text{critVar}_A(Y) = \emptyset \).

Induction Step
- \( e_1 e_2 \) By definition \( \text{critVar}_A(e_1 e_2) = \emptyset \) implies that \( \text{critVar}_A(e_1) = \emptyset \) and \( \text{critVar}_A(e_2) = \emptyset \). Then by the Induction Hypothesis \( \text{critVar}_A(e_1[X/e']) = \emptyset \) and \( \text{critVar}_A(e_2[X/e']) = \emptyset \). By definition \( (e_1 e_2)[X/e'] = e_1[X/e'] e_2[X/e'] \), so:

\[
\text{critVar}_A((e_1 e_2)[X/e']) = \text{critVar}_A(e_1[X/e'] e_2[X/e']) \\
= \text{critVar}_A(e_1[X/e']) \cup \text{critVar}_A(e_2[X/e']) \\
= \emptyset \cup \emptyset \\
= \emptyset
\]

- \( \lambda t.e \) We assume that \( X \notin \text{var}(t) \) and \( \text{var}(t) \cap \text{FV}(e') = \emptyset \). We know that \( \text{opaqueVar}_A(t) \cap \text{FV}(e) = \emptyset \) and \( \text{critVar}_A(e) = \emptyset \) from \( \text{critVar}_A(\lambda t.e) = \emptyset \). Moreover \( \text{opaqueVar}_A(t) \subseteq \text{var}(t) \), so \( \text{opaqueVar}_A(t) \cap \text{FV}(e') = \emptyset \). Since the intersection of set is distributive, we have that \( \text{opaqueVar}_A(t) \cap (\text{FV}(e) \cup \text{FV}(e')) = (\text{opaqueVar}_A(t) \cap \text{FV}(e)) \cup (\text{opaqueVar}_A(t) \cap \text{FV}(e')) = \emptyset \). Since \( \text{FV}(e[X/e']) \subseteq \text{FV}(e) \cup \text{FV}(e') \), then \( \text{opaqueVar}_A(t) \cap \text{FV}(e[X/e']) = \emptyset \). On the other hand by the Induction Hypothesis \( \text{critVar}_A(e[X/e']) = \emptyset \). Therefore

\[
\text{critVar}_A((\lambda t.e)[X/e']) = \text{critVar}_A((\lambda t.e[X/e'])) \\
= (\text{opaqueVar}_A(t) \cap \text{FV}(e[X/e'])) \cup \text{critVar}_A(e[X/e']) \\
= \emptyset \cup \emptyset \\
= \emptyset
\]

- \( \text{let}_m t = e_1 \) in \( e_2 \) We assume that \( X \notin \text{var}(t) \), \( \text{var}(t) \cap \text{FV}(e') = \emptyset \), and \( \text{var}(t) \cap \text{FV}(e_1) = \emptyset \). Since \( \text{critVar}_A(\text{let}_m t = e_1 \text{ in } e_2) = \emptyset \) then \( \text{opaqueVar}_A(t) \cap \text{FV}(e_2) = \emptyset \), \( \text{critVar}_A(e_1) = \emptyset \) and \( \text{critVar}_A(e_2) = \emptyset \). From \( \text{var}(t) \cap \text{FV}(e') = \emptyset \) and \( \text{opaqueVar}_A(t) \subseteq \text{var}(t) \) we know that
opaqueVar_{A}(t) \cap FV(e') = \emptyset. As in the previous case, opaqueVar_{A}(t) \cap (FV(e_2) \cup FV(e')) = \emptyset and FV(e_2[X/e']) \subseteq FV(e_2) \cup FV(e'), therefore opaqueVar_{A}(t) \cap FV(e_2[X/e']) = \emptyset.

On the other hand by the Induction Hypothesis critVar_{A}(e_1[X/e']) = \emptyset and critVar_{A}(e_2[X/e']) = \emptyset. Therefore
\[
\text{critVar}_{A}((\text{let} \ t = e_1, \text{in} \ e_2)[X/e']) = \text{critVar}_{A}((\text{let} \ t = e_1[X/e'] \text{ in} \ e_2[X/e']) = (\text{opaqueVar}_{A}(t) \cap FV(e_2[X/e'])) \cup \text{critVar}_{A}(e_1[X/e']) \cup \text{critVar}_{A}(e_2[X/e']) = \emptyset \cup \emptyset \cup \emptyset = \emptyset
\]

The proofs for the \(let_{pm}\) and \(let_{p}\) cases are equal to the \(let_{m}\) case.

**Lemma 7.**

Let \(A\) be a set of assumptions, \(\tau\) a type and \(\pi \in \mathcal{T}_{\text{Subst}}\) such that for every type variable \(\alpha\) which appears in \(\tau\) and does not appear in \(\text{FTV}(A)\) then \(\alpha \notin \text{Dom}(\pi)\) and \(\alpha \notin \text{Rng}(\pi)\). Then \((\text{Gen}(\tau, A))\pi = \text{Gen}(\tau\pi, A\pi)\).

**Proof.** We will study what happens with a type variable \(\alpha\) of \(\tau\) in both cases (types that are not variables are not modified by the generalization step).

- \(\alpha \in \text{FTV}(\tau)\) and \(\alpha \in \text{FTV}(A)\). In this case it cannot be generalized in \(\text{Gen}(\tau, A)\), so in \((\text{Gen}(\tau, A))\pi\) it will be transformed into \(\alpha\pi\). Because \(\alpha \in \text{FTV}(A)\), then all the variables in \(\alpha\pi\) are in \(\text{FTV}(A\pi)\) and they cannot be generalized. Therefore in \((\text{Gen}(\tau\pi, A\pi))\alpha\) will also be transformed into \(\alpha\pi\).
- \(\alpha \in \text{FTV}(\tau)\) and \(\alpha \notin \text{FTV}(A)\). In this case \(\alpha\) will be generalized in \(\text{Gen}(\tau, A)\), and as \(\pi\) does not affect a generalized variable, it will remain in \((\text{Gen}(\tau, A))\pi\). Because \(\alpha\) is not in \(\text{Dom}(\pi)\), then \(\alpha\pi = \alpha\). \(\alpha \notin \text{Rng}(\pi)\) and \(\alpha \notin \text{FTV}(A)\), so it cannot appear in \(A\pi\). Therefore \(\alpha\) will also be generalized in \((\text{Gen}(\tau\pi, A\pi))\).

\(\square\)

**Lemma 8 (Generalization and substitutions).**

\(\text{Gen}(\tau, A)\pi \succ \text{Gen}(\tau\pi, A\pi)\)

**Proof.** It is clear that if a type variable \(\alpha\) in \(\tau\) is not generalized in \(\text{Gen}(\tau, A)\) (because it occurs in \(\text{FTV}(A)\)), then in the first type-scheme it will appear as \(\alpha\pi\). In the second type scheme it will also appear as \(\alpha\pi\) because all the variables in \(\alpha\pi\) will be in \(A\pi\) (as \(\alpha \in \text{FTV}(A)\)). Therefore in every generic instance of the two type-schemes this part will be the same. On the other hand, if a type variable \(\alpha\) is generalized in \(\text{Gen}(\tau, A)\) then it will also appear generalized in \(\text{Gen}(\tau, A)\pi\) (\(\pi\) will not affect it). It does not matter what happens with this part \(\alpha\pi\) in \(\text{Gen}(\tau\pi, A\pi)\) because in every generic instance of \(\text{Gen}(\tau, A)\pi\) the generalized \(\alpha\) will be able to adopt all the types of any generic instance of the part \(\alpha\pi\) in \(\text{Gen}(\tau\pi, A\pi)\).

\(\square\)
Lemma 9.

If \( \frac{A}{\frac{B}{\frac{C}{\frac{D}{E}}}} \) then \( \frac{F}{G} \).

Proof. From definition of \( \frac{H}{\frac{I}{\frac{J}{\frac{K}{L}}}} \) we know that \( \frac{M}{\frac{N}{\frac{O}{\frac{P}{Q}}}} \). We need to prove that \( \frac{R}{\frac{S}{\frac{T}{\frac{U}{V}}}} \).

Lemma 10.

\( A \vdash e_1 : \tau_1, \ldots, A \vdash e_n : \tau_n \iff A \vdash (e_1, \ldots, e_n) : (\tau_1, \ldots, \tau_n) \)

Proof. Straightforward.

Theorem \([P]\) (Properties of the typing relations).

a) If \( A \vdash e : \tau \) then \( A \vdash e : \tau \)

b) Let \( s \) be a symbol which does not appear in \( e \). Then \( A \vdash (s : \sigma) \)

c) If \( A \vdash (X : \tau_x) \) then \( A \vdash (X : \tau_x) \)

d) If \( A \vdash (s : \sigma) \) then \( A \vdash (s : \sigma) \)

Proof.

Base Case

- \([\text{ID}]\) If we have a derivation of \( A \vdash s : \tau \) using \([\text{ID}]\) is because \( \tau \) is a

generic instance of the type-scheme \( A(g) = \forall \pi, \tau \).

We can change this type-scheme by other equivalent \( \forall \pi \).

Induction Step

We have six different cases to consider accordingly to the inference rule used in

the last step of the derivation.
– [APP] In this case we have a derivation

\[ \frac{A \vdash e_1 : \tau_1 \rightarrow \tau \quad A \vdash e_2 : \tau_1}{A \vdash e_1 \ e_2 : \tau} \]

By the Induction Hypothesis \( A \pi \vdash e_1 : (\tau_1 \rightarrow \tau) \pi \) and \( A \pi \vdash e_2 : \tau_1 \pi \). Then \( (\tau_1 \rightarrow \tau) \pi \equiv \tau_1 \pi \rightarrow \tau \pi \) so we can construct a derivation

\[ \frac{A \pi \vdash e_1 : \tau_1 \pi \rightarrow \tau \pi \quad A \pi \vdash e_2 : \tau_1 \pi}{A \vdash e_1 \ e_2 : \tau \pi} \]

– [LET] The derivation has the form

\[ \frac{A \vdash \{X_1 : \tau_1\} \vdash t : \tau_1 \quad A \vdash \{X_1 : \tau_1\} \vdash e : \tau}{A \vdash \lambda_1 e : \tau_1 \rightarrow \tau} \]

By the Induction Hypothesis \( (A \vdash \{X_1 : \tau_1\}) \pi \vdash \lambda_1 e : \tau_1 \pi \) and \( (A \vdash \{X_1 : \tau_1\}) \pi \vdash e : \tau \pi \). But \( (A \vdash \{X_1 : \tau_1\}) \pi \equiv A \pi \Theta \{\{X_1 : \tau_1\} \mid \pi \equiv A \pi \Theta \{X_1 : \tau_1\} \) so we can build the type derivation

\[ \frac{A \pi \Theta \{X_1 : \tau_1\} \vdash t : \tau_1 \pi \quad A \pi \Theta \{X_1 : \tau_1\} \vdash e : \tau \pi}{A \pi \vdash \lambda_1 e : \tau_1 \rightarrow \tau \pi} \]

– [LET\_m] The type derivation is

\[ \frac{A \vdash \{X_1 : \tau_1\} \vdash t : \tau_1 \quad A \vdash e_1 : \tau_1 \quad A \vdash \{X_1 : \tau_1\} \vdash e_2 : \tau}{A \vdash \text{let}_m t = e_1 \text{ in } e_2 : \tau} \]

By the Induction Hypothesis \( (A \vdash \{X_1 : \tau_1\}) \pi \vdash t : \tau_1 \pi \), \( A \pi \vdash e_1 : \tau_1 \pi \) and \( (A \vdash \{X_1 : \tau_1\}) \pi \vdash e_2 : \tau \). As in the previous case \( (A \vdash \{X_1 : \tau_1\}) \pi \equiv A \pi \Theta \{X_1 : \tau_1\} \), so

\[ \frac{A \pi \Theta \{X_1 : \tau_1\} \vdash t : \tau_1 \pi \quad A \pi \vdash e_1 : \tau_1 \pi \quad A \pi \Theta \{X_1 : \tau_1\} \vdash e_2 : \tau \pi}{A \pi \vdash \text{let}_m t = e_1 \text{ in } e_2 : \tau \pi} \]

– [LET\_pm] The derivation will be

\[ \frac{A \vdash e_1 : \tau_x \quad A \vdash \{X : \text{Gen}(\tau_x, A)\} \vdash e_2 : \tau}{A \vdash \text{let}^{\text{pm}}_x X = e_1 \text{ in } e_2 : \tau} \]

First, we create a substitution \( \pi' \) that maps the variables of \( \tau_x \) which do not appear in \( FTV(A) \) to fresh variables which are not in \( FTV(A) \) and do not occur in \( Dom(\pi) \) nor in \( \text{Ring}(\pi) \). Then by the Induction Hypothesis \( A \pi' \vdash e_1 : \tau_x \pi' \). Since \( \pi' \) does not contain in its domain any variable in \( FTV(A) \), then \( A \pi' = A \) and \( A \vdash e_1 : \tau_x \pi' \). \( \pi' \) only substitutes variables which do not appear in \( A \) by variables which are not in \( A \) either, so \( \text{Gen}(\tau_x, A) \Rightarrow \text{Gen}(\tau_x \pi', A) \). Then \( A \vdash \{X : \text{Gen}(\tau_x \pi', A)\} \vdash e_2 : \tau \) is a valid derivation, and by the Induction Hypothesis \( (A \vdash \{X : \text{Gen}(\tau_x \pi', A)\}) \pi \vdash e_2 : \tau \pi \), which is the same that \( A \pi \vdash \{X : \text{Gen}(\tau_x \pi', A)\} \pi \vdash e_2 : \tau \pi \). By construction of \( \pi' \)
we know that for every variable of $\tau_x$, which does not appear in $\mathcal{A}$ it will not be in $\text{Dom}(\pi)$ nor in $\text{Rng}(\pi)$. Then we can apply Lemma 7 and we have that $\mathcal{A}_2 = \{X : \text{Gen}(\tau_x, \mathcal{A}_1)\} \vdash e_2 : \tau_t$. By the Induction Hypothesis over $\mathcal{A} \vdash e_1 : \tau_x \pi'$ we obtain $\mathcal{A}_1 \vdash e_1 : \tau_x \pi'$. With this information we can construct a derivation

\[
\begin{array}{c}
\text{[LET]}
\end{array}
\]

- [LET] Similar to the [LET] case.
- [LET] Similar to the [LET] case, but instead of having to handle one single $\tau_x$, we need to handle a set of $\tau_i$. The main idea is the same, creating a substitution $\pi'$ to rename the variables of the $\tau_i$ which do not appear in $\mathcal{A}$ and avoids their presence in the substitution $\pi$. Then we can apply Lemma 7 to all the generalizations and proceed as in the [LET] case.

\[
\begin{array}{c}
\text{[LET]}
\end{array}
\]

- [LET] If $\mathcal{A} \vdash e : \tau$ then $\mathcal{A} \vdash e : \tau_t$

By definition of $\vdash$ we know that $\mathcal{A} \vdash e : \tau$ and $\text{critVar}(\pi) = \emptyset$. Then by Theorem 1-a $\mathcal{A} \vdash e : \tau_t$. To prove that $\text{critVar}(\mathcal{A}_2(e)) = \emptyset$ we use the decrease of opaque variables, stated in Lemma 4. From $\mathcal{A} \vdash e : \tau$ and $\mathcal{A} \vdash e : \tau_t$ we know that for every pattern $t$ in $e$ we have a derivation $\mathcal{A} \vdash \{X_i : \tau_i\} \vdash t : \tau_i$ and $\mathcal{A} \vdash \{X_i : \tau_i\} \vdash t : \tau_t$, being $X_i$ the data variables in $t$. Then we can prove that $\text{critVar}(\mathcal{A}_2(e)) = \emptyset$ by induction over the structure of $e$.

