Type Inference for Rank-2 Intersection Types using Set Unification

Pedro Ângelo[1,2,3] and Mário Florido[1,2,4]

[1] DCC/FCUP - Departamento de Ciência de Computadores, Faculdade de Ciências da Universidade do Porto
[2] LIACC - Laboratório de Inteligência Artificial e Ciência de Computadores
[3] up201207861@fc.up.pt
[4] amflorid@fc.up.pt

Abstract. Several type inference approaches for rank-2 idempotent and commutative intersection types have been presented in the literature. Type inference relies in two stages: type constraint generation and solving. Defining constraint generation rules is rather straightforward, with one exception. To infer the type of an application, several derivations of the argument are required, one for each instance of the domain type of the function. The types of these derivations are then constrained against the instances. Noting that these derivations are isomorphic, by renaming of type variables, they can be obtained via a duplication operation on a single derivation of the argument. The application rule then constrains the intersection type resulting from duplication against the domain type of the function, resulting in an equality constraint between intersections. By treating intersections as sets, these constraints can be solved by solving a set unification problem, thus ensuring the types of the argument unify with the domain type of the function. Here we present a new type inference algorithm for rank-2 intersection types, which relies on set unification to solve equality constraints between intersections, and show it is both sound and complete.

Keywords: Intersection types · Type inference · Set unification.

1 Introduction

The benefits (and the costs) of strong static typing in programming languages are now generally recognized. Languages such as ML, Haskell or Java are examples of the use of strong typing. To avoid the extra effort of declaring types for every part of the program, compilers should infer types as much as possible. And to avoid rejecting well behaved programs as much as possible, type inference should be able to support some form of polymorphism. Two of the main options for polymorphism are universally quantified types (such as the Damas-Milner type system [13] and System $\mathcal{F}$ [24,23,35]), and intersection types [10].

Intersection types originate in the works of Barendregt, Coppo and Dezani [11,10,5] and give us a characterization of the strongly normalizable terms. New attention was given to intersection type systems due to a result of Kfoury and Wells [30] which proved that these systems are decidable for restrictions of finite rank, which correspond to a large class of typable terms.

Consider the following example: in intersection type systems $\lambda x \ . \ x \ x$ has type $(\alpha \wedge \alpha \rightarrow \beta) \rightarrow \beta$. Note that the two (non-unifiable) types of the variable x belong to the domain type of the abstraction linked by the intersection operator. A more interesting example is the term $(\lambda x \ . \ x \ x) \ I$, where I is the identity function $\lambda x \ . \ x$. This term has type $\alpha \rightarrow \alpha$ which does not involve intersections, although it is not typable in the simply typed lambda calculus [12,26] because it has a non-typable subterm.

Intersection type systems characterise the set of strongly normalising terms and have an huge expressive power typing more terms than the simply typed lambda calculus or the type system of pure ML or core Haskell. Applications of intersection type systems in programming language theory cover diverse topics including the design of programming languages [36,6], program analysis [32], program synthesis [21], and extensions such as refinement, union and gradual types [22,19,18,3,8,9]. But this huge expressive power comes with a price. Type theoretic problems such as type inference and inhabitation are undecidable in general [38,4].

In [30] Wells and Kfoury define an intersection type system which types exactly the strongly normalizable terms and show that every finite-rank restriction of this system, using Leivant's notion of rank [31], has principal typings and also has decidable type inference. This system used expansion variables, which are subject to substitution as are ordinary variables and a unification-based type inference algorithm using a new form of unification called β-unification. Due to the complexity of type inference algorithms for higher finite ranks, the most successful decidable fragments of intersection type systems have focused on the rank-2 restriction. The rank of a type can be easily determined by its syntactic tree. A type is of rank n if no path from the root of the syntactic tree of the type to an intersection passes to the left of n arrows. Rank 0 and 1 are equivalent to the simple typed lambda-calculus. But starting from rank 2, the systems type more terms than the type system of pure ML or Core Haskell.

Van Bakel presents a unification algorithm as the basis of type inference for a rank-2 system [39]. Later, independent work by Trevor Jim also solves the same problem for practical programming language issues such as recursive definitions and separate compilation [28]. Damiani [14] also studied rank-2 principal typings with intersection types and focus his work on rank-2 typable recursive definitions.