**Base Case**
- (s) $\text{critVar}(\mathcal{A}_2(e)) = \emptyset$ by definition.

**Induction Step**
- (c1) By the Induction Hypothesis we have that $\text{critVar}(\mathcal{A}_2(e_1)) = \emptyset$ and $\text{critVar}(\mathcal{A}_2(e_2)) = \emptyset$, so $\text{critVar}(\mathcal{A}_2(e_1, e_2)) = \text{critVar}(\mathcal{A}_2(e_1)) \cup \text{critVar}(\mathcal{A}_2(e_2)) = \emptyset \cup \emptyset = \emptyset$.
- (c2) By the Induction Hypothesis $\text{critVar}(\mathcal{A}_2(e)) = \emptyset$. $\text{critVar}(\mathcal{A}_2(t)) = \emptyset$, so $\text{critVar}(\mathcal{A}_2(t) \cap \text{var}(t)) = \emptyset$. By Lemma 4 we know that $\text{opaqueVar}(\mathcal{A}_2(t)) \subseteq \text{opaqueVar}(\mathcal{A}_2(t) \cap \text{var}(t)) = \emptyset$. Then $\text{critVar}(\mathcal{A}_2(\lambda t.e)) = (\text{opaqueVar}(\mathcal{A}_2(t) \cap \text{var}(t))) \cup \text{critVar}(\mathcal{A}_2(e)) = \emptyset \cup \emptyset = \emptyset$.
- (c3) Similar to the previous case.

\[
\begin{array}{c}
\text{[LET]}
\end{array}
\]

- (b.1) Let be $s$ a symbol which does not appear in $e$. Then $\mathcal{A} \vdash e : \tau \iff \mathcal{A} \vdash \{s : \sigma_s\} \vdash e : \tau$.

$\Rightarrow$ We will proceed by induction over the size of the derivation tree.

**Base Case**

\[
\begin{array}{c}
24
\end{array}
\]
\( \text{[ID]} \) In this case the derivation will be:

\[
\text{[ID]} \quad \Rightarrow \quad A \vdash s : \tau
\]

where \( A(g) \supset \tau \). If we add an assumption over a symbol different from \( s \) then \( (A \oplus \{s : \sigma_s\})(g) \supset \tau \), so

\[
\text{[ID]} \quad \Rightarrow \quad A \oplus \{s : \sigma_s\} \vdash s : \tau
\]

\textbf{Induction Step}

\( \text{[APP]} \) The derivation will have the form:

\[
\begin{align*}
\text{[APP]} \quad & \quad A \vdash e_1 : \tau' \rightarrow \tau & A \vdash e_2 : \tau' \\
& \quad \Rightarrow \quad A \vdash e_1 e_2 : \tau
\end{align*}
\]

By the Induction Hypothesis then \( A \oplus \{s : \sigma_s\} \vdash e_1 : \tau' \rightarrow \tau \) and \( A \oplus \{s : \sigma_s\} \vdash e_2 : \tau' \), therefore:

\[
\begin{align*}
\text{[APP]} \quad & \quad A \oplus \{s : \sigma_s\} \vdash e_1 : \tau' \rightarrow \tau & A \oplus \{s : \sigma_s\} \vdash e_2 : \tau' \\
& \quad \Rightarrow \quad A \oplus \{s : \sigma_s\} \vdash e_1 e_2 : \tau
\end{align*}
\]

\( \text{[A]} \) We have a type derivation

\[
\begin{align*}
\text{[A]} \quad & \quad A \oplus \{X_i : \tau_i\} \vdash t : \tau' & A \oplus \{X_i : \tau_i\} \vdash e : \tau \\
& \quad \Rightarrow \quad A \vdash \lambda t.e : \tau' \rightarrow \tau
\end{align*}
\]

By the Induction Hypothesis then \( (A \oplus \{X_i : \tau_i\}) \oplus \{s : \sigma_s\} \vdash t : \tau' \) and \( (A \oplus \{X_i : \tau_i\}) \oplus \{s : \sigma_s\} \vdash e : \tau \). \( s \) does not appear in \( \lambda t.e \), so it will different from all the variables \( X_i \) and by Observation 3 \( (A \oplus \{X_i : \tau_i\}) \oplus \{s : \sigma_s\} \) is the same as \( (A \oplus \{s : \sigma_s\}) \oplus \{X_i : \tau_i\} \). Therefore we can build a type derivation:

\[
\begin{align*}
\text{[A]} \quad & \quad (A \oplus \{s : \sigma_s\}) \oplus \{X_i : \tau_i\} \vdash t : \tau' & (A \oplus \{s : \sigma_s\}) \oplus \{X_i : \tau_i\} \vdash e : \tau \\
& \quad \Rightarrow \quad A \oplus \{s : \sigma_s\} \vdash \lambda t.e : \tau' \rightarrow \tau
\end{align*}
\]

\( \text{[LET}_m) \) The type derivation will be:

\[
\begin{align*}
\text{[LET}_m) \quad & \quad A \oplus \{X_i : \tau_i\} \vdash t : \tau_t & A \vdash e_1 : \tau_t & A \oplus \{X_i : \tau_i\} \vdash e_2 : \tau \\
& \quad \Rightarrow \quad A \vdash \text{let}_m t = e_1 \text{ in } e_2 : \tau
\end{align*}
\]

By the Induction Hypothesis then \( (A \oplus \{X_i : \tau_i\}) \oplus \{s : \sigma_s\} \vdash t : \tau_t \), \( A \oplus \{s : \sigma_s\} \vdash e_1 : \tau_t \) and \( (A \oplus \{X_i : \tau_i\}) \oplus \{s : \sigma_s\} \vdash e : \tau \). As in the previous case \( (A \oplus \{X_i : \tau_i\}) \oplus \{s : \sigma_s\} = (A \oplus \{s : \sigma_s\}) \oplus \{X_i : \tau_i\} \), so we can build a type derivation:

\[
\begin{align*}
& \quad \Rightarrow \quad (A \oplus \{s : \sigma_s\}) \oplus \{X_i : \tau_i\} \vdash t : \tau_t \\
& \quad \Rightarrow \quad A \oplus \{s : \sigma_s\} \vdash e_1 : \tau_t \\
& \quad \Rightarrow \quad (A \oplus \{s : \sigma_s\}) \oplus \{X_i : \tau_i\} \vdash e_2 : \tau \\
\text{[LET}_m) \quad & \quad (A \oplus \{s : \sigma_s\}) \oplus \{X_i : \tau_i\} \vdash e_2 : \tau \\
& \quad \Rightarrow \quad A \oplus \{s : \sigma_s\} \vdash \text{let}_m t = e_1 \text{ in } e_2 : \tau
\end{align*}
\]
\[ \text{[LET}^X_{\text{pm}} \text{]} \quad \text{The type derivation will be:} \]

\[
\begin{array}{c}
\text{[LET}^X_{\text{pm}} \text{]} \\
\frac{A \vdash e_1 : \tau_x \quad A \uplus \{ X : \text{Gen}(\tau_x, A) \} \vdash e_2 : \tau}{A \vdash \text{let}_m X = e_1 \text{ in } e_2 : \tau}
\end{array}
\]

Here, \( \text{Gen}(\tau_x, A) \) may be different from \( \text{Gen}(\tau_x, A \uplus \{ s : \sigma_s \}) \). This is caused because there are some type variables \( \sigma_i \) in \( FTV(\tau_x) \) such that they appear free in \( A \) but not in \( A \uplus \{ s : \sigma_s \} \) (they appear only in a previous assumption for \( s \) in \( A \)) or because there are some type variables \( \pi_i \) in \( FTV(\tau_x) \) such that they do not occur free in \( A \) but they do appear free in \( A \uplus \{ s : \sigma_s \} \) (they are added by \( \sigma_s \)). The first group of variables will be generalized in \( \text{Gen}(\tau_x, A \uplus \{ s : \sigma_s \}) \) but not in \( \text{Gen}(\tau_x, A) \). To handle the second group we can create a type substitution \( \pi \) from \( \pi_i \) to fresh type variables. This way \( \text{Gen}(\tau_x, A \uplus \{ s : \sigma_s \}) \) will be a type-scheme more general than \( \text{Gen}(\tau_x, A) \), and by Theorem \( \text{[ID]} \) then \( A \uplus \{ X : \text{Gen}(\tau_x, A \uplus \{ s : \sigma_s \}) \} \vdash e_2 : \tau \). By Theorem \( \text{[ID]} \) we obtain the derivation \( A \uplus \{ X : \text{Gen}(\tau_x, A \uplus \{ s : \sigma_s \}) \} \vdash e_2 : \tau \).

\[ \text{Therefore we can build the type derivation:} \]

\[
\begin{array}{c}
\text{[LET}^X_{\text{pm}} \text{]} \\
\frac{A \uplus \{ s : \sigma_s \} \vdash e_1 : \tau_x \quad (A \uplus \{ s : \sigma_s \}) \uplus \{ X : \text{Gen}(\tau_x, A \uplus \{ s : \sigma_s \}) \} \vdash e_2 : \tau}{A \uplus \{ s : \sigma_s \} \vdash \text{let}_m X = e_1 \text{ in } e_2 : \tau}
\end{array}
\]

\[ \text{[LET}^h_{\text{pm}} \text{]} \quad \text{Similar to the [LET}_m\text{]} \text{ case.} \]

\[ \text{[LET}_p\text{]} \quad \text{Similar to the [LET}^X_{\text{pm}} \text{]} \text{ case, creating a substitution } \pi \text{ that solves the problem of the type variables which were generalized wrt. } A \text{ but not wrt. } A \uplus \{ s : \sigma_s \}. \]

\[ \iff \quad \text{We will proceed again by induction over the size of the derivation tree.} \]

\[ \text{Base Case} \]

\[ \text{When the type derivation only applies the [ID] rule the proof is straightforward.} \]

\[ \text{Induction Step} \]

\[ \text{[APP]} \quad \text{The derivation will have the form:} \]

\[
\begin{array}{c}
\text{[APP]} \\
\frac{A \uplus \{ s : \sigma_s \} \vdash e_1 : \tau' \rightarrow \tau \quad A \uplus \{ s : \sigma_s \} \vdash e_2 : \tau'}{A \uplus \{ s : \sigma_s \} \vdash e_1 e_2 : \tau}
\end{array}
\]

By the Induction Hypothesis then \( A \vdash e_1 : \tau' \rightarrow \tau \) and \( A \vdash e_2 : \tau' \), therefore:

\[
\begin{array}{c}
\text{[APP]} \\
\frac{A \vdash e_1 : \tau' \rightarrow \tau \quad A \vdash e_2 : \tau'}{A \vdash e_1 e_2 : \tau}
\end{array}
\]
— $[\lambda e]$. We have the type derivation:

$$
[\lambda e] \frac{(\mathcal{A} \oplus \{ s : \sigma_s \}) \oplus \{ X_i : \tau_i \} \vdash t : \tau'}{(\mathcal{A} \oplus \{ s : \sigma_s \}) \oplus \{ X_i : \tau_i \} \vdash e : \tau) \\
\frac{\mathcal{A} \oplus \{ s : \sigma_s \} \vdash \lambda t.e : \tau'}{\mathcal{A} \vdash \lambda t.e : \tau' \rightarrow \tau}
$$

Since $s$ is not in $\lambda t.e$, $s$ will be different from all the variables $X_i$ and $(\mathcal{A} \oplus \{ s : \sigma_s \}) \oplus \{ X_i : \tau_i \}$ will be the same as $(\mathcal{A} \oplus \{ X_i : \tau_i \}) \oplus \{ s : \sigma_s \}$. Having $(\mathcal{A} \oplus \{ X_i : \tau_i \}) \oplus \{ s : \sigma_s \} \vdash t : \tau'$ and $(\mathcal{A} \oplus \{ X_i : \tau_i \}) \oplus \{ s : \sigma_s \} \vdash e : \tau$ we can apply the Induction Hypothesis and obtain $\mathcal{A} \oplus \{ X_i : \tau_i \} \vdash t : \tau'$ and $\mathcal{A} \oplus \{ X_i : \tau_i \} \vdash e : \tau$. With these two derivation we can build:

$$
[\lambda e] \frac{\mathcal{A} \oplus \{ X_i : \tau_i \} \vdash t : \tau'}{\mathcal{A} \vdash \lambda t.e : \tau' \rightarrow \tau}
$$

— $[\text{LET}_m]$. Similar to the $[\lambda e]$ case.

— $[\text{LET}_x]$. This case has to deal with the same problems as in $[\text{LET}_pm]$ of the $\implies$ case. We have a type derivation:

$$
[\text{LET}_pm] \frac{\mathcal{A} \oplus \{ s : \sigma_s \} \vdash e_1 : \tau_x}{\mathcal{A} \oplus \{ s : \sigma_s \} \vdash \text{let}_{pm} X = e_1 \text{ in } e_2 : \tau}
$$

Again, the problem is that $\text{Gen}(\tau_x, \mathcal{A} \oplus \{ s : \sigma_s \})$ may not be the same as $\text{Gen}(\tau_x, \mathcal{A})$. As before, there may be variables $\overline{\sigma}$ in $\text{FTV}(\tau_x)$ which appear free in $\mathcal{A} \oplus \{ s : \sigma_s \}$ but not in $\mathcal{A}$, and variables $\overline{\tau}$ in $\text{FTV}(\tau_x)$ which do not occur free in $\mathcal{A} \oplus \{ s : \sigma_s \}$ but they do appear free in $\mathcal{A}$. The first group is not problematic, because they are variables which will be generalised in $\text{Gen}(\tau_x, \mathcal{A})$ but not in $\text{Gen}(\tau_x, \mathcal{A} \oplus \{ s : \sigma_s \})$. To solve the problem with the second group we create a type substitution $\pi$ from $\overline{\tau}$ to fresh variables. This way $\text{Gen}(\tau_x \pi, \mathcal{A})$ will be a more general type-scheme than $\text{Gen}(\tau_x, \mathcal{A} \oplus \{ s : \sigma_s \})$. Applying Theorem 4 then $(\mathcal{A} \oplus \{ s : \sigma_s \}) \oplus \{ X : \text{Gen}(\tau_x \pi, \mathcal{A}) \} \vdash e_2 : \tau$. As $s$ is different from $X$, then $(\mathcal{A} \oplus \{ s : \sigma_s \}) \oplus \{ X : \text{Gen}(\tau_x, \mathcal{A}) \}$ is the same as $(\mathcal{A} \oplus \{ X : \text{Gen}(\tau_x, \mathcal{A}) \}) \oplus \{ s : \sigma_s \}$, so the derivation $(\mathcal{A} \oplus \{ X : \text{Gen}(\tau_x, \mathcal{A}) \}) \oplus \{ s : \sigma_s \} \vdash e_2 : \tau$ is correct. Applying the Induction Hypothesis to this derivation we obtain $\mathcal{A} \oplus \{ X : \text{Gen}(\tau_x \pi, \mathcal{A}) \} \vdash e_2 : \tau$. By Theorem 4a $(\mathcal{A} \oplus \{ s : \sigma_s \}) \pi \vdash e_1 : \tau_x \pi$, which is equal to $\mathcal{A} \oplus \{ s : \sigma_s \} \vdash e_1 : \tau_x \pi$ because $\overline{\sigma}$ do not occur free in $\mathcal{A}$. Applying the Induction Hypothesis to this derivation, we obtain $\mathcal{A} \vdash e_1 : \tau_x \pi$. Therefore we can build the type derivation:

$$
[\text{LET}_pm] \frac{\mathcal{A} \vdash e_1 : \tau_x \pi}{\mathcal{A} \vdash \text{let}_{pm} X = e_1 \text{ in } e_2 : \tau}
$$

— $[\text{LET}_pm]$. Similar to the $[\lambda e]$ case.

— $[\text{LET}_p]$. Similar to the $[\text{LET}_pm]$ case.
b.2) Let be a symbol which does not appear in , and any type. Then 

\[ A \vdash e : \tau \iff A \oplus \{s : \sigma_s\} \vdash e : \tau. \]

\( \rightarrow \) By definition of \( A \vdash e : \tau \), \( A \vdash e : \tau \) and \( \text{critVar}_A(e) = \emptyset \). Since \( s \) does not occur in \( e \) by Theorem 1-b, \( A \oplus \{s : \sigma_s\} \vdash e : \tau \). It will also be true that \( \text{critVar}_{A \oplus \{s : \sigma_s\}}(e) = \emptyset \) because the opaque variables in the patterns will not change by adding the new assumption, and neither the variables appearing in the rest of the expression. Therefore \( A \oplus \{s : \sigma_s\} \vdash e : \tau \).

\( \leftarrow \) By definition of \( A \vdash \{s : \sigma_s\} \vdash e : \tau \), \( A \vdash e : \tau \) and \( \text{critVar}_{A \oplus \{s : \sigma_s\}}(e) = \emptyset \). Since \( s \) does not appear in \( e \), by Theorem 1-b, \( A \vdash e : \tau \). As in the previous case the critical variables of \( e \) will not change by deleting an assumption which is not used, so \( A \vdash e : \tau \).

\[ \square \]

c.1) If \( A \oplus \{X : \tau_x\} \vdash e : \tau \) and \( A \oplus \{X : \tau_x\} \vdash e' : \tau_x \) then \( A \oplus \{X : \tau_x\} \vdash e[X/e'] : \tau \).