All these previous algorithms rely on extensions to first-order unification [37], either explicit, as in [39,30], or implicit, as in [27,28], where a more general form of type constraints corresponding to subtyping is first generated, and subsequently, in the constraint solving phase, further simplified by rewriting subtyping into equalities.

Originally [11,10], intersection types were denoted by finite sets of types:

"The main idea is to define from an arbitrary set of types $\{\tau_1, \cdots, \tau_n\}$ *a "se-*

quence" $[\tau_1, \cdots, \tau_n]$ whose underlying set of terms can be interpreted as the intersection of those of $\tau_1, \cdots, \tau_n$." [10]

Picking up on this original motivation, we here define a new type inference algorithm for rank-2 intersection types which relies on *set unification* [16,17] to solve the type constraints generated by function applications.

The main contributions of this paper are the following:

- A unification-based type inference algorithm for rank-2 intersection types using set unification. The algorithm is terminating and always returns principal typings when it halts. One nice feature of this algorithm is its similarity with type inference for simple types [33] - just replace first-order unification by set unification.
- Proofs of soundness and completeness of the algorithm, meaning that the outputs of type inference are types which are derivable in a rank-2 intersection type system, and more, they are principal typings in the sense that every other type derivable in the type system may be obtained from them using substitution.

It is important to note that the majority of the discussed results can be obtained by the other previously defined rank-2 intersection type inference algorithms. Nonetheless, it is our belief that the work in this paper constitutes further a step towards a better understanding of the role of set unification as the base of type inference algorithms for intersection types and may highlight how intersections at different depth are related to different restrictions of set unification in the type inference mechanism.

The paper is organized as follows. Section 2 introduces the syntax of the system. A rank-2 intersection type system where every type declared in the context is used in the type derivation is presented in section 3. The formalization of the type inference algorithm, along with its components, follows in section 4. The first phase of the algorithm consists of the constraint generation rules, which are detailed in subsection 4.1. In particular, we present an alternative design to the rule for applications: by requiring only one derivation and then duplicating it, there is a derivation of the argument for each instance in the domain type of the function. Set unification, explained in subsection 4.2, will be required to solve equality constraints between intersection types. The general constraint solving rules are presented in subsection 4.3. We finally produce the type inference algorithm, along with important properties, in subsection 4.4. The conclusion follows in section 5.

2 Types and Terms

Our language is an intersection typed lambda calculus à la Curry, which supports term constants, such as integers and booleans, and built-in addition. Other arithmetic operations can be defined similarly. The syntax of our language is given by the following grammar:

Definition 1 (Syntax).

$$\begin{array}{llll} \textit{monotypes} & \tau & ::= & B \mid \alpha \mid \sigma \to \tau \\ \textit{sequences} & \sigma & ::= & \tau_1 \wedge \ldots \wedge \tau_n \mid \phi \\ \textit{terms} & M & ::= & k \mid x \mid \lambda x\ .\ M \mid M\ M \mid M + M \\ \textit{typing context} & \Gamma & ::= & \emptyset \mid \Gamma, x : \sigma \qquad \textit{with } \sigma \in \mathcal{T}_1 \\ \textit{constraint} & C & ::= & \sigma \doteq \sigma \\ \textit{constraints} & C^* & ::= & \emptyset \mid C^* \cup C \end{array}$$

B ranges over base types such as Int and Bool, α and β range over type variables and ϕ ranges over sequence variables. τ and ρ range over monotypes i.e. the top level constructor is not the intersection type connective, and σ and υ range over sequences. M and N range over terms, x, y and z range over term variables and k ranges over constants, such as integers and booleans. Γ ranges over typing contexts, and $\emptyset$ represents an empty context. C ranges over equality constraints, written as $\sigma \doteq \sigma$, and C^* ranges over multisets of equality constraints C.

Remark 1. The indexes i, j, m, n, p and q range over the set $\mathbb{Z}_0^+$.

Remark 2. We distinguish meta-variables presented in this paper with different subscript natural numbers, and also with superscript apostrophe.