We will proceed by induction over the size of the expression \( e \).

**Base Case**

\( \rightarrow \) [ID] If \( s \neq X \) then \( s[X/e'] \equiv s \). On the contrary, if \( s = X \) then the derivation will be:

\[ \text{[ID]} \quad A \vdash X : \tau_x \]
\[ X[X/e'] \equiv e', \text{ and the type derivation } A \vdash e' : \tau_x \text{ comes from the hypothesis.} \]

**Induction Step**

\( \rightarrow \) [APP] Just the application of the Induction Hypothesis.

\( \rightarrow \) [A] We can assume that \( \lambda t.e \) is such that the variables \( \overline{X}_t \) in its pattern do not appear in \( A \oplus \{X : \tau_x\} \) nor in \( FV(e) \). The derivation will have the form:

\[ \text{[A]} \quad (A \oplus \{X : \tau_x\}) \vdash t : \tau' \]
\[ (A \oplus \{X : \tau_x\}) \vdash e : \tau \]
\[ A \vdash \{X : \tau_x\} \vdash \lambda t.e : \tau' \rightarrow \tau \]

As \( X \) is different from \( \overline{X}_t \) then \( (\lambda t.e)[X/e'] \equiv \lambda t.(e[X/e']) \), so the first derivation remains the same. We have from the hypothesis that \( A \vdash e' : \tau_x \). Since none of the \( \overline{X}_t \) appear in \( e' \) then by Theorem 1-b we can...
add assumptions over that variables and obtain a derivation \((A \cup \{X : \tau_x\}) \cup \{X_i : \tau_i\} \vdash e' : \tau_x\). Because \(X \neq X_i\) for all \(i\) then by Observation 3 \((A \cup \{X : \tau_x\}) \cup \{X_i : \tau_i\} \vdash X : \tau_x\). We have
\((A \cup \{X_i : \tau_i\}) \cup \{X : \tau_x\} \vdash e : \tau\) and \((A \cup \{X_i : \tau_i\}) \cup \{X : \tau_x\} \vdash e' : \tau_x\), so applying the Induction Hypothesis we obtain \((A \cup \{X_i : \tau_i\}) \cup \{X : \tau_x\} \vdash e[X/e'] : \tau\). Therefore we can build a new derivation:

\[
\begin{align*}
(A \cup \{X : \tau_x\}) \cup \{X_i : \tau_i\} &\vdash t : \tau' \\
\begin{array}{c}
[A]
\end{array} &
(A \cup \{X : \tau_x\}) \cup \{X_i : \tau_i\} \vdash e[X/e'] : \tau \\
A \cup \{X : \tau_x\} &\vdash \lambda t.(e[X/e']) : \tau' \rightarrow \tau
\end{align*}
\]

\[\text{[LET}_m\text{]}\] The proof is similar to the \([A]\) case, provided that the variables of the pattern \(t\) do not occur in \(\text{FV}(e')\) nor in \(A \cup \{X : \tau_x\}\).

\[\text{[LET}_m'^{X}\text{]}\] In this case \(Y\) is a fresh variable. The type derivation will be:

\[
\begin{array}{c}
\text{[LET}_m'^{X}\text{]}
\end{array} \\
A \cup \{X : \tau_x\} \vdash e_1 : \tau_x \\
(A \cup \{X : \tau_x\}) \cup \{Y : \text{Gen}(\tau_x, A \cup \{X : \tau_x\})\} \vdash e_2 : \tau \\
A \cup \{X : \tau_x\} \vdash \text{let}_m' Y = e_1 \text{ in } e_2 : \tau
\]

By the Induction Hypothesis \(A \cup \{X : \tau_x\} \vdash e_1[X/e'] : \tau_x\). \(X \neq Y\) and \(Y \not\in \text{FV}(e')\), so by Theorem \([\Box]\) we can add an assumption over the variable \(Y\) and get a derivation \((A \cup \{X : \tau_x\}) \cup \{Y : \text{Gen}(\tau_x, A \cup \{X : \tau_x\})\} \vdash e' : \tau_x\). By Observation 3 \((A \cup \{X : \tau_x\}) \cup \{Y : \text{Gen}(\tau_x, A \cup \{X : \tau_x\})\} \vdash (A \cup \{Y : \text{Gen}(\tau_x, A \cup \{X : \tau_x\})\}) \cup \{X : \tau_x\} \vdash X : \tau_x\), so by the Induction Hypothesis \((A \cup \{Y : \text{Gen}(\tau_x, A \cup \{X : \tau_x\})\}) \cup \{X : \tau_x\} \vdash e_2[X/e'] : \tau\). Again by Observation 3 \((A \cup \{X : \tau_x\}) \cup \{Y : \text{Gen}(\tau_x, A \cup \{X : \tau_x\})\} \vdash (A \cup \{X : \tau_x\}) \cup \{Y : \text{Gen}(\tau_x, A \cup \{X : \tau_x\})\} \vdash X : \tau_x\)

Therefore we can construct a derivation:

\[
\begin{array}{c}
\text{[LET}_m'^{X}\text{]}
\end{array} \\
A \cup \{X : \tau_x\} \vdash e_1[X/e'] : \tau_x \\
(A \cup \{X : \tau_x\}) \cup \{Y : \text{Gen}(\tau_x, A \cup \{X : \tau_x\})\} \vdash e_2[X/e'] : \tau \\
A \cup \{X : \tau_x\} \vdash \text{let}_m' Y = e_1[X/e'] \text{ in } e_2[X/e'] : \tau
\]

\[\text{[LET}_m'^{h}\text{]}\] Equal to the \([\text{LET}_m]\) case.

\[\text{[LET}_p\text{]}\] The proof follows the same ideas as \([\text{LET}_m]\) and \([\text{LET}_m'^{X}\text{]}\).
\[\square\]

c.2) If \(A \cup \{X : \tau_x\} \vdash e \vdash \tau\) and \(A \cup \{X : \tau_x\} \vdash \bullet e' : \tau_x\) then \(A \cup \{X : \tau_x\} \vdash \bullet e[X/e'] \vdash \tau\).

From the definition of \(\vdash \bullet\) we know that \(A \cup \{X : \tau_x\} \vdash e : \tau\), \(A \cup \{X : \tau_x\} \vdash e' : \tau_x\), \(\text{critVar}(A \cup \{X : \tau_x\})(e) = \emptyset\) and \(\text{critVar}(A \cup \{X : \tau_x\})(e') = \emptyset\). Then by Theorem \([\Box]\) we also know that \(e \vdash \tau\). By Lemma \([\Box]\) we also know that \(e[X/e'] \vdash \tau\). So by definition \(A \cup \{X : \tau_x\} \vdash \bullet e[X/e'] \vdash \tau\). \(\square\)

d.1) If \(A \vdash \{s : \sigma\} \vdash e : \tau\) and \(\sigma' > \sigma\), then \(A \vdash \{s : \sigma'\} \vdash e : \tau\).
Base Case
We have a type derivation:

\[\text{[ID]} \quad \mathcal{A} \vdash \{ s : \sigma \} \vdash s : \tau\]

where \( \sigma \succ \tau \). By Definition of generic instance, since \( \sigma' \succ \sigma \) then \( \sigma' \succ \tau \). So we can build the derivation:

\[\text{[ID]} \quad \mathcal{A} \vdash \{ s : \sigma' \} \vdash s : \tau\]

Induction Step

- \text{[APP]} We have a type derivation:

\[\text{[APP]} \quad \mathcal{A} \vdash \{ s : \sigma \} \vdash e_1 : \tau' \rightarrow \tau \quad \mathcal{A} \vdash \{ s : \sigma \} \vdash e_2 : \tau' \]

\[\mathcal{A} \vdash \{ s : \sigma \} \vdash e_1 e_2 : \tau\]

By the Induction Hypothesis we have that \( \mathcal{A} \vdash \{ s : \sigma' \} \vdash e_1 : \tau' \rightarrow \tau \) and \( \mathcal{A} \vdash \{ s : \sigma' \} \vdash e_2 : \tau' \). Then we can construct a type derivation with the more general assumptions:

\[\text{[APP]} \quad \mathcal{A} \vdash \{ s : \sigma' \} \vdash e_1 : \tau' \rightarrow \tau \quad \mathcal{A} \vdash \{ s : \sigma' \} \vdash e_2 : \tau' \]

\[\mathcal{A} \vdash \{ s : \sigma' \} \vdash e_1 e_2 : \tau\]

- \[A\] We can assume that \( s \) is different from all the variables \( X_i \). The type derivation will be:

\[\text{[A]} \quad (\mathcal{A} \vdash \{ s : \sigma \}) \vdash \{ X_i : \tau_i \} \vdash t : \tau' \quad (\mathcal{A} \vdash \{ s : \sigma \}) \vdash \{ X_i : \tau_i \} \vdash e : \tau \]

\[\mathcal{A} \vdash \{ s : \sigma \} \vdash \lambda t.e : \tau' \rightarrow \tau\]

Since \( s \) is different from the variables \( X_i \), then \((\mathcal{A} \vdash \{ s : \sigma \}) \vdash \{ X_i : \tau_i \} \) is the same as \((\mathcal{A} \vdash \{ X_i : \tau_i \}) \vdash \{ s : \sigma \}\). Therefore \((\mathcal{A} \vdash \{ X_i : \tau_i \}) \vdash \{ s : \sigma \} \vdash t : \tau'\) and \((\mathcal{A} \vdash \{ X_i : \tau_i \}) \vdash \{ s : \sigma \} \vdash e : \tau\). By the Induction Hypothesis we have that \((\mathcal{A} \vdash \{ X_i : \tau_i \}) \vdash \{ s : \sigma' \} \vdash t : \tau'\) and \((\mathcal{A} \vdash \{ X_i : \tau_i \}) \vdash \{ s : \sigma' \} \vdash e : \tau\) and changing again the order in the assumptions we can build a derivation:

\[\text{[A]} \quad (\mathcal{A} \vdash \{ s : \sigma' \}) \vdash \{ X_i : \tau_i \} \vdash t : \tau' \quad (\mathcal{A} \vdash \{ s : \sigma' \}) \vdash \{ X_i : \tau_i \} \vdash e : \tau \]

\[\mathcal{A} \vdash \{ s : \sigma' \} \vdash \lambda t.e : \tau' \rightarrow \tau\]

- \text{[LET}_m] The proof is similar to the \([A]\) case.

- \text{[LET}_p\text{]} We assume that \( s \neq X \). The type derivation is:

\[\text{[LET}_p\text{]} \quad (\mathcal{A} \vdash \{ s : \sigma \}) \vdash e_1 : \tau_x \]

\[\mathcal{A} \vdash \{ s : \sigma \} \vdash \text{let}_p X = e_1 \text{ in } e_2 : \tau\]

By the Induction Hypothesis we have \( \mathcal{A} \vdash \{ s : \sigma' \} \vdash e_1 : \tau_x \). As \( \sigma' \succ \sigma \) then by Observation \([2]\) \( \text{FTV}(\sigma') \subseteq \text{FTV}(\sigma) \). Therefore \( \text{FTV}(\mathcal{A} \vdash \{ s : \sigma' \}) = \text{FTV}(\mathcal{A}_x) \cup \text{FTV}(\sigma') \subseteq \text{FTV}(\mathcal{A}_x) \cup \text{FTV}(\sigma) = \text{FTV}(\mathcal{A} \vdash \{ s : \sigma \}) \), being \( \mathcal{A}_x \) the result of deleting from \( \mathcal{A} \) all the assumptions for the symbol \( s \). With this information it is clear that \( \text{Gen}(\tau_x, \mathcal{A} \vdash \{ s : \sigma' \}) \succ \text{Gen}(\tau_x, \mathcal{A} \vdash \{ s : \sigma \}) \)
because more variables could be generalized in $Gen(\tau_x, A \oplus \{s : \sigma\})$. Then by the Induction Hypothesis $(A \oplus \{s : \sigma\}) \oplus \{X : Gen(\tau_x, A \oplus \{s : \sigma\})\} \vdash e_2 : \tau$. As $s \neq X$ then we can change the order of the assumptions and obtain a derivation $(A \oplus \{X : Gen(\tau_x, A \oplus \{s : \sigma\})\}) \oplus \{s : \sigma\} \vdash e_2 : \tau$. Again by the Induction Hypothesis $(A \oplus \{X : Gen(\tau_x, A \oplus \{s : \sigma\})\}) \oplus \{s : \sigma\} \vdash e_2 : \tau$.

With these derivations we can build the one we were trying to construct:

$$\begin{array}{c}
A \oplus \{s : \sigma\} \vdash e_1 : \tau_x \\
[\text{LET}_p^X] \quad (A \oplus \{s : \sigma\}) \oplus \{X : Gen(\tau_x, A \oplus \{s : \sigma\})\} \vdash e_2 : \tau \\
A \oplus \{s : \sigma\} \vdash \text{let}_p X = e_1 \text{ in } e_2 : \tau
\end{array}$$

- [LET$_{pm}^h$] Similar to the [A] case.
- [LET$_p^m$] The proof is similar to the [LET$_p^X$] case.

\[\square\]

**Theorem 2 (Type preservation of the let transformation).**

Assume $A \vdash^* e : \tau$ and let $P \equiv \{f_{X_i} : i_1 \rightarrow X_i\}$ be the rules of the projection functions needed in the transformation of $e$ according to Fig. 3. Let also $A'$ be the set of assumptions over that functions, defined as $A' \equiv \{f_{X_i} : Gen(\tau_{X_i}, A)\}$, where $A \vdash^* \lambda i. X_i : \tau_{X_i} | i X_i$. Then $A \oplus A' \vdash^* TRL(e) : \tau$ and $wt_{A \oplus A'}(P)$.

**Proof.** By structural induction over the expression $e$.

**Base Case**

- $s$) Straightforward.

**Induction Step**

- $e_1 \ e_2$) We have the type derivation:

$$\begin{array}{c}
A \vdash e_1 : \tau_1 \rightarrow \tau \\
\text{APP} \quad A \vdash e_2 : \tau_1 \\
\quad A \vdash e_1 \ e_2 : \tau
\end{array}$$

Let be $A^1$ and $A^2$ the assumptions over the projection functions needed in $e_1$ and $e_2$ respectively. The by the Induction Hypothesis $A \oplus A^1 \vdash TRL(e_1)$ and $A \oplus A^2 \vdash TRL(e_2)$. Clearly the set of assumptions $A'$ over the projection functions needed in the whole expression is $A^1 \oplus A^2$. Then by Theorem 1 both derivations $A \oplus A' \vdash TRL(e_1)$ and $A \oplus A' \vdash TRL(e_2)$ are valid, and we can construct the type derivation:

$$\begin{array}{c}
A \oplus A' \vdash TRL(e_1) : \tau_1 \rightarrow \tau \\
\text{APP} \quad A \oplus A' \vdash TRL(e_2) : \tau_1 \\
\quad A \oplus A' \vdash TRL(e_1) \ TRL(e_2) : \tau
\end{array}$$

- let$_K X = e_1 \text{ in } e_2$) There are two cases, depending on the $K$:

  **let$_m X = e_1 \text{ in } e_2$**

  The type derivation will be
\( A \oplus \{ X : \tau \} \vdash X : \tau \)
\( A \vdash e_1 : \tau \)
\( \text{[LET]_m} \quad A \vdash _m X = e_1 \text{ in } e_2 : \tau \)

By the Induction Hypothesis \( A \vdash TRL(e_1) : \tau \) and \( A \oplus \{ X : \tau \} \vdash TRL(e_2) : \tau \). Then we can build the type derivation

\( A \oplus \{ X : \tau \} \vdash X : \tau \)
\( A \vdash TRL(e_1) : \tau \)
\( \text{[LET]_m} \quad A \vdash TRL(e_1) \text{ in } TRL(e_2) : \tau \)

\( \text{let}_p X = e_1 \text{ in } e_2 : \tau \)

The type derivation for the original expression is

\( A \oplus \{ X : \tau \} \vdash X : \tau \)
\( A \vdash e_1 : \tau \)
\( \text{[LET]_m} \quad A \vdash \{ X : \text{Gen}(\tau, A) \} \vdash e_2 : \tau \)
\( \text{[LET]_m} \quad A \vdash _m X = e_1 \text{ in } e_2 : \tau \)

By the Induction Hypothesis \( A \vdash TRL(e_1) : \tau \) and \( A \oplus \{ X : \text{Gen}(\tau, A) \} \vdash TRL(e_2) : \tau \). Then we can build the type derivation