As in the original system [10,34], we consider the intersection connective $\wedge$ as commutative, e.g. $\tau \wedge \rho = \rho \wedge \tau$, and idempotent, e.g. $\tau \wedge \tau = \tau$. We do not consider associativity, since we are not dealing with a binary operator. Therefore, an intersection type $\tau_1 \wedge \ldots \wedge \tau_n$ is seen as the set of types $\tau_1, \ldots, \tau_n$. Given a sequence $\tau_1 \wedge \ldots \wedge \tau_n$, each τ_i is called an *instance* of the intersection. We allow sequences of size one, so σ and υ also range over monotypes, or monotypes with wildcards. Sequences can only appear in the left-hand side of the arrow type constructor, therefore the shape of a (valid) arrow type is $\sigma \to \tau$. The intersection type connective $\wedge$ has a higher precedence than the arrow type constructor $\to$, and $\to$ associates to the right.

We use χ (possibly with subscripts) to range over sets of type, and sequence, variables.

Definition 2 (Type Variables). *We define the function $tvars(.)$, that returns the set of type, and sequence, variables occurring in a given type, as follows: $tvars(\sigma) \stackrel{def}{=} \{\alpha \mid \alpha \text{ occurs in } \sigma\} \cup \{\phi \mid \phi \text{ occurs in } \sigma\}$.*

Definition 3 (Free Variables). *We define the function $fvars(.)$, that returns the set of free term variables occurring in a given term, as follows: $fvars(M) \stackrel{def}{=} \{x \mid x \text{ occurs free in } M\}$.*

Definition 4 (Atomic Type Sets). *We categorize atomic types in our language according to the following sets:*

$$\begin{array}{lll} \mathcal{T}_{base} & = & \{B \mid B \text{ is a base type}\} \\ \mathcal{T}_{tvar} & = & \{\alpha \mid \alpha \text{ is a type variable}\} \\ \mathcal{T}_{svar} & = & \{\phi \mid \phi \text{ is a sequence variable}\} \end{array}$$

According to the definition of rank restriction [31,28], a *rank n intersection type* can have no intersection type connective $\wedge$ to the left of n or more arrow type constructors $\rightarrow$:

Definition 5 (Rank). *We categorize the types of our language according to rank:*

$$\begin{array}{llcl} \textit{simple types} & \mathcal{T}_0 & = & \mathcal{T}_{base} \cup \mathcal{T}_{tvar} \cup \{\tau \rightarrow \rho \mid \tau,\ \rho \in \mathcal{T}_0\} \\ \textit{rank 1 types} & \mathcal{T}_1 & = & \mathcal{T}_0 \cup \mathcal{T}_{svar} \cup \{\tau_1 \wedge \ldots \wedge \tau_n \mid \tau_1,\ \ldots,\ \tau_n \in \mathcal{T}_0\} \\ \textit{rank 2 types} & \mathcal{T}_2 & = & \mathcal{T}_0 \cup \{\sigma \rightarrow \tau \mid \sigma \in \mathcal{T}_1,\ \tau \in \mathcal{T}_2\} \end{array}$$

We restrict types in our system to be only of up to rank 2, so the only possible types are those belonging to $\mathcal{T}_1 \cup \mathcal{T}_2$, e.g. $(((\tau \rightarrow \rho) \wedge \tau) \rightarrow \rho) \rightarrow \tau$ is not a valid type.

Remark 3. We denote the singleton context, which contains only one type binding, as $x : \sigma$. We write Γ_1, Γ_2 for the union of contexts Γ_1 and Γ_2, assuming Γ_1 and Γ_2 are disjoint.