\( A \oplus \{ X : \tau \} \vdash X : \tau \)
\( A \vdash TRL(e_1) : \tau \)
\( \text{[LET]_m} \quad A \oplus \{ X : \text{Gen}(\tau, A) \} \vdash TRL(e_2) : \tau \\
\text{[LET]_m} \quad A \vdash _m X = TRL(e_1) \text{ in } TRL(e_2) : \tau \)

\(- \text{let}_m X = e_1 \text{ in } e_2 : \tau 

The type derivation for the original expression is

\( A \vdash e_1 : \tau \)
\( \text{[LET]_m} \quad A \oplus \{ X : \text{Gen}(\tau, A) \} \vdash e_2 : \tau \\
\text{[LET]_m} \quad A \vdash _m X = e_1 \text{ in } e_2 : \tau \)

By the Induction Hypothesis \( A \vdash TRL(e_1) : \tau \) and \( A \oplus \{ X : \text{Gen}(\tau, A) \} \vdash TRL(e_2) : \tau \). The type derivation \( A \oplus \{ X : \tau \} \vdash X : \tau \) is trivial, so we can build the type derivation

\( A \oplus \{ X : \tau \} \vdash X : \tau \)
\( A \vdash TRL(e_1) : \tau \)
\( \text{[LET]_m} \quad A \oplus \{ X : \text{Gen}(\tau, A) \} \vdash TRL(e_2) : \tau \\
\text{[LET]_m} \quad A \vdash _m X = TRL(e_1) \text{ in } TRL(e_2) : \tau \)

\(- \text{let}_m t = e_1 \text{ in } e_2 : \tau 

In this case the original type derivation is:

\( A \oplus \{ X \vdash t : \tau \}
\( A \vdash e_1 : \tau \)
\( \text{[LET]_m} \quad A \oplus \{ X : \tau \} \vdash e_2 : \tau \\
\text{[LET]_m} \quad A \vdash _m t = e_1 \text{ in } e_2 : \tau \)
It is easy to see that if $A \oplus \{X_i : \tau_i\} \vdash t : \tau_i$ then $A \vdash \lambda t. X_i : \tau_i \rightarrow \tau_i$. The assumptions over the projections functions in $A'$ will be $\{f_{X_i} : Gen(\tau'_i \rightarrow \tau'_i, A')\}$, where $A \equiv \lambda t. X_i : \tau_i \rightarrow \tau_i$. Since $A \vdash \lambda t. X_i : \tau_i \rightarrow \tau_i$ we can assume that $A \pi X_i = A$ (Observation 4), and by Theorem 5 we know that exists a type substitution $\pi$ such that $A \pi X_i \pi = A \pi = A$ and $(\tau'_i \rightarrow \tau'_i) \pi = \tau_i \rightarrow \tau_i$. Therefore we can be sure that $Gen(\tau'_i \rightarrow \tau'_i, A) \succ \tau_i \rightarrow \tau_i$, because $\pi$ substitutes only the type variables in $\tau'_i \rightarrow \tau'_i$ which are generalized in $Gen(\tau'_i \rightarrow \tau'_i, A)$. If $A'$ contains all the assumptions over the projection functions needed in the whole expression, it contains assumptions over projection functions in both cases is the same (as $t$ is a pattern we use $[LET_{pm}]$, and this rule acts equal to $[LET_m]$) and the transformed expressions are the same.

- $let_{pm} \ t = e_1 \ in \ e_2$) This case is equal to the previous one because the derivation of the original expression in both cases is the same (as $t$ is a pattern we use $[LET_{pm}]$, and this rule acts equal to $[LET_m]$) and the transformed expressions are the same.

- $let_p \ t = e_1 \ in \ e_2$) The type derivation will be:
\[
\begin{align*}
\mathcal{A} \oplus \{X_i : \tau_i\} & \vdash t : \tau_i \\
\mathcal{A} \vdash e_1 : \tau_i \\
[\text{LET}_p] & \quad \mathcal{A} \oplus \{X_i : \text{Gen}(\tau_i, \mathcal{A})\} \vdash e_2 : \tau \\
& \quad \mathcal{A} \vdash \text{let}_p \ t = e_1 \ in \ e_2 : \tau
\end{align*}
\]

As in the previous case, \(\mathcal{A}'\) will be \(\{f_X : \text{Gen}(\tau'_i \rightarrow \tau'_i, \mathcal{A})\}\), where \(\mathcal{A} \parallel \lambda \cdot X : \tau_i \rightarrow \tau'_i \parallel \pi_X\). In addition, \(\mathcal{A}\pi_X = A\) (by the Observation 7). \(\text{Gen}(\tau'_i \rightarrow \tau'_i, \mathcal{A}) \triangleright \tau_i \rightarrow \tau_i\) and \(\mathcal{A}' \equiv \mathcal{A}^1 \oplus \mathcal{A}^2 \oplus \mathcal{A}'\). Then we can build a type derivation:

\[
\begin{align*}
\mathcal{A} \oplus \mathcal{A}' & \oplus \{Y : \tau_i\} \vdash Y : \tau_i \\
\mathcal{A} & \oplus \mathcal{A}' \vdash \text{TRL}(e_1) : \tau_i \\
[\text{LET}_p] & \quad \mathcal{A}'_1 \vdash \text{let}_m \ X_1 = f_X, Y \ in \ \ldots \ in \ \text{TRL}(e_2) : \tau \\
& \quad \mathcal{A} \oplus \mathcal{A}' \vdash \text{let}_p \ Y = \text{TRL}(e_1) \ in \ \text{let}_p \ X_1 = f_X, Y \ in \ \text{TRL}(e_2) : \tau
\end{align*}
\]

where the derivation \(\mathcal{A}_Y \vdash \text{let}_m \ X_1 = f_X, Y \ in \ \ldots \ in \ \text{TRL}(e_2) : \tau\) is

\[
\begin{align*}
[\text{ID}] & \quad \mathcal{A}'_1 \vdash \text{let}_m \ X_1 = f_X, Y \ in \ \ldots \ in \ \text{TRL}(e_2) : \tau \\
& \quad \mathcal{A}'_1 \vdash f_X, Y : \tau_i \\
[\text{APP}] & \quad \mathcal{A}'_1 \vdash f_X, Y : \tau_i \\
& \quad \mathcal{A}'_2 \vdash Y : \tau_i \\
& \quad \mathcal{A}'_3 \vdash Y : \tau_i \\
& \quad \mathcal{A}'_4 \vdash f_X, Y : \tau_i \\
[\text{LET}_p] & \quad \mathcal{A}'_5 \vdash \text{let}_p \ Y = \text{TRL}(e_1) \ in \ \text{let}_p \ X_1 = f_X, Y \ in \ \ldots \ in \ \text{TRL}(e_2) : \tau
\end{align*}
\]

being \(\mathcal{A}'_1 \equiv \mathcal{A} \oplus \mathcal{A}' \oplus \{Y : \text{Gen}(\tau_i, \mathcal{A} \oplus \mathcal{A}')\}\) and \(\mathcal{A}'_1 \equiv \mathcal{A}'_{i-1} \oplus \{X_{i-1} : \text{Gen}(\tau_{i-1}, \mathcal{A}'_{i-1})\}\).

As in the previous case, all the derivations \(\mathcal{A}'_1 \vdash f_X, Y : \tau_i\) are valid, because \(\mathcal{A}'_1 \vdash Y : \tau_i\). Notice that \(\text{Gen}(\tau_i, \mathcal{A}) = \text{Gen}(\tau_i, \mathcal{A} \oplus \mathcal{A}')\), as Observation 7 states, since \(\text{FTV}(\mathcal{A}) = \text{FTV}(\mathcal{A} \oplus \mathcal{A}')\). For the same reason, \(\text{Gen}(\tau_i, \mathcal{A}) = \text{Gen}(\tau_i, \mathcal{A}')\), so the chain of let expressions will collect the same set of assumptions over the variables \(X_i : \{X_i : \text{Gen}(\tau_i, \mathcal{A})\}\). By the Induction Hypothesis, we know that \(\mathcal{A} \oplus \{X_i : \text{Gen}(\tau_i, \mathcal{A})\} \oplus \mathcal{A}^2 \vdash \text{TRL}(e_2) : \tau\) and by Theorem 7 we can add the assumptions \(\mathcal{A}^1 \oplus \mathcal{A}^2 \oplus \{Y : \text{Gen}(\tau_i, \mathcal{A} \oplus \mathcal{A}')\}\) and obtain \(\mathcal{A} \oplus \{X_i : \text{Gen}(\tau_i, \mathcal{A})\} \oplus \mathcal{A}^2 \oplus \mathcal{A}^2 \oplus \{Y : \text{Gen}(\tau_i, \mathcal{A} \oplus \mathcal{A}')\} \vdash \text{TRL}(e_2) : \tau\). Then reorganizing the assumptions we obtain \(\mathcal{A} \oplus \mathcal{A}' \oplus \{Y : \text{Gen}(\tau_i, \mathcal{A} \oplus \mathcal{A}')\} \oplus \{X_i : \text{Gen}(\tau_i, \mathcal{A})\} \vdash \text{TRL}(e_2) : \tau\). Since \(\text{Gen}(\tau_i, \mathcal{A}) = \text{Gen}(\tau_i, \mathcal{A}')\) then the previous derivation is equal to \(\mathcal{A}'_{n+1} \vdash \text{TRL}(e_2) : \tau\).

In all the cases it is true that \(\text{ut}_{\mathcal{A} \oplus \mathcal{A}'}(P)\). Let \(X_i\) a data variable which is projected in the transformed expression, and \(t_i\) the compound pattern of a let expression where it appears. By Observation 7 we know that in the derivation \(\mathcal{A} \vdash^* e : \tau\) will appear a derivation \(\mathcal{A} \oplus \mathcal{A}'' \oplus \{X_i : \tau'_i\} \vdash t_i : \tau_i\) for a set of assumptions \(\mathcal{A}''\) over some variables and \(X_i\) will not be opaque in \(t_i\) wrt. \(\mathcal{A} \oplus \mathcal{A}'' \oplus \{X_i : \tau'_i\}\). Then it is clear that \(\mathcal{A} \vdash \lambda t_i.X_i : \tau_i \rightarrow \tau'_i\) and by Theorem 8 the type inference \(\mathcal{A} \parallel \lambda t_i.X_i : \tau_i \parallel X_i\) will be correct. By Theorem 6 \(\mathcal{A}\pi_X \vdash \lambda t_i.X_i : \tau_i\), and since by Observation 6 \(\mathcal{A}\pi_X = \mathcal{A}\), then \(\mathcal{A} \vdash \lambda t_i.X_i : \tau_i\).
\(\tau_{X_i}\) is a valid derivation. Clearly \(X_i\) is not opaque in \(t_i\) wrt. \(\mathcal{A}\), because only the assumptions for non variable symbols are used. Then \(critVar_{A}(\lambda t_i.X_i) = \emptyset\), so \(\mathcal{A} \vdash^{*} \lambda t_i.X_i : \tau_{X_i}\) and \(\mathcal{A} \vdash^{*} \lambda t_i.X_i : \tau_{X_i}\). \(A'\) contains assumptions over projection functions, and they do not appear in \(\lambda t_i.X_i\), so by Theorem 1b we can add these assumptions and obtain \(\mathcal{A} \vdash A' \vdash^{*} \lambda t_i.X_i : \tau_{X_i}\). We know that in \(A'\) there will appear an assumption \(\{f_{X_i} : Gen(\tau_{X_i}, \mathcal{A})\}\) for the projection function of the variable \(X_i\), with rule \(f_{X_i} : t_i \rightarrow X_i\). We know that \(FTV(\mathcal{A}) = FTV(\mathcal{A} \oplus \mathcal{A'})\) because since all the assumptions in \(\mathcal{A}\) are of the form \(Gen(\tau_{X_i}, \mathcal{A})\) they will not add any type variable, and since no \(f_{X_i}\) appears in \(\mathcal{A}\) they will not shadow any assumption. Then \(\tau_{X_i}\) will be a variant of \(Gen(\tau_{X_i}, \mathcal{A})\).

Therefore for every data variable \(X_i\) which is projected then \(\mathcal{A} \vdash \lambda t_i.X_i : \tau_{X_i}\) and \(\tau_{X_i}\) is a variant of \(\mathcal{A} \vdash \mathcal{A'}(f_{X_i}) = Gen(\tau_{X_i}, \mathcal{A})\), so all the program rules \(f_{X_i} : t_i \rightarrow X_i \in \mathcal{P}'\) are well-typed wrt. \(\mathcal{A} \vdash \mathcal{A'}\) and \(\mathcal{w}_{\mathcal{A} \vdash \mathcal{A'}}(\mathcal{P}')\).

**Theorem 3** (Subject Reduction wrt \(\vdash\)).

If \(\mathcal{A} \vdash e : \tau\) and \(\mathcal{w}_{\mathcal{A}}(\mathcal{P})\) and \(\mathcal{P} \vdash e \rightarrow^{\ell} e'\) then \(\mathcal{A} \vdash e' : \tau\).

**Proof.** We proceed by case distinction over the rule of the let-rewriting relation \(\rightarrow^{\ell}\) (Fig. 4) that we use to reduce \(e\) to \(e'\):

- (Fapp) If we reduce an expression \(e\) using the (Fapp) rule is because \(e\) has the form \(f_{t_1\theta} \ldots t_n\theta\) (being \(f_{t_1} \ldots t_n \rightarrow r\) a rule in \(\mathcal{P}\) and \(\theta \in \mathcal{P}Subst\)) and \(e'\) is \(r\theta\). In this case we want to prove that \(\mathcal{A} \vdash r\theta : \tau\). Since \(\mathcal{w}_{\mathcal{A}}(\mathcal{P})\), then \(\mathcal{A} \vdash^{*} \lambda t_1 \ldots t_n.r : \tau_1 \rightarrow \ldots \rightarrow \tau_n \rightarrow \tau'\), being \(\tau_1 \rightarrow \ldots \rightarrow \tau_n \rightarrow \tau'\) a variant of \(\mathcal{A}(f)\). We assume that the variables of the patterns \(\overline{t_i}\) do not appear in \(\mathcal{A}\) or in \(\mathcal{R}(\theta)\). The tree for this type derivation will be:

\[
\frac{\mathcal{A} \vdash t_n : \tau'_n \quad \mathcal{A} \vdash r : \tau'}{\mathcal{A} \vdash \tau_n \rightarrow \tau'}
\]

where \(\mathcal{A}_j \equiv (\ldots (\mathcal{A} \oplus \{X_{i_1} : \tau'_{i_1}\}) \oplus \ldots) \oplus \{X_{j_1} : \tau'_{j_1}\}\) and \(X_{j_1}\) is the \(i\)-th variable of the pattern \(t_j\). We can write \(\mathcal{A}_n\) as \(\mathcal{A} \oplus \mathcal{A'}\), being \(A'\) the set of assumption over the variables of the patterns. As these variables are all different (the left hand side of the rules is linear), by Theorem 1b we can add the rest of the assumptions to the \(\mathcal{A}_j\) to get \(\mathcal{A}_n\) and the derivation will remain valid, so \(\forall j \in [1, n]. \mathcal{A} \vdash t_j : \tau'_j\). Besides \(critVar_{A}(\lambda t_1 \ldots t_n.r) = \emptyset\), so \(\sigma\) every variable \(X_{j_i}\) which appears in \(r\) is transparent in the pattern \(t_j\) where it comes.

It is a premise that \(\mathcal{A} \vdash f_{t_1\theta} \ldots t_n\theta : \tau\), and the tree of the type derivation will be:

\[
\frac{\mathcal{A} \vdash t_1\theta \ldots \tau_{n-2}\theta : \tau_{n-1} \rightarrow (\tau_n \rightarrow \tau)}{\mathcal{A} \vdash t_n\theta : \tau_n}
\]

\[
\frac{\mathcal{A} \vdash f_{t_1\theta} \ldots t_{n-2}\theta : \tau_{n-1} \rightarrow \tau_n \rightarrow \tau}{\mathcal{A} \vdash f_{t_1\theta} \ldots t_{n}\theta : \tau_n \rightarrow \tau}
\]

\[
\frac{\mathcal{A} \vdash f_{t_1\theta} \ldots t_{n}\theta : \tau_n \rightarrow \tau}{\mathcal{A} \vdash f_{t_1\theta} \ldots t_{n-1}\theta : \tau_{n-1} \rightarrow \tau_n \rightarrow \tau}
\]

35
where the type derivation \( A \vdash f \ t_1 \ldots t_{n-2} : \tau_{n-1} \rightarrow (\tau_n \rightarrow \tau) \) is

\[
\begin{align*}
\frac{[\text{ID}] \quad A \vdash f : \tau_1 \rightarrow \ldots \rightarrow \tau_n \rightarrow \tau \quad A \vdash f : \tau_n \rightarrow \tau} \hline
A \vdash t_1 \theta : \tau_1
\end{align*}
\]

\[
\begin{align*}
\frac{[\text{APP}] \quad \vdots} \hline
A \vdash f \ t_1 \theta \ldots t_{n-2} : \tau_{n-1} \rightarrow (\tau_n \rightarrow \tau)
\end{align*}
\]

Because of that, we know that \( b) \quad \forall j \in [1,n], \ A \vdash t_j \theta : \tau_j \quad \text{and} \quad A \vdash f : \tau_1 \rightarrow \ldots \rightarrow \tau_n \rightarrow \tau, \) being \( \tau_1 \rightarrow \ldots \rightarrow \tau_n \rightarrow \tau \) a generic instance of the type \( A(f). \) Then there will exists a type substitution \( \pi \) such that \( (\tau_1' \rightarrow \ldots \rightarrow \tau_n' \rightarrow \tau')\pi = \tau_1 \rightarrow \ldots \rightarrow \tau_n \rightarrow \tau, \) so \( \forall j \in [1,n], \ \tau_j'\pi = \tau_j \) and \( \tau'\pi = \tau. \) What is more, \( \text{Dom}(\pi) \) does not contain any free type variable in \( A, \) since \( \pi \) transforms a variant of the type of \( A(f) \) into a generic instance of the type of \( A(f). \) Then by Theorem \( \text{[1-a]} \) \( A_n\pi \vdash t_j : \tau_j'\pi, \) which is equal to \( c) \ A \oplus A'\pi \vdash t_j : \tau_j'\pi. \)

With \( a), \ b) \) and \( c) \) and by Lemma \( \text{[1]} \) we can state that for every transparent variable \( X_{ji} \) in \( r \) then \( A \vdash X_{ji}\theta : \tau_{ji}'\pi. \) None of the variables in \( A' \) appear in \( X_{ji}\theta, \) so by Theorem \( \text{[1-b]} \) we can add these assumptions and obtain \( A_n \vdash X_{ji}\theta : \tau_{ji}'\pi. \) According to the first derivation, we have \( A_n \vdash r : \tau'. \) Here we can apply the Theorem \( \text{[1-a]} \) again and get a derivation \( A_n\pi \vdash r : \tau'\pi. \) Because \( A_n\pi \vdash X_{ji}\theta : \tau_{ji}'\pi, \) then by Theorem \( \text{[1-c]} \) \( A_n\pi \vdash r\theta : \tau'\pi. \) As we have eliminated the variables in the expression, by Theorem \( \text{[1-b]} \) we can delete their assumptions, obtaining a derivation \( A\pi \vdash r\theta : \tau'\pi \) (remember that \( A_n \) is \( A \oplus A' \)). And finally using the information we have about \( \pi, \) this derivation is equal to \( A \vdash r\theta : \tau, \) the derivation we wanted to obtain.

- (LetIn) In this case \( A \vdash e_1e_2 : \tau \) and \( P \vdash e_1e_2 \rightarrow^1 \text{let}_m \ X = e_2 \text{ in } e_1. \) The type derivation of \( e_1e_2 \) will have the form:

\[
\begin{align*}
\quad [\text{APP}] \quad A \vdash e_1 : \tau_1 \rightarrow \tau \quad A \vdash e_2 : \tau_1 \quad A \vdash e_1e_2 : \tau
\end{align*}
\]

With this information we could build a type judgment for the \( \text{let}_m \) expression

\[
\begin{align*}
[\text{LET}_m] \quad A \oplus \{ X : \tau_1 \} \vdash e_1 : \tau_1 \rightarrow \tau \quad A \oplus \{ X : \tau_1 \} \vdash X : \tau_1 \quad A \oplus \{ X : \tau_1 \} \vdash e_1X : \tau
\end{align*}
\]

\[
A \vdash \text{let}_m \ X = e_2 \text{ in } e_1X : \tau
\]

\( A \oplus \{ X : \tau_1 \} \vdash X : \tau_1 \) is a valid derivation because is an application of the \( [\text{ID}] \) rule. And since \( X \) is a fresh variable, by Theorem \( \text{[1-b]} \) we can add the assumption and obtain \( A \oplus \{ X : \tau_1 \} \vdash e_1 : \tau_1 \rightarrow \tau. \)

- (Bind) We will distinguish between the \( \text{let}_m \) and the \( \text{let}_p \) case. In both cases we assume that the variable \( X \) is fresh.

\( \text{let}_m \) In the \( \text{let}_m \) case the type derivation will have the form:

\[
\begin{align*}
[\text{LET}_m] \quad A \oplus \{ X : \tau_1 \} \vdash X : \tau_1 \quad A \vdash t : \tau_2 \quad A \oplus \{ X : \tau_1 \} \vdash e : \tau
\end{align*}
\]

\[
A \vdash \text{let}_m \ X = t \text{ in } e \text{ in } e_2X : \tau
\]
As \( X \) is different from all the variables \( X_i \) of the pattern \( t \), then by Theorem 1b we can add the assumption over the variable \( X \) and obtain the derivation \( A \vdash \{ X : \tau_i \} \vdash t : \tau_i \). Applying the Theorem 1c then \( A \vdash \{ X : \tau_i \} \vdash e[X/t] : \tau_i \). \( X \) will not appear in \( e[X/t] \), so again by Theorem 1b we can eliminate the assumption, concluding that \( A \vdash e[X/t] : \tau_i \).

**let_p** Here the type derivations will be:

\[
\begin{align*}
A \vdash \{ X : \tau_i \} \vdash X : \tau_i & \quad A \vdash t : \tau_i & \quad A \vdash \{ X : Gen(\tau_i, A) \} \vdash e : \tau \\
\hline
A \vdash \text{let}_p X = t \text{ in } e : \tau
\end{align*}
\]

and we want to prove that \( A \vdash e[X/t] : \tau \). We have a type derivation for \( A \vdash \{ X : Gen(\tau_i, A) \} \vdash e : \tau \), and according to Observation 7 there will be derivations \( (A \vdash \{ X : Gen(\tau_i, A) \}) \vdash A_i' \vdash X : \tau_i \) for every appearance of \( X \) in \( e \). In these cases, \( A_i' \) will only contain assumptions over variables \( X_i \) in let or lambda expressions of \( e \). Suppose that all these variables have been renamed to fresh variables. We can create a type substitution \( \pi \) from the variables \( \overline{X_i} \) of \( \tau_i \) which do not appear in \( \overline{A} \) to fresh type variables \( \overline{\Theta} \). It is clear that \( Gen(\tau_i, A) \) is equivalent to \( Gen(\tau_i, \pi, A) \), so \( A \vdash \{ X : Gen(\tau_i, \pi, A) \} \vdash e : \tau \) is a valid derivation. By Theorem 1a \( A \pi \vdash t : \tau_i \pi \), and since \( \overline{X_i} \) are not in \( A \) then \( A \vdash t : \tau_i \pi \). \( X \) and \( \overline{X_i} \) are fresh so they do not appear in \( t \) and by Theorem 1b we can add assumptions to the derivation \( A \vdash t : \tau_i \pi \), obtaining \( (A \vdash \{ X : Gen(\tau_i, \pi, A) \}) \vdash A_i' \vdash t : \tau_i \pi \). The types \( \tau_i \) will be generic instances of \( Gen(\tau_i, A) \), and also of \( Gen(\tau_i, \pi, A) \). Then for each \( \tau_i \) there will exist a type substitution \( \pi_i' \) from the generalized variables \( \overline{\Theta_i} \) in \( Gen(\tau_i, \pi, A) \) to types that will hold \( \tau_i \pi \pi_i' \equiv \tau_i \). By Theorem 1a we can convert \( (A \vdash \{ X : Gen(\tau_i, \pi, A) \}) \vdash A_i' \vdash t : \tau_i \pi \) into \((A \vdash \{ X : Gen(\tau_i, \pi, A) \}) \vdash A_i' \pi_i \vdash t : \tau_i \pi \pi_i' \), and since \( \overline{\Theta_i} \) are fresh variables then \((A \vdash \{ X : Gen(\tau_i, \pi, A) \}) \vdash A_i' \vdash t : \tau_i \pi \pi_i' \) (note that \( \pi_i' \) does not affect \( Gen(\tau_i, \pi, A) \) because the variables \( \overline{\Theta_i} \) are generalized). This way in every place of the original derivation where we have \((A \vdash \{ X : Gen(\tau_i, A) \}) \vdash A_i' \vdash X : \tau_i \) we could place a derivation \((A \vdash \{ X : Gen(\tau_i, A) \}) \vdash A_i' \vdash t : \tau_i \). The resulting expression of this substitution will be \( e[X/t] \), so \( A \vdash \{ X : Gen(\tau_i, A) \} \vdash e[X/t] : \tau_i \). It is clear that \( X \) does not appear in \( e[X/t] \), so by Theorem 1b we can eliminate the assumption over the \( X \) and obtain a derivation \( A \vdash e[X/t] \vdash \pi \), as we wanted to prove.

- **(Elim)** In this case it does not matter what type of let expression it was (let_m or let_p). The rewriting step will be of the form \( P \vdash \text{let}_p X = e_1 \text{ in } e_2 \rightarrow^l e_2 \).

The type derivation of \( A \vdash \text{let}_p X = e_1 \text{ in } e_2 \vdash \tau \) will have a branch \( A \vdash \{ X : \sigma' \} \vdash e_2 : \tau \) for some \( \sigma \). Since we are using the (Elim) rule, \( X \) does not appear in \( e_2 \) so by Theorem 1b we can derive the same type eliminating that assumption, obtaining \( A \vdash e_2 : \tau \).

- **(Flat_m)** There are two cases, depending on the second let expression. In both cases we assume that \( X \neq Y \).

  - \( P \vdash \text{let}_m X = (\text{let}_m Y = e_1 \text{ in } e_2) \text{ in } e_3 \rightarrow^l \text{let}_m Y = e_1 \text{ in } (\text{let}_m X = e_2 \text{ in } e_3) \).
The type derivation will be:

\[
\begin{align*}
\Delta \vdash \{Y : \tau_y\} + Y : \tau_y \\
\Delta \vdash e_1 : \tau_y \\
\frac{\text{LET}_m}{\Delta \vdash \{Y : \tau_y\} + e_2 : \tau_x} \\
\frac{\text{LET}_m}{\Delta \vdash \text{let}_m \ Y = e_1 \text{ in } e_2 : \tau_x} \\
\frac{\Delta \vdash \{X : \tau_x\} \vdash X : \tau_x \quad \Delta \vdash \{X : \tau_x\} \vdash e_3 : \tau}{\Delta \vdash \text{let}_m \ X = (\text{let}_m \ Y = e_1 \text{ in } e_2) \text{ in } e_3 : \tau}
\end{align*}
\]

Then we can build a type derivation

\[
\begin{align*}
\frac{\Delta \vdash \{Y : \tau_y\} + \{X : \tau_x\} \vdash X : \tau_x}{\Delta \vdash \{Y : \tau_y\} + e_2 : \tau_x} \\
\frac{\Delta \vdash \{Y : \tau_y\} + \{X : \tau_x\} \vdash e_3 : \tau}{\Delta \vdash \text{let}_m \ X = e_2 \text{ in } e_3 : \tau} \\
\frac{\Delta \vdash \{Y : \tau_y\} \vdash Y : \tau_y \quad \Delta \vdash e_1 : \tau_y}{\Delta \vdash \text{let}_m \ Y = e_1 \text{ in } (\text{let}_m \ X = e_2 \text{ in } e_3) : \tau}
\end{align*}
\]

The only two derivations which do not come from the hypotheses are \((\Delta \vdash \{Y : \tau_y\}) + \{X : \tau_x\} \vdash X : \tau_x\) and \((\Delta \vdash \{Y : \tau_y\}) + \{X : \tau_x\} \vdash e_3 : \tau\). The first is the application of the \([\text{ID}]\) rule. From the hypotheses we have a derivation \(\Delta \vdash \{X : \tau_x\} \vdash e_3 : \tau\). Since we are rewriting using the \((\text{Flat})\) rule, we are sure that \(Y\) is not in \(e_3\) and by Theorem \([1]\)b we can add the assumption over the \(Y\), obtaining the derivation \((\Delta \vdash \{X : \tau_x\}) + \{Y : \tau_y\} \vdash e_3 : \tau\). \(X\) is different from \(Y\), so according to Observation \([2]\), \((\Delta \vdash \{X : \tau_x\}) + \{Y : \tau_y\}\) is the same as \((\Delta \vdash \{Y : \tau_y\}) + \{X : \tau_x\}\). Therefore \((\Delta \vdash \{Y : \tau_y\}) + \{X : \tau_x\} \vdash e_3 : \tau\) is a valid derivation.

- \(\mathcal{P} \vdash \text{let}_m \ X = (\text{let}_p \ Y = e_1 \text{ in } e_2) \text{ in } e_3 \rightarrow^l \text{let}_p \ Y = e_1 \text{ in } (\text{let}_m \ X = e_2 \text{ in } e_3)\). Similar to the previous case.

- \((\text{Flat}_p)\) We will treat the two different cases:

  - \(\mathcal{P} \vdash \text{let}_p \ X = (\text{let}_p \ Y = e_1 \text{ in } e_2) \text{ in } e_3 \rightarrow^l \text{let}_p \ Y = e_1 \text{ in } (\text{let}_p \ X = e_2 \text{ in } e_3)\).

  The type derivation of the original expression is (being \(A_Y \equiv \Delta \vdash \{Y : \text{Gen}(\tau_y, A)\}\))

\[
\begin{align*}
\frac{\Delta \vdash \{Y : \tau_y\} \vdash Y : \tau_y}{\Delta \vdash e_1 : \tau_y} \\
\frac{\Delta \vdash e_2 : \tau_x}{\Delta \vdash \text{let}_p \ Y = e_1 \text{ in } e_2 : \tau_x} \\
\frac{\Delta \vdash \{X : \tau_x\} \vdash X : \tau_x \quad \Delta \vdash \{X : \text{Gen}(\tau_x, A)\} \vdash e_3 : \tau}{\Delta \vdash \text{let}_p \ X = (\text{let}_p \ Y = e_1 \text{ in } e_2) \text{ in } e_3 : \tau}
\end{align*}
\]
With this derivations as hypothesis we can build a type derivation of the new expression

\[
\begin{align*}
\text{LET}_p \quad & A \vdash \{X : \tau_x\} \vdash X : \tau_x \\
\text{LET}_p \quad & A \vdash e_2 : \tau_x \\
& A \vdash \{X : \text{Gen}(\tau_x, A\_Y)\} \vdash \{Y : \tau_y\} \vdash Y : \tau_y \\
& A \vdash e_1 : \tau_y \\
& A \vdash \{Y : \tau_y\} \vdash Y : \tau_y \\
& A \vdash \{X : \text{Gen}(\tau_x, A\_Y)\} \vdash e_3 : \tau \\
& A \vdash \{Y : \tau_y\} \vdash Y : \tau_y \\
& A \vdash e_1 : \tau_y \\
& A \vdash \{Y : \tau_y\} \vdash Y : \tau_y \\
& A \vdash e_1 : \tau_y \\
& A \vdash \{Y : \tau_y\} \vdash Y : \tau_y \\
& A \vdash \text{let}_p X = e_1 \text{ in } \{Y : \tau_y\} \vdash e_2 \text{ in } e_3 : \tau
\end{align*}
\]

\[A \vdash \{Y : \tau_y\} \vdash Y : \tau_y, A \vdash e_1 : \tau_y\]
and \(A \vdash e_2 : \tau_x\) are the same derivations that appear in the original type derivation; and \(A \vdash \{X : \tau_x\} \vdash X : \tau_x\) holds trivially applying the [[ID] rule. But the derivation \(A \vdash \{Y : \text{Gen}(\tau_y, A\_Y)\} \vdash e_3 : \tau\) has to be proven. As before, since \(Y \notin \text{FV}(e_3)\) by Theorem [1b] we can add an assumption over the \(Y\) and the derivation

\[A \vdash \{Y : \text{Gen}(\tau_x, A\_Y)\} \vdash e_3 : \tau\]

will remain valid. Because \(X \neq Y\) then by Observation [3] \((A \vdash \{X : \text{Gen}(\tau_x, A)\}) \vdash \{Y : \text{Gen}(\tau_y, A)\}\) is the same as \((A \vdash \{Y : \text{Gen}(\tau_y, A)\}) \vdash \{X : \text{Gen}(\tau_x, A)\}\), and the derivation \((A \vdash \{Y : \text{Gen}(\tau_y, A)\}) \vdash \{X : \text{Gen}(\tau_x, A)\} \vdash e_3 : \tau\) will be correct. Clearly \(\text{Gen}(\tau_x, A\_Y)\) is not equal to \(\text{Gen}(\tau_x, A)\) because a previous assumption for \(Y\) can be shadowed so that some free type variables in \(A\) are not in \(A\_Y\). In the generalization step this means that some variables can be generalized in \(\text{Gen}(\tau_x, A\_Y)\) but not in \(\text{Gen}(\tau_x, A)\). The other case never happens because adding \(\{Y : \text{Gen}(\tau_y, A)\}\) to \(A\) never adds free type variables: if some type variable in \(\tau_y\) is not in \(\text{FTV}(A)\) then it will be generalized and will not be in \(\text{FTV}(A\_Y)\) either. Therefore \(\text{Gen}(\tau_x, A\_Y) \vdash \text{Gen}(\tau_x, A)\), and by Theorem [1d] the derivation

\[A \vdash \{Y : \text{Gen}(\tau_y, A)\} \vdash \{X : \text{Gen}(\tau_x, A)\} \vdash e_3 : \tau\]

is valid.