Definition 6 (Joining Typing Contexts). *Let Γ_1 and Γ_2 be two typing contexts. $\Gamma_1 \wedge \Gamma_2$ is a typing context, where $x : \sigma \in \Gamma_1 \wedge \Gamma_2$ if and only if σ is defined as follows:*

$$\sigma = \begin{cases} \sigma_1 \wedge \sigma_2, & if\ x : \sigma_1 \in \Gamma_1\ and\ x : \sigma_2 \in \Gamma_2 \\ \sigma_1, & if\ x : \sigma_1 \in \Gamma_1\ and\ \neg\exists\sigma_2\ .\ x : \sigma_2 \in \Gamma_2 \\ \sigma_2, & if\ \neg\exists\sigma_1\ .\ x : \sigma_1 \in \Gamma_1\ and\ x : \sigma_2 \in \Gamma_2 \end{cases}$$

3 Type System

In figure 1 we define an intersection type system where every type declared in the context is used in the type derivation, a property which is going to be quite useful in subsequent results.

The two rules for abstractions, [T-AbsI] and [T-AbsK], are necessary because in this system if there is a derivation of $\Gamma \vdash_\wedge M : \sigma$ and x does not occur free in M, then there is not a type declaration for x in Γ. The set of types for a given term M in this system is strictly included in the set of types for M in the original intersection type system of Coppo and Dezani [11,10]. For example, the type $(\alpha_1 \cap \alpha_2) \rightarrow \alpha_1$ types $\lambda x\ .\ x$ in the Coppo-Dezani type system but not in our system. The reason for this is that types in intersections for free variables can only be introduced with the T-APP rule and thus each element of the intersection corresponds to a type that is actually used in the type derivation. However the set of terms typable in both systems is the same and corresponds to the strongly normalizable terms (a proof of this for a similar type system can be found in [20]).

One peculiarity of this type system is that it does not satisfy the property of *subject reduction* as it is shown by the following example:

$$[\text{T-Con}]\ \frac{\text{k is a constant of base type B}}{\emptyset \vdash_\wedge k : B} \qquad [\text{T-Var}]\ \frac{}{x : \tau \vdash_\wedge x : \tau}$$

$$[\text{T-AbsI}]\ \frac{\Gamma, x : \sigma \vdash_\wedge M : \tau}{\Gamma \vdash_\wedge \lambda x\ .\ M : \sigma \to \tau} \qquad [\text{T-AbsK}]\ \frac{\Gamma \vdash_\wedge M : \tau}{\Gamma \vdash_\wedge \lambda x\ .\ M : \sigma \to \tau}\ x \notin fvars(M)$$

$$[\text{T-App}]\ \frac{\begin{array}{c}\Gamma \vdash_\wedge M : \tau_1 \wedge \ldots \wedge \tau_n \to \tau \\ \forall i \in 1..n\ .\ \Gamma_i \vdash_\wedge N : \tau_i\end{array}}{\Gamma \wedge \Gamma_1 \wedge \ldots \wedge \Gamma_n \vdash_\wedge M\ N : \tau}$$

$$[\text{T-Add}]\ \frac{\Gamma_1 \vdash_\wedge M : \mathit{Int} \qquad \Gamma_2 \vdash_\wedge N : \mathit{Int}}{\Gamma_1 \wedge \Gamma_2 \vdash_\wedge M + N : \mathit{Int}}$$

Fig. 1. Intersection Type System ($\Gamma \vdash_\wedge M : \sigma$)

Example 1. In this system

$$z : \alpha_2 \to \beta \vdash_\wedge \lambda x\ .\ (\lambda y\ .\ z)\ x\ x : \alpha_1 \cap \alpha_2 \to \beta$$

and

$$\lambda x\ .\ (\lambda y\ .\ z)\ x\ x \underset{\beta}{\to} \lambda x\ .\ z\ x$$

but

$$z : \alpha_2 \to \beta \not\vdash_\wedge \lambda x\ .\ z\ x : \alpha_1 \wedge \alpha_2 \to \beta$$

The lack of subject reduction also happens in other restrictions of intersection type systems where every type in the environment has to be used in the type derivation [15,30]. The reason for the lack of subject reduction is that there is no weakening introducing unneeded type assumptions. Note that the lack of subject reduction is not a problem, because derivations in this system can be easily translated into derivations on more standard systems of intersection types which have subject reduction. Defining the system without a weakening mechanism makes the later analysis about type inference much easier.

4 Type Inference

We follow a conventional approach to type inference [40]: a constraint generation phase generates type constraints from the term, and a constraint solving phase which solves these constraints to generate type substitutions.