- \(\mathcal{P} \vdash \text{let}_p X = (\text{let}_m Y = e_1 \text{ in } e_2) \text{ in } e_3 \rightarrow \text{let}_p Y = e_1 \text{ in } (\text{let}_p X = e_2 \text{ in } e_3)\).

The type derivation of the original expression is:

\[
\begin{align*}
\text{LET}_m \quad & A \vdash \{Y : \tau_y\} \vdash Y : \tau_y \\
& A \vdash e_1 : \tau_y \\
& A \vdash \{Y : \tau_y\} \vdash e_2 : \tau_x \\
& A \vdash \{X : \tau_x\} \vdash X : \tau_x \\
& A \vdash \{X : \text{Gen}(\tau_x, A)\} \vdash e_3 : \tau \\
& A \vdash \{Y : \tau_y\} \vdash Y : \tau_y \\
& A \vdash e_1 : \tau_y \\
& A \vdash \{Y : \tau_y\} \vdash Y : \tau_y \\
& A \vdash e_1 : \tau_y \\
& A \vdash \{Y : \tau_y\} \vdash Y : \tau_y \\
& A \vdash \text{let}_m Y = e_1 \text{ in } e_2 : \tau_x \\
& A \vdash \text{let}_m Y = e_1 \text{ in } e_2 : \tau_x \\
& A \vdash \text{let}_p X = (\text{let}_m Y = e_1 \text{ in } e_2) \text{ in } e_3 : \tau
\end{align*}
\]

and we want to build one of the form (being \(A\_Y \equiv A \vdash \{Y : \text{Gen}(\tau_y, A)\}\)):

\[
\begin{align*}
& A \vdash \{X : \tau_x\} \vdash X : \tau_x \\
& A \vdash e_2 : \tau_x \\
& A \vdash \{X : \text{Gen}(\tau_x, A\_Y)\} \vdash e_3 : \tau \\
& A \vdash \text{let}_p X = e_2 \text{ in } e_3 : \tau \\
& A \vdash \{Y : \tau_y\} \vdash Y : \tau_y \\
& A \vdash e_1 : \tau_y \\
& A \vdash \{Y : \tau_y\} \vdash Y : \tau_y \\
& A \vdash e_1 : \tau_y \\
& A \vdash \{Y : \tau_y\} \vdash Y : \tau_y \\
& A \vdash \text{let}_p Y = e_1 \text{ in } \{Y : \tau_y\} \vdash e_2 \text{ in } e_3 : \tau
\end{align*}
\]

39
The derivations $A \oplus \{ Y : \tau_y \} \vdash Y : \tau_y$ and $A \vdash e_1 : \tau_y$ come from the original derivation; and $A_{Y} \oplus \{ X : \tau_x \} \vdash X : \tau_x$ is the trivial application of the [ID] rule. From the original derivation we have $A \oplus \{ Y : \tau_y \} \vdash e_2 : \tau_x$. It is easy to see that $Gen(\tau_y, A) \vdash \tau_y$, so by Theorem 1d $A_{Y} \vdash e_2 : \tau_x$. We also have from the original derivation that $A \oplus \{ X : Gen(\tau_x, A) \} \vdash e_3 : \tau$. We know that $Y \not\in FV(e_3)$, so by Theorem 1b we can add an assumption over that variable and the derivation $(A \oplus \{ X : Gen(\tau_x, A) \}) \oplus \{ Y : Gen(\tau_y, A) \} \vdash e_3 : \tau$ will be valid. $X$ is different from $Y$, so according to Observation 3 the set of assumptions $(A \oplus \{ X : Gen(\tau_x, A) \}) \oplus \{ Y : Gen(\tau_y, A) \}$ is the same as $(A \oplus \{ Y : Gen(\tau_y, A) \}) \oplus \{ X : Gen(\tau_x, A) \}$. By the same reasons given in the previous case $(Gen(\tau_x, A_{Y}) \vdash Gen(\tau_x, A)$, so by Theorem 1d the derivation $A_{Y} \oplus \{ X : Gen(\tau_x, A_{Y}) \} \vdash e_3 : \tau$ will be valid.

- (LetAp) We will distinguish between the different let expressions.

$let_{m}$ The rewriting step is $P \vdash (let_{m} X = e_1 in e_2)e_3 \rightarrow let_{m} X = e_1 in e_2e_3$.

The type derivation of $(let_{m} X = e_1 in e_2)e_3$ is:

$$
\begin{array}{l}
A \vdash X : \tau_1 \\
A \vdash e_1 : \tau_1 \\
\hline
\text{LET}_{m}
\end{array}
\Rightarrow
\begin{array}{l}
A \vdash \{ X : \tau_1 \} \vdash e_2 : \tau_1 \rightarrow \tau \\
\hline
\text{APP}
\end{array}
\Rightarrow
\begin{array}{l}
A \vdash let\_{m} X = e_1 in e_2 : \tau_1 \rightarrow \tau \\
A \vdash e_3 : \tau_1 \\
\hline
\end{array}
\Rightarrow
\begin{array}{l}
A \vdash (let\_{m} X = e_1 in e_2)e_3 : \tau
\end{array}
$$

We want to construct a type derivation of the form:

$$
\begin{array}{l}
A \vdash X : \tau_1 \vdash e_2 : \tau_1 \rightarrow \tau \\
\hline
\text{APP}
\end{array}
\Rightarrow
\begin{array}{l}
A \vdash \{ X : \tau_1 \} \vdash e_2e_3 : \tau \\
\hline
\text{LET}_{m}
\end{array}
\Rightarrow
\begin{array}{l}
A \vdash \{ X : \tau_1 \} \vdash X : \tau_1 \\
A \vdash e_1 : \tau_1 \\
\hline
\end{array}
\Rightarrow
\begin{array}{l}
A \vdash let\_{m} X = e_1 in e_2e_3 : \tau
\end{array}
$$

All the derivations appear in the original derivation, except $A \oplus \{ X : \tau_1 \} \vdash e_3 : \tau_1$. Because we are using (LetAp), we are sure that $X$ does not appear in $FV(e_3)$. From the original derivation we have that $A \vdash e_3 : \tau_1$, and by Theorem 1b we can add an assumption over the variable $X$ and obtain the derivation $A \oplus \{ X : \tau_1 \} \vdash e_3 : \tau_1$.

$let_{p}$ Similar to the $let_{m}$ case.

- (Contx) We have a derivation $A \vdash C[e] : \tau$, so according to the Observation in that derivation will appear a derivation a) $A \oplus A' \vdash e : \tau'$, being $A'$ a set of assumptions over variables. If we apply the rule (Contx) to reduce an expression $C[e]$ is because we reduce the expression $e$ using any of the other rules of the let-rewriting relation b) $P \vdash e \rightarrow l \ e'$. We also know by Observation $A \vdash C[e'] : \tau$. With a), b) and c) the Induction Hypothesis states that $A \oplus A' \vdash e' : \tau'$, and by Lemma 5 then $A \vdash C[e'] : \tau$. □

40
Theorem 4 (Soundness of \( \vdash \) wrt \( \triangleright \))

1) \( A \vdash e : \tau | \pi \implies A \triangleright e : \tau \)

Proof.
We proceed by induction over the size of the type inference \( A \vdash e : \tau | \pi \).

Base Case

- \([\text{id}]\) We have a type inference of the form:
  \[
  \vdash A \triangleright g : \tau | \text{id}
  \]
  where \( A(g) = \sigma \) and \( \tau \) is a variant of \( \sigma \). It is clear that if \( \tau \) is a variant of \( \sigma \) it is also a generic instance of \( \sigma \), and \( A \text{id} \equiv A \) so the following type derivation is valid:
  \[
  \vdash A \triangleright g : \tau
  \]

Induction Step

- \([\text{app}]\) The type inference is:
  \[
  \vdash e_1 : \tau_1 | \pi_1, A \triangleright e_2 : \tau_2 | \pi_2 \]
  \[
  \vdash e_1 e_2 : \alpha | \pi_1 \pi_2
  \]
  where \( \pi = \text{mgu}(\tau_1 \pi_2, \tau_2 \rightarrow \alpha) \), being \( \alpha \) a fresh type variable. By the Induction Hypothesis we have that \( A \pi_1 \triangleright e_1 : \tau_1 \) and \( A \pi_2 \triangleright e_2 : \tau_2 \). We can apply Theorem 1-a to both derivations and obtain \( A \pi_1 \pi_2 \triangleright e_1 : \tau_1 \pi_2 \) and \( A \pi_1 \pi_2 \triangleright e_2 : \tau_2 \pi \). Since we know that \( \tau_1 \pi_2 \pi = (\tau_2 \rightarrow \alpha) \pi = \tau_2 \pi \rightarrow \alpha \pi \) then we can construct the type derivation:
  \[
  \vdash A \pi_1 \pi_2 \triangleright e_1 : \tau_1 \pi_2 \rightarrow \alpha \pi, A \pi_1 \pi_2 \triangleright e_2 : \tau_2 \pi
  \]

- \([\text{let}]\) The type inference will be of the form:
  \[
  \vdash A \triangleright \lambda t.e : \tau | \pi \]
  where \( \pi \) are fresh type variables. By the Induction Hypothesis we have that \( A t \triangleright X_i : \alpha_i \triangleright t \) and \( A t \pi \triangleright X_i : \alpha_i \triangleright \pi \). We can apply Theorem 1-a to the first derivation and obtain \( A t \pi \triangleright \lambda t.e : \tau | \pi \). Therefore the following type derivation is correct:
  \[
  \vdash A t \pi \triangleright \lambda t.e : \tau_1 \pi \rightarrow \tau | \pi
  \]

- \([\text{let}_m]\) In this case the type inference will be:
\[ A \cup \{ X_i : \alpha_i \} \vdash t : \tau_i | A \]
\[ \pi \vdash e : \tau_1 | \pi \]

\[ \text{ILET}_m \] \[ (A \cup \{ X_i : \alpha_i \} \cup \pi \pi \pi \vdash e_2 : \tau_2 | \pi \]

\[ A \vdash let_m t = e_1 in e_2 : \tau_2 | \pi \pi \pi \]

where \( \pi \) are fresh type variables and \( \pi = mgu(\tau_1, \tau_1) \). By the Induction Hypothesis we have that \( \pi \vdash e : \tau_1 \) and \( A \pi_1 \pi \pi_2 \vdash e_2 : \tau_2 \). We can apply Theorem 1-a to the first two derivations and obtain \( A \pi_1 \pi \pi \pi_2 \vdash t : \tau_1 \pi_1 \pi \pi_2 \) and as \( \tau_1 \pi_1 \pi = \tau_1 \pi \) then we can build a type derivation of the form:

\[ A \pi_1 \pi \pi_2 \vdash t : \tau_1 \pi_2 \]
\[ A \pi_1 \pi_2 \vdash e : \tau_1 \pi_2 \]

\[ \text{LET}_m \]

\[ A \vdash let_m t = e_1 in e_2 : \tau_2 | \pi \pi \pi \]

By the Induction Hypothesis we have the type derivations \( A \pi_1 \vdash e_1 : \tau_1 \) and \( A \pi_1 \pi_2 \vdash \{ X : Gen(\tau_1, A \pi_1) \} \vdash e_2 : \tau_2 \). We can construct a type substitution \( \pi \in TSubst \) such that maps the type variables in \( FTV(\pi) \cup FTV(A \pi_1) \) to fresh variables. Then it is clear that \( Gen(\pi, A \pi_1) = Gen(\tau_1, A \pi_1) \). On the other hand, all the variables in \( \tau_1 \pi \) which are not in \( FTV(A \pi_1) \) are fresh so they do not appear in \( \pi_2 \), and by Lemma 7 \( Gen(\tau_1, A \pi_1) \pi_2 = Gen(\tau_1 \pi \pi_2, A \pi_1 \pi_2) \). Therefore the type derivation

\[ A \pi_1 \pi_2 \vdash \{ X : Gen(\tau_1 \pi \pi_2, A \pi_1 \pi_2) \} \vdash e_2 : \tau_2 \]

is correct. By Theorem 1-a we obtain \( A \pi_1 \pi \pi_2 \vdash e_1 : \tau_1 \pi \pi_2 \), and as \( Dom(\pi) \cap FTV(A \pi_1) = \emptyset \) then \( A \pi_1 \pi_2 \vdash e_1 : \tau_1 \pi \pi_2 \).

Finally with these derivations we can build the type derivation we intended:

\[ \text{LET}_{pm} \]

\[ A \pi_1 \pi_2 \vdash e_1 : \tau_1 \pi \pi_2 \]
\[ A \pi_1 \pi_2 \vdash \{ X : Gen(\tau_1 \pi \pi_2, A \pi_1 \pi_2) \} \vdash e_2 : \tau_2 \]

\[ A \vdash let_{pm} t = e_1 in e_2 : \tau_2 | \pi \pi \pi \]

- \[ \text{ILET}^X_{pm} \] This case is similar to the \[ \text{LET}_m \] case.
- \[ \text{ILET}^X_{pm} \] In this case we have an inference of the form:

\[ A \vdash \{ X_i : \alpha_i \} \vdash t : \tau_i | A \]
\[ \pi \vdash e_1 : \tau_1 | \pi \]

\[ \text{ILET}_p \]

\[ A \pi \pi_1 \pi \vdash \{ X_i : Gen(\alpha_i, \pi_1 \pi_1, A \pi_1 \pi_1) \} \vdash e_2 : \tau_2 | \pi \pi \pi \]

\[ A \vdash let_p t = e_1 in e_2 : \tau_2 | \pi \pi \pi \]

where \( \pi = mgu(\tau_1 \pi_1, \tau_1) \). By the Induction Hypothesis we have \( A \pi \pi_1 \pi \pi_2 \vdash \{ X_i : Gen(\alpha_i, \pi_1 \pi_1 \pi_2) \} \vdash e_2 \) and \( A \pi \pi_1 \vdash \{ X_i : \alpha_i \} \vdash t : \tau_i \), \( A \pi \pi_1 \vdash e_1 : \tau_1 \pi \). Let be \( \beta_i \) the type variables in all the types \( \alpha_i \pi_1 \pi_1 \) which do
not appear in $A_{\pi_1 \pi_2}$. We can create a type substitution $\pi'$ from $\beta_i$ to fresh variables. It is clear that $Gen(\alpha_i, \pi_1 \pi_2, A_{\alpha_i \pi_1 \pi_2}) = Gen(\alpha_i, \pi_1 \pi_2, A_{\alpha_i \pi_1 \pi_2})$, as $\pi'$ only substitutes the variables that will be generalized by fresh ones which will also be generalized, so it is a renaming of the bounded variables (Observation 1). Therefore the derivation

$$A_{\pi_1 \pi_2} \oplus \{X_i : Gen(\alpha_i, \pi_1 \pi_2, A_{\pi_1 \pi_2})\} \vdash e_2 : \tau_2$$

is also valid. Applying the Theorem to the first two derivations we obtain $A_{\pi_1 \pi_2} \oplus \{X_i : \alpha_i, \pi_1 \pi_2 \} \vdash e_1 : \tau_1 \pi_2$ and $A_{\pi_1 \pi_2} \vdash e_1 : \tau_1 \pi_2$. By construction, no variable in $Dom(\pi')$ or $Rng(\pi')$ is in $FTV(A_{\pi_1 \pi_2})$, so $A_{\pi_1 \pi_2} \vdash e_2 : \tau_2$. By Lemma 7 we know that $Gen(\alpha_i, \pi_1 \pi_2, A_{\pi_1 \pi_2}) = Gen(\alpha_i, \pi_1 \pi_2, A_{\pi_1 \pi_2})$, so the derivation $A_{\pi_1 \pi_2} \vdash \{X_i : Gen(\alpha_i, \pi_1 \pi_2, A_{\pi_1 \pi_2})\} \vdash e_2 : \tau_2$ is correct. With this derivations as premises we can build the expected one:

$A_{\pi_1 \pi_2} \oplus \{X_i : \alpha_i, \pi_1 \pi_2 \} \vdash e_1 : \tau_1 \pi_2$

$A_{\pi_1 \pi_2} \vdash e_1 : \tau_1 \pi_2$

$\vdash e_2 : \tau_2$

(remembering that $\tau_1 \pi_2 = \tau_1 \pi$ because of $\pi$ is a mgu).

\[\square\]

2) $A \models^\bullet e : \tau | \pi \Longrightarrow A \vdash^\bullet e : \tau$

By definition of $\models^\bullet$ we have that $A \models^\bullet e : \tau$ and $\text{critVar}_{A_{\pi}}(e)$. Applying the soundness of $\models$ (Theorem 4) we have that $A_{\pi} \vdash e : \tau$. Since $A_{\pi} \vdash e : \tau$ and $\text{critVar}_{A_{\pi}}(e)$, then by definition of $\vdash^\bullet$ we have $A_{\pi} \vdash^\bullet e : \tau$.

\[\square\]

Theorem 5 (Completeness of $\models$ wrt $\vdash$).

$A_{\pi} \vdash e : \tau \Longrightarrow \exists \pi, \pi' \rangle. A \models e : \tau | \pi \land A_{\pi} \pi'' = A_{\pi'} \land \pi'' = \tau'$.

Proof.

This proof is based on the proof of completeness of algorithm $W$ in [12]. We proceed by induction over the size of the type derivation.

Base Case

- [ID] In this case we have a type derivation:

  \[\text{ID} - A_{\pi'} \vdash s : \tau'\]

  if $A_{\pi'}(s) = \sigma$ and $\sigma \succ \tau'$. Let’s suppose that $A(s) = \forall \alpha_i. \tau''$ (with $\alpha'$ fresh variables), then $\sigma = (\forall \alpha_i. \tau'') \pi' = \forall \alpha_i. (\tau'' \pi')$. Since $\sigma \succ \tau'$ then there exists a type substitution $[\alpha_i / \tau_i]$ such that $\tau' = (\tau'' \pi')[\alpha_i / \tau_i]$. Let $\beta_i$ be fresh variables. As $\tau''[\alpha_i / \beta_i]$ is a variant of $\forall \alpha_i. \tau''$ then the following type inference is correct:

\[\ldots\]
Induction Step

- [APP] The type derivation will be:

\[
\begin{align*}
\mathcal{A}\vdash \pi' &:\tau_1' \rightarrow \tau' \\
\mathcal{A}\vdash \pi'' &:\tau_2'' \rightarrow \tau'' \\
\mathcal{A}\vdash \pi' &:\tau_1' \rightarrow \tau' \\
\mathcal{A}\vdash \pi'' &:\tau_2'' \rightarrow \tau'' \\
\mathcal{A}\vdash \pi &:\tau_1\pi\pi'' \rightarrow \tau'' \\
\mathcal{A}\vdash \pi &:\tau_1\pi\pi'' \rightarrow \tau'' \\
\mathcal{A}\vdash \pi &:\tau_1\pi\pi'' \rightarrow \tau'' \\
\mathcal{A}\vdash \pi &:\tau_1\pi\pi'' \rightarrow \tau'' \\
\end{align*}
\]

By the Induction Hypothesis we know that \( \mathcal{A} \vdash e_1 : \tau_1 | \pi_1 \) and there is a type substitution \( \pi'' \) such that \( \pi''_1 = \tau_1' \rightarrow \tau' \) and \( \mathcal{A}\vdash \pi'' = \mathcal{A}\pi''_1 \). Since \( \mathcal{A}\vdash \pi'' = \mathcal{A}\pi''_1 \) then the derivation \( (\mathcal{A}\vdash \pi''_1) \vdash e_2 : \tau_2' \) is correct, and again by the Induction Hypothesis we know that \( \mathcal{A}\vdash e_2 : \tau_2 | \pi_2 \) and that there exists a type substitution \( \pi''_2 \) such that \( \tau_2 \pi''_2 = \tau_1' \) and \( \mathcal{A}\vdash \pi''_2 = \mathcal{A}\pi''_2 \). We can assume that \( \pi''_2 \) is minimal, so \( \text{Dom}(\pi''_2) \subseteq \text{FTV}(\tau_2) \cup \text{FTV}(\mathcal{A}\pi''_2) \).

In order to prove that the existence of a type inference \( \mathcal{A} \vdash e_1 : \alpha | \pi | \pi_2 \) we need to prove that there exists a most general unifier for \( \tau_1 | \pi_1 | \tau_2 \) (being \( \alpha \) a fresh variable). For that, we will construct a type substitution \( \pi_u \) which will unify these two types. We know that \( \mathcal{A}\vdash \pi_1'' = \mathcal{A}\pi_1''_1 \) and \( \pi_u \equiv \pi''_2 + \pi''_1 | \beta + [\alpha/\tau'] \). \( \pi_u \) is well defined because the domains of the three substitutions are disjoints. According to Observation 6, the variables in \( \text{FTV}(\tau_2) \), \( \text{Dom}(\pi_u) \) or \( \text{Rng}(\pi_u) \) which are not in \( \text{FTV}(\mathcal{A}\pi_1''_1) \) are fresh variables and cannot occur in \( B \). Since the variables in \( B \) are neither in \( \text{FTV}(\mathcal{A}\pi_1) \) nor in \( \text{Rng}(\pi_u) \) then they do not appear in \( \text{FTV}(\mathcal{A}\pi_1''_1) \) either; and as \( \pi''_2 \) is minimal then no variable in \( B \) could occur in \( \text{Dom}(\pi''_2) \). Besides \( \alpha \) is fresh, and it can occur neither in \( \pi''_2 \) nor in \( \pi_1'' | \beta \). Applying \( \pi_u \) to \( \tau_2 \rightarrow \alpha \) we obtain \( (\tau_2 \rightarrow \alpha) \pi_u = \tau_2 \pi_u = \alpha \pi_u = \tau_2 \pi''_2 \rightarrow \alpha | \beta | \pi''_1' = \tau_1' \rightarrow \tau' \). On the other hand, \( \tau_1 | \pi_2 \pi_u = \tau_1' \rightarrow \tau' \) because if a type variable of \( \tau_1 \) is in \( \mathcal{A}\pi_1 \) then \( \tau_1 \pi_2 \pi_u = \tau_1 \pi_2 \pi''_2 = \tau_1 \pi''_1' = \tau_1' \rightarrow \tau' \), and if not it will be in \( B \) and \( \pi_u \) will not affect it, so \( \tau_1 \pi_2 \pi_u = \tau_1 \pi_u = \tau_1 \pi''_1' | \beta = \tau_1' \rightarrow \tau' \). Since \( \pi_u \) is an unifier, then there will exists a most general unifier \( \pi \) of \( \tau_1 \pi_1 \pi_2 \tau_2 \) and \( \tau_2 \rightarrow \alpha \). Therefore the following type inference is correct:

\[
\begin{align*}
\mathcal{A}\vdash e_1 : \tau_1 | \pi_1 \\
\mathcal{A}\vdash e_2 : \tau_2 | \pi_2 \\
\mathcal{A}\vdash e_1 e_2 : \alpha | \pi_1 \pi_2 \pi \\
\end{align*}
\]
We assume that the variables $X_i$ in the pattern $t$ do not appear in $A\pi'$ (nor in $A$). In this case the type derivation is:

\[
\begin{align*}
\frac{A\pi' \oplus \{X_i : \tau_i\} \vdash t : \tau'_i \quad A\pi' \oplus \{X_i : \tau_i\} \vdash e : \tau'}{A\pi' \vdash \text{let } e : \tau'_i \rightarrow \tau'}
\end{align*}
\]

Let $\pi_i$ be fresh type variables and $\pi_g \equiv [\alpha_i/\pi_i]$. Then the first derivation is equal to $(A \oplus \{X_i : \alpha_i\})\pi'\pi_g \vdash t : \tau'_i$. By the Induction Hypothesis we know that $(A \oplus \{X_i : \alpha_i\})\pi'\pi_g \vdash \pi_e$ and that exists a type substitution $\pi''$ such that $(A \oplus \{X_i : \alpha_i\})\pi'\pi_g = (A \oplus \{X_i : \alpha_i\})\pi_1\pi''$ and $\tau_e\pi'' = \tau'$. Because the data variables $X_i$ do not appear in $A$, then it is true that $A\pi'\pi_g = A\pi'$, and for every type variable $\alpha_i\pi'\pi_g = \alpha_i\pi_1\pi''$.

Using these equalities we can write $A\pi' \oplus \{X_i : \tau_i\}$ as $A\pi_1\pi'' \oplus \{X_i : \alpha_i\pi_1\pi''\}$, that is the same as $(A \oplus \{X_i : \alpha_i\})\pi_1\pi''$. Then, the second derivation is equal to $(A \oplus \{X_i : \alpha_i\})\pi_1\pi'' \vdash \pi_e : \tau'_i$, and by the Induction Hypothesis $(A \oplus \{X_i : \alpha_i\})\pi_1\pi'' \vdash e : \tau_e\pi_1\pi''$ and there exists a type substitution $\pi''$ such that $(A \oplus \{X_i : \alpha_i\})\pi_1\pi'' = (A \oplus \{X_i : \alpha_i\})\pi_1\pi_1\pi''$ and $\tau_e\pi_1\pi'' = \tau'$. As before, it is also true that $A\pi_1\pi'' = A\pi_1\pi_1\pi''$ and for every type variable $\alpha_i\pi_1\pi'' = \alpha_i\pi_1\pi_1\pi''$. We can assume that $\pi''$ is minimal, so $Dom(\pi'') \subseteq FTV(\tau_e) \cup FTV((A \cup \{X_i : \alpha_i\})\pi_1\pi_1\pi'')$. Therefore the type inference for the lambda expression exists and have the form

\[
\begin{align*}
\frac{(A \oplus \{X_i : \alpha_i\})\pi_1\pi'' \vdash \pi_e \quad (A \oplus \{X_i : \alpha_i\})\pi_1\pi'' \vdash e : \tau_e\pi_1\pi'' \quad \gamma \vdash \lambda \text{ e } \tau_e\pi_1\pi'' \rightarrow \tau_e\pi_1\pi''}{\gamma \vdash \lambda \text{ e } t : \tau_e\pi_1\pi''}
\end{align*}
\]

We do not prove that there exists a type substitution $\pi''$ such that $A\pi' = A\pi_1\pi''$ and $(\tau_1, \pi\pi_e \rightarrow \tau_e)\pi'' = \tau'_i \rightarrow \tau'$. Let be $B \equiv Dom(\pi'') \cap FTV((A \oplus \{X_i : \alpha_i\})\pi_1\pi_1\pi'')$ and $\pi'' = \pi''_B + \pi''_{\pi_e}$, which is well defined because the domains are disjoints. According to Observation $\Box$ the variables which are not in $FTV((A \oplus \{X_i : \alpha_i\})\pi_1\pi_1\pi'')$ and appear in $FTV(\tau_e)$, $Dom(\pi_e)$ or in $Rng(\pi_e)$ are fresh, so they cannot be in $B$. As these variables do not appear in $Rng(\pi_e)$ then they do not appear in $FTV((A \oplus \{X_i : \alpha_i\})\pi_1\pi_1\pi'')$; so the variables in $B$ are not in $Dom(\pi_e)$ and the domains of $\pi''_B$ and $\pi''_{\pi_e}$ are disjoints.

It is clear that $A\pi' = A\pi_1\pi'' = A\pi_1\pi_e\pi'' = A\pi_1\pi_e\pi''$ because $\pi''_B$ is part of $\pi''$. To prove that $(\tau_1, \pi\pi_e \rightarrow \tau_e)\pi'' = \tau'_i \rightarrow \tau'$ we need to prove that $\tau_e\pi_e\pi'' = \tau'_i$ and $\tau_e\pi_e\pi'' = \tau'$. The second part is straightforward because $\tau' = \tau_e\pi_e\pi'' = \tau_e\pi''$. To prove the first one we will distinguish over the type variables in $\tau_e$. For all the type variables of $\tau_e$ which are in $(A \oplus \{X_i : \alpha_i\})\pi_1\pi_1\pi''$ (i.e. they are not in $B$) we know that $\tau_1, \pi\pi_e \rightarrow \tau_e)\pi'' = \tau'_i$ because $(A \oplus \{X_i : \alpha_i\})\pi_1\pi'' = (A \oplus \{X_i : \alpha_i\})\pi_1\pi_e\pi''$. For the variables in $\tau_e$ which are in $B$ the case is simpler because we know they do not appear in $Dom(\pi_e)$, therefore so $\tau_1, \pi\pi_e \rightarrow \tau_e)\pi'' = \tau'_i$.

We assume that the variables $X_i$ of the pattern $t$ are fresh and do not occur in $A\pi'$ (nor in $A$). Then the type derivation will be:
Let \( \alpha_i \) be fresh type variables, and \( \pi_g \equiv (\alpha_i/\tau_i) \). Since \( \alpha_i \) are fresh it is clear that \( A\tau' \vdash x \in \tau' \) and \( \alpha_i\pi_g \tau_g = \alpha_i \tau_g = \tau_i \) for every type variable \( \alpha_i \). Then we can write the first derivation as \( (A \vdash (\{X_i : \alpha_i\})\pi' \tau_g \vdash t : \tau'_t) \) and by the Induction Hypothesis \( A \vdash (\{X_i : \alpha_i\}) \pi \tau \) and there is a type substitution \( \tau''_i \) such that \( (A \vdash (\{X_i : \alpha_i\})\pi' \tau_g = (A \vdash (\{X_i : \alpha_i\}) \pi \tau''_i \) and \( \tau_i \tau''_i = \tau'_t \). Since the data variables \( X_i \) do not appear in \( A\tau' \) then \( A\tau' = A\pi' \tau_g = A\pi \tau''_i \) and for every type variable \( \alpha_i\pi' \tau_g = \alpha_i \tau_g = \tau_i = \alpha_i \tau''_i \). Since \( A\tau' = A\pi \tau''_i \) then we can write the second derivation as \( A\pi' \vdash e : \tau'd \) and by the Induction Hypothesis \( A\pi \vdash e : \tau \) and there exists a type substitution \( \tau''_i \) such that \( A\pi \tau''_i = A\pi \tau''_i \) and \( \tau_i \tau''_i = \tau'_i \). We can assume that \( \tau''_i \) is minimal, so \( Dom(\tau''_i) \subseteq FTV(\tau_i) \). Now we have to prove that \( \tau_i \pi_i \) is defined for every type variable \( \alpha_i \) and \( \pi_g \). For the type variables \( \alpha_i \) we will be fresh variables, so they will not be any of the variables in \( B \). As the variables in \( B \) occur neither in \( FTV(\alpha_i) \) nor in \( Rug(\pi_i) \) then they do not appear in \( A\pi \pi_i \); and as \( \tau''_i \) is minimal then no variable in \( B \) occurs in \( Dom(\tau''_i) \).

\( \pi_u \) is an unifier of \( \tau_i \pi_i \) and \( \tau_1 \) because \( \tau_i \pi_i \pi_u = \tau_i \pi_u = \tau'_i \). The first case is easy because \( \tau_i \pi_i = \tau_i \tau''_i = \tau'_i \). To prove the second we will distinguish over the type variables of \( \tau_1 \). For the type variables of \( \tau_1 \) in \( A\pi \) (i.e. those which are not in \( B \)) we know that \( \tau_i \pi_i \pi_u = \tau_i \pi_i \tau''_i = \tau_i \tau''_i = \tau'_i \), and for the others (those in \( B \)) we know they are fresh and do not appear in \( \tau_1 \), so \( \tau_i \pi_i \pi_u = \tau_i \pi_u = \tau_i \tau''_i |_B = \tau'_i \). Therefore there will exist a most general unifier \( \pi \), and \( \pi_u = \pi \).