We define substitution on types in the standard way [33], extended to allow intersections.

Definition 7 (Substitution). *Let S range over standard type substitutions [33]. We write $[\alpha \mapsto \tau]$ for a type substitution on monotypes that maps a type variable α into a monotype τ; and $[\phi \mapsto \sigma]$ for a type substitution on sequences that maps a sequence variable ϕ into a sequence σ.*

For each type system rule in figure 1, we require an analogous constraint generation rule. Deriving these from the type system is done in a rather straightforward manner: convert judgments in the premises to constraint generation judgments, while making the type opaque; then convert the judgment in the conclusion, adding constraints that reflect how types relate to each other in the type system.

Deriving a constraint generation rule from [T-App] is not as straightforward. In the type system rule for applications, the function is assumed to be typed with an arrow type. However, the same assumption cannot be made for the constraint generation rules. Therefore, two constraint generation rules for applications are required: [G-App$\wedge$] where this assumption holds, and [G-App], where an opaque type is inferred for the function. In standard systems [27], the application rule which assumes the type of the function is an arrow type behaves similarly to rule [T-App]. The rule ensures there are distinct type derivations of the argument, exactly one for each instance of the domain type of the function. By having distinct type derivations, the rule ensures the argument fits into each occurrence of the bound variable in the body of the lambda abstraction.

Here we follow a different approach. Instead of having several derivations, the application rule has a single derivation of the argument. Then, we duplicate the type obtained from this derivation, constraining each copy to each instance in the domain type of the function. We define the duplication operation as in [39]:

Definition 8 (Duplication). *Let $\chi = \{\alpha_1, \ldots, \alpha_j\} \cup \{\phi_{j+1}, \ldots, \phi_m\}$ be a set of type and sequence variables; let $\beta_{11}, \ldots, \beta_{1n}, \ldots, \beta_{m1}, \ldots, \beta_{mn}$ be fresh type variables; and let $S_i = [\alpha_1 \mapsto \beta_{1i}, \ldots, \alpha_j \mapsto \beta_{ji}, \phi_{j+1} \mapsto \beta_{(j+1)i}, \ldots, \phi_m \mapsto \beta_{mi}]$, for $1 \leq i \leq n$. The duplication function $duplicate^n_\chi(\tau)$ is defined as follows: $duplicate^n_\chi(\tau) \stackrel{def}{=} S_1(\tau) \wedge \ldots \wedge S_n(\tau)$.*

The argument χ represents the set of variables that will be duplicated, and the argument n represents the number of duplications. Therefore, n fresh variables β are required for each type variable in χ, to ensure new duplications. Only simple types ($\tau \in \mathcal{T}_0$) are duplicated, so sequence variables ϕ that might appear in the type are treated as simple types and replaced by type variables β. Note that if duplication is applied to a type without type variables, due to idempotence, duplication will return the same type, e.g. $duplicate^2_\chi(Int \to Int) = (Int \to Int) \wedge (Int \to Int)$, which is the same as $Int \to Int$. On the other hand, if type variables are considered, duplication will generate n many copies of the type, e.g. $duplicate^2_{\{\alpha_1,\alpha_2\}}(\alpha_1 \to \alpha_2) = (\beta_1 \to \beta_3) \wedge (\beta_2 \to \beta_4)$.

We give meaning to constraints through a satisfaction relation $\models$. A substitution S satisfies a constraint $\sigma \doteq \upsilon$ if and only if applying the substitution to both types in the constraint yields an equality. Taking into account that intersection types are idempotent and commutative, two sequences are equal if both share the same set of instances. Since we allow sequences of size one, the equality constraint between monotypes $\tau \doteq \rho$ is an instance of $\sigma \doteq \upsilon$, i.e. $S \models \tau \doteq \rho \iff S(\tau) = S(\rho)$.

Definition 9 (Constraint Satisfaction).