We also know that \( A\pi' = A\pi_i \tau''_i = A\pi_i \pi_i \pi_u = A\pi_i \pi_i \pi_o \) and for every type variable \( \alpha_i \pi_i \pi_o \pi_o = \tau_i \) (for the type variables of \( \alpha_i \)) which are in \( A\pi_i \) then \( \alpha_i \pi_i \pi_i \pi_o = \alpha_i \pi_i \pi_o = \alpha_i \pi_i \pi_i = \alpha_i \pi_i \pi''_i \) and for the rest of the variables -those in \( B \)- then \( \alpha_i \pi_i \pi_i \pi_o = \alpha_i \pi_i \pi_o = \alpha_i \pi_i \pi_u = \alpha_i \pi_i \pi_i |_B = \tau_i \).

Then we can write the third derivation as \( (A \vdash (\{X_i : \alpha_i\})\pi_i \pi_i \pi_o \vdash e_2 : \tau'') \) and by the Induction Hypothesis \( A \vdash (\{X_i : \alpha_i\}) \pi \pi \) and there exists a type substitution \( \tau''_2 \) such that \( \tau \tau''_2 = \tau' \) and \( (A \vdash (\{X_i : \alpha_i\})\pi_i \pi_i \pi_o = (A \vdash (\{X_i : \alpha_i\}) \pi_i \pi_i \pi_i \pi''_2 \). Since the variables \( X_i \) do not appear in \( A \), in particular it is true that \( A\pi_i \pi_i \pi_o = A\pi_i \pi_i \pi_i \pi''_2 \).

With these three type inferences we can build the type inference for the let expression:
Theorem 6 (Maximality of $\triangleright\triangleright$).

\begin{itemize}
  \item [iLET_m] $\mathcal{A} \triangleright\triangleright t : \tau_1 | \pi_{\tau}$
  \item \(\mathcal{A} \triangleright\triangleright e_1 : \tau_1 | \pi_{\tau}\\\)
  \item \(\mathcal{A} \triangleright\triangleright e_2 : \tau_2 | \pi_{\tau_2} \)
  \item \(\mathcal{A} \triangleright\triangleright \text{let}_m t = e_1 \text{ in } e_2 : \tau_2 | \pi_{\tau_1 \pi_{\tau_2}} \)
\end{itemize}

being $\pi = mgu(\tau_1, \tau_1)$. To finish this case we only have to prove that there exists a type substitution $\pi''$ such that $\tau_2 | \pi'' = \tau'$ and $\mathcal{A} \triangleright\triangleright \pi'' = \mathcal{A} \triangleright\triangleright \pi_{\tau_1 \pi_2 \pi''}$. This substitution $\pi''$ is $\pi''_2$.

- [LET_{pm}^X] We assume that $X$ does not occur in $\mathcal{A}$. We have a type derivation:

\begin{itemize}
  \item \(\mathcal{A} \triangleright\triangleright e_1 : \tau_1 | \pi_1\\\)
  \item \(\mathcal{A} \triangleright\triangleright \{ X : \text{Gen}(\tau_1, \pi_1') \} \triangleright\triangleright e_2 : \tau_2 | \pi_2\\\)
  \item \(\mathcal{A} \triangleright\triangleright \text{let}_{pm} \ X = e_1 \text{ in } e_2 : \tau_2 | \pi_{\tau_1 \pi_2} \)
\end{itemize}

By the Induction Hypothesis we have that $\mathcal{A} \triangleright\triangleright e_1 : \tau_1 | \pi_1$ and there exists a type substitution $\pi''_1$ such that $\mathcal{A} \triangleright\triangleright \pi'' = \mathcal{A} \triangleright\triangleright \pi''_1$ and $\tau_1 | \pi''_1 = \tau'_1$. Gen$(\tau'_1, \pi''_1) = \text{Gen}(\tau_1, \pi''_1) \triangleright \text{Gen}(\tau'_1, \pi''_1)'$. Then by Theorem 5 we have that the type derivation $\mathcal{A} \triangleright\triangleright \{ X : \text{Gen}(\tau_1, \pi_1') \} \triangleright\triangleright e_2 : \tau_2 | \pi_2$ is valid. We can write this derivation as $\mathcal{A} \triangleright\triangleright \{ X : \text{Gen}(\tau_1, \pi_1) \} \triangleright\triangleright e_2 : \tau_2 | \pi_2$ and applying the Induction Hypothesis we obtain that $\mathcal{A} \triangleright\triangleright \{ X : \text{Gen}(\tau_1, \pi_1) \} \triangleright\triangleright \tau_2 | \pi_2$. Since $X$ does not appear in $\mathcal{A}$ the last equality means that $\mathcal{A} \triangleright\triangleright \pi''_2 = \mathcal{A} \triangleright\triangleright \pi''_1$ and $\mathcal{A} \triangleright\triangleright \mathcal{A} \triangleright\triangleright \pi''_2 = \mathcal{A} \triangleright\triangleright \mathcal{A} \triangleright\triangleright \pi''_1$. With the previous type inferences we can construct a type inference for the whole expression:

\begin{itemize}
  \item [iLET_{pm}^X] $\mathcal{A} \triangleright\triangleright e_1 : \tau_1 | \pi_1\\\)
  \item \(\mathcal{A} \triangleright\triangleright \{ X : \text{Gen}(\tau_1, \pi_1) \} \triangleright\triangleright e_2 : \tau_2 | \pi_2\\\)
  \item \(\mathcal{A} \triangleright\triangleright \text{let}_{pm} \ X = e_1 \text{ in } e_2 : \tau_2 | \pi_{\tau_1 \pi_2} \)
\end{itemize}

In this case it is easy to see that there exists a type substitution $(\pi''_2)$ such that $\tau_2 | \pi''_2 = \tau'_2$ and $\mathcal{A} \triangleright\triangleright \mathcal{A} \triangleright\triangleright \mathcal{A} \triangleright\triangleright \pi''_2 = \mathcal{A} \triangleright\triangleright \mathcal{A} \triangleright\triangleright \mathcal{A} \triangleright\triangleright \pi''_2$.

- [LET_{pm}^6] Equal to the [LET_m] case.

- [LET_t] The proof of this case follows the same ideas as the cases [LET_m] and [LET_{pm}^X].

Theorem 6 (Maximality of $\triangleright\triangleright$).

\begin{itemize}
  \item [a)] $\Pi_{\ast,e} \mid \mathcal{A}$ has a maximum element $\iff \exists \tau_g \in \text{SType}, \pi_g \in \text{TSubst.} \mathcal{A} \triangleright\triangleright e : \tau_g | \pi_g$.
  \item [b)] If $\mathcal{A} \triangleright\triangleright e : \tau' | \pi$ then there exists a type substitution $\pi''$ such that $\mathcal{A} \triangleright\triangleright \pi'' = \mathcal{A} \triangleright\triangleright \pi''$.
\end{itemize}

Proof.

\begin{itemize}
  \item [a)]
    \begin{itemize}
      \item $\iff$ If $\mathcal{A} \triangleright\triangleright e : \tau_g | \pi_g$ then by Lemma 9 $\Pi_{\ast,e} = \Pi_{\ast,e}$. Since $\mathcal{A} \triangleright\triangleright e : \tau_g | \pi_g$ (by definition of $\triangleright\triangleright$) by Theorem 9 we know that $\Pi_{\ast,e}$ has a maximum element, and also $\Pi_{\ast,e}$.
    \end{itemize}
\end{itemize}
We will prove that \( \forall e \in \tau_g \pi_g \Rightarrow \Pi_{\cdot e}^\bullet \) has not a maximum element.

(A) \( \forall e \in \tau_g \pi_g \) because \( \forall e \in \tau_g \pi_g \). We know from Theorem 9 that if \( \forall e \in \tau_g \pi_g \) then \( \Pi_{\cdot e}^\bullet \) has not a maximum element. Then by Theorem 5 it cannot exists any type derivation \( \forall e \vdash \tau' \), so \( \Pi_{\cdot e}^\bullet \) is empty.

Since \( \Pi_{\cdot e}^\bullet \subseteq \Pi_{\cdot e}^\bullet \) then \( \Pi_{\cdot e}^\bullet = \emptyset \) and cannot contain any maximum element.

(B) \( \forall e \in \tau_g \pi_g \) because \( \exists e \vdash \tau_g \pi_g \) and \( \text{critVar}_{\cdot \pi_g}(e) \neq \emptyset \). We will proceed by case distinction over the cause of the critical variables:

(B.1) \( \text{critVar}_{\cdot \pi_g}(e) \neq \emptyset \) because for every pattern \( t_j \) and for every variable \( X \) such that \( \exists X \vdash t_j \) then \( \forall X \vdash t_j \pi_g \) and \( \forall \pi_g \vdash t_j \pi_g \).

Let be \( \beta_k \) all the type variables causing opacity, and \( \tau^1 \) and \( \tau^2 \) two non unifiable types (\( \text{bool} \) and \( \text{char} \), for example). Then we can define \( \pi_1 \equiv [\beta_k/\tau^1] \) and \( \pi_2 \equiv [\beta_k/\tau^2] \). Since \( \exists X \vdash e \vdash \tau_g \pi_g \) by Theorem 4 \( \forall X \vdash e \vdash \tau_g \pi_g \), and by Theorem 4 \( \forall X \vdash e \vdash \tau_g \pi_g \).

We have eliminated the cause of opacity, so \( \text{critVar}_{\cdot \pi_g}(e) = \emptyset \) and \( \text{critVar}_{\cdot \pi_g}(e) = \emptyset \), i.e., \( \pi_g \pi_1, \pi_g \pi_2 \in \Pi_{\cdot e}^\bullet \). Finally since \( \tau^1 \) and \( \tau^2 \) are not unifiable, the only substitution more general that \( \pi_g \pi_1 \) and \( \pi_g \pi_2 \) that could be in \( \Pi_{\cdot e}^\bullet \) is \( \pi_g \) (substitutions more general than \( \pi_g \) cannot be in \( \Pi_{\cdot e}^\bullet \), and neither in \( \Pi_{\cdot e}^\bullet \)). But \( \pi_g \) is not in \( \Pi_{\cdot e}^\bullet \) because \( \text{critVar}_{\cdot \pi_g}(e) \neq \emptyset \). Therefore \( \Pi_{\cdot e}^\bullet \) cannot have a maximum element because we have found two elements in \( \Pi_{\cdot e}^\bullet \) that do not have any “greater” element in \( \Pi_{\cdot e}^\bullet \).

(B.2) \( \text{critVar}_{\cdot \pi_g}(e) \neq \emptyset \) because there exists some pattern \( t_j \) in \( e \) in which there is any variable \( X \) that is opaque because of type variables that do not occur in \( \forall X \vdash e \vdash \tau_g \pi_g \). Intuitively in this case these type variables will have appeared because of there exist a symbol in \( t_j \) whose type is a type-scheme, and that fresh variables come from the fresh variant used. From Theorem 5 we know that for every \( \pi_e \in \Pi_{\cdot e}^\bullet \) then \( \forall X \vdash e \vdash \tau_g \pi_g \) for some type substitution \( \pi' \). But \( \text{critVar}_{\cdot \pi_g}(e) = \text{critVar}_{\cdot \pi_g}(e) \neq \emptyset \), because we always have fresh type variables causing opacity (since they come from type-schemes, substitutions do not affect them). Therefore for every \( \pi_e \in \Pi_{\cdot e}^\bullet \) then \( \text{critVar}_{\cdot \pi_g}(e) \neq \emptyset \), and as \( \Pi_{\cdot e} \subseteq \Pi_{\cdot e}^\bullet \) then \( \Pi_{\cdot e}^\bullet = \emptyset \), so it has not a maximum element.
b) By definition of $\vdash^*$ and $\equiv^*$ we know that $A\pi' \vdash e : \tau'$ and $A \equiv e : \tau | \pi$. Then by Theorem 5 we know that there exists a type substitution $\pi''$ such that $A\pi' = A\pi\pi''$ and $\tau' = \tau \pi'$. 

**Theorem 7 (Soundness of $B$).**

$B(A, \mathcal{P}) = \pi \implies wt_{A\pi}(\mathcal{P})$.

*Proof.* From $B(A, \mathcal{P}) = \pi$ we have $A \equiv^* (\varphi(r_1), \ldots, \varphi(r_m)) : (\tau_1, \ldots, \tau_m) | \pi$, and by Theorem 4 then $A\pi \vdash^* (\varphi(r_1), \ldots, \varphi(r_m)) : (\tau_1, \ldots, \tau_m)$. In order to prove $wt_{A\pi}(\mathcal{P})$ we need to prove that every rule $r_i \equiv f_i \ t_1 \ldots t_n \rightarrow e_i$ in $\mathcal{P}$ is well-typed wrt. $A\pi$. From Lemma 10 we know that $A\pi \vdash^* \varphi(r_i) : \tau_i$, so $A\pi \vdash^* \text{pair } \lambda t_1 \ldots t_n, e_i \ f_i : \tau_i$. This derivation can only be constructed if $A\pi \vdash^* \lambda t_1 \ldots t_n, e_i : \tau_i$ and $A\pi \vdash^* f_i : \tau_i$, and as the last derivation is just an application of rule [ID], $A\pi(f_i) \succ \tau_i$. We will distinguish between the case that $A(f_i)$ is a simple type or a closed type-scheme:

a) If $A(f_i)$ is a simple type, then $A\pi(f_i)$ too. In this case $A\pi(f_i) \succ \tau_i$ can only be true if $A\pi(f_i) = \tau_i$, so trivially $\tau_i$ is a variant of $A\pi(f_i)$. Therefore $A\pi \vdash^* \lambda t_1 \ldots t_n, e_i : \tau_i$ and $\tau_i$ is a variant of $A\pi(f_i)$, so rule $r_i$ is well-typed wrt. $A\pi$.

b) $A(f_i)$ is a closed type scheme, so $A(f_i) = A\pi(f_i)$. From step 2.- of $B$ we know that in this case $\tau_i$ is a variant of $A(f_i)$, and also of $A\pi(f_i)$. Then since $A\pi \vdash^* \lambda t_1 \ldots t_n, e_i : \tau_i$ rule $r_i$ is well-typed wrt. $A\pi$.

**Theorem 8 (Maximality of $B$).**

If $wt_{A\pi}(\mathcal{P})$ and $B(A, \mathcal{P}) = \pi$ then $\exists \pi''$ such that $A\pi' = A\pi\pi''$.

*Proof.* Since $wt_{A\pi}(\mathcal{P})$ we know that for every rule $r_i \equiv f_i \ t_1 \ldots t_n \rightarrow e_i$ in $\mathcal{P}$ there exists a type derivation $A\pi' \vdash^* \lambda t_1 \ldots t_n, e_i : \tau_i'$ and $\tau_i'$ is a variant of the type $A\pi(f_i)$. Then $A\pi' \vdash^* f_i : \tau_i'$, and we can construct type derivations $A\pi' \vdash^* \text{pair } \lambda t_1 \ldots t_n, e_i : \tau_i'$ with these derivations we can build $A\pi' \vdash^* (\varphi(r_1), \ldots, \varphi(r_m)) : (\tau_1', \ldots, \tau_m')$ by Lemma 10. From $B(A, \mathcal{P}) = \pi$ we know that $A \equiv^* (\varphi(r_1), \ldots, \varphi(r_m)) : (\tau_1, \ldots, \tau_m) | \pi$, so by Theorem 6 there will exist some type substitution $\pi''$ such that $A\pi' = A\pi\pi''$.

**Theorem 9 (Maximality of $\equiv^*$).**

$\Pi_{A, e}$ has a maximum element $\pi \iff \exists \pi_g, \pi_g \in SType. A \equiv e : \tau_g | \pi_g$.

*Proof.*

$\implies$) If $\Pi_{A, e}$ has maximum element $\pi$ then there will be some type $\tau$ such that $A\pi \vdash e : \tau$. Then by Theorem 5 we know that $A \equiv e : \tau_g | \pi_g$.

$\Leftarrow$) We know from Theorem 5 that for every type substitution $\pi' \in \Pi_{A, e}$ there exists a type substitution $\pi''$ such that $A\pi' = A\pi\pi''$. Then $\pi | FTV(A) \lesssim \pi''$. From Theorem 4 we know that $\pi | FTV(A)$ is in $\Pi_{A, e}$, so it is the maximum element.