1. $S \models \emptyset$
2. $S \models \sigma \doteq \upsilon \iff S(\sigma) = S(\upsilon)$
3. $S \models C^* \iff S \models C$ *for all* $C \in C^*$

Definition 10 (Lifting Type Variables). *We lift function* $tvars(.)$*, from definition 2, to typing contexts* Γ *and equality constraints* C^* *in the obvious way.*

Definition 11 (Lifting Substitution). *We lift substitutions, from definition 7, to:*

- *typing contexts* Γ *in the obvious way;*
- *constraints in the following way:* $S(\sigma \doteq \upsilon) \stackrel{def}{=} S(\sigma) \doteq S(\upsilon)$*. Also,* $S(C^* \cup C) \stackrel{def}{=} S(C^*) \cup S(C)$ *and* $S(\emptyset) \stackrel{def}{=} \emptyset$*.*

Definition 12 (Lifting Duplication). *Assuming* $S_1, \ldots, S_n$ *are type substitutions generated from* χ *according to definition 8, we lift function* $duplicate^n_\chi(.)$*, from definition 8, to:*

- *typing contexts in the following way:* $duplicate^n_\chi(\Gamma) \stackrel{def}{=} S_1(\Gamma) \wedge \ldots \wedge S_n(\Gamma)$*;*
- *constraints in the following way:* $duplicate^n_\chi(C^*) \stackrel{def}{=} S_1(C^*) \cup \ldots \cup S_n(C^*)$*.*

Besides duplication the type of argument derivations in the application rule, we must also duplicate the typing context and constraints, to simulate several derivations of the same term. These derivations are just renamings of type variables of the original derivation.

Definition 13 (Duplication). *Let* $\langle \Gamma, \tau, C^* \rangle$ *be a triple composed of a typing context* Γ*, a type* τ *and constraints* C^**. We define the* duplication *function as* $duplicate^n(\langle \Gamma, \tau, C^* \rangle) = \langle [\Gamma_1, \ldots, \Gamma_n], [\tau_1, \ldots, \tau_n], [C^*_1, \ldots, C^*_n] \rangle$ *where:*

- $\chi = tvars(\Gamma) \cup tvars(\tau) \cup tvars(C^*)$*;*
- $duplicate^n_\chi(\Gamma) \equiv \Gamma_1 \wedge \ldots \wedge \Gamma_n$*;*
- $duplicate^n_\chi(\tau) \equiv \tau_1 \wedge \ldots \wedge \tau_n$*;*
- $duplicate^n_\chi(C^*) \equiv C^*_1 \cup \ldots \cup C^*_n$*.*

4.1 Constraint Generation

We define the constraint generation rules in figure 2. We follow [27], assigning fresh type variables to variables in [G-Var]. No assumptions are made for the type of the term variable, allowing it to be constrained to the correct type according to the context. Similarly to the type system, there are two constraint generation rules for lambda abstractions: [G-AbsI], when the bound variable occurs free in the body, and [G-AbsK], when it does not. When the bound variable occurs free in the body, rule [G-Var] will gather type assumptions in the context. Then, rules containing several premises, [G-App], [G-App$\wedge$] and [G-Add], join the contexts under an intersection (definition 6). Due to this, the

$$[\text{G-C}_{\text{ON}}]\ \frac{\text{k is a constant of base type B}}{\emptyset \vdash_\wedge k : B \mid \emptyset} \qquad [\text{G-V}_{\text{AR}}]\ \frac{\alpha \text{ fresh}}{x:\alpha \vdash_\wedge x : \alpha \mid \emptyset}$$

$$[\text{G-A}_{\text{BS}}\text{I}]\ \frac{\Gamma, x:\sigma \vdash_\wedge M : \tau \mid C^*}{\Gamma \vdash_\wedge \lambda x\ .\ M : \sigma \to \tau \mid C^*}$$

$$[\text{G-A}_{\text{BS}}\text{K}]\ \frac{\Gamma \vdash_\wedge M : \tau \mid C^* \qquad \phi \text{ fresh}}{\Gamma \vdash_\wedge \lambda x\ .\ M : \phi \to \tau \mid C^*}\ x \notin fvars(M)$$

$$[\text{G-A}_{\text{PP}}\wedge]\ \frac{\begin{array}{c}\Gamma_1 \vdash_\wedge M : \tau_1 \wedge \ldots \wedge \tau_n \to \tau \mid C_1^* \qquad \Gamma_2 \vdash_\wedge N : \rho \mid C_2^* \\ \mathit{duplicate}^n(\langle \Gamma_2, \rho, C_2^* \rangle) = \langle [\Gamma_{21}, \ldots, \Gamma_{2n}], [\rho_1, \ldots, \rho_n], [C_{21}^*, \ldots, C_{2n}^*] \rangle \\ C = \tau_1 \wedge \ldots \wedge \tau_n \doteq \rho_1 \wedge \ldots \wedge \rho_n \end{array}}{\Gamma_1 \wedge \Gamma_{21} \wedge \ldots \wedge \Gamma_{2n} \vdash_\wedge M\ N : \tau \mid C_1^* \cup C_{21}^* \cup \ldots \cup C_{2n}^* \cup C}$$

$$[\text{G-A}_{\text{PP}}]\ \frac{\Gamma_1 \vdash_\wedge M : \tau \mid C_1^* \qquad \Gamma_2 \vdash_\wedge N : \rho \mid C_2^* \qquad \alpha \text{ fresh}}{\Gamma_1 \wedge \Gamma_2 \vdash_\wedge M\ N : \alpha \mid C_1^* \cup C_2^* \cup \{\tau \doteq \rho \to \alpha\}}$$

$$[\text{G-A}_{\text{DD}}]\ \frac{\Gamma_1 \vdash_\wedge M : \tau \mid C_1^* \qquad \Gamma_2 \vdash_\wedge N : \rho \mid C_2^*}{\Gamma_1 \wedge \Gamma_2 \vdash_\wedge M + N : \mathit{Int} \mid C_1^* \cup \{\tau \doteq \mathit{Int}\} \cup C_2^* \cup \{\rho \doteq \mathit{Int}\}}$$

Fig. 2. Constraint Generation ($\Gamma \vdash_\wedge M : \tau \mid C^*$)

domain of the function type in the conclusion of rule [G-AbsI] corresponds to the intersection of the types of all ocurrences of the bound variable, which is given by the context in the premise of the rule. When the bound variable does not occur free in the body, there is no information regarding the type for the domain. Rule [G-AbsK] then returns an arrow type whose domain is a fresh sequence variable.

Whereas in the type system, we have a single application rule, two constraint generation rules are required: [G-App$\wedge$] and [G-App]. In [G-App$\wedge$], the type of the function term is an arrow and its domain is an intersection. Then, the type of the function term, particularly the domain $\tau_1 \wedge \ldots \wedge \tau_n$, constrains how many derivations are needed of the argument term. For each instance in the domain type of the function, a derivation of the argument is required. Furthermore, each instance must unify with its corresponding argument's type.

However, instead of following the standard approach [27] of ensuring multiple derivations of the argument, we explore a different approach. In fact, generating multiple derivations of the argument amounts to duplicating type variables found in the context, type and constraints. We made this explicit in rule [G-App$\wedge$].

If the type of the function term is not an arrow, then there is no information on the number of derivations required of the argument term, so only one is needed. Furthermore, the type of the function is constrained to be an arrow type, and its domain to match the argument's type, as specified in [G-App].

We show the following properties of our constraint generation algorithm:

Lemma 1 (Soundness of Constraint Generation). *If* $\Gamma \vdash_\wedge M : \tau \mid C^*$ *and* $S \models C^*$ *then* $S(\Gamma) \vdash_\wedge M : S(\tau)$.

Proof. Proof by induction on the length of the derivation tree of $\Gamma \vdash_\wedge M : \tau \mid C^*$.

Lemma 2 (Completeness of Constraint Generation). *If* $S_1(\Gamma) \vdash_\wedge M : \tau$ *then* $\Gamma \vdash_\wedge M : \rho \mid C^*$ *s.t. the domain of* S_1 *is disjoint from* χ*, and* $\exists S_2$ *s.t.* S_2 *agrees with* S_1 *except at* χ, $S_2 \models C^*$ *and* $S_2(\rho) = \tau$*, where* χ *are the fresh variables introduced in the derivation of* $\Gamma \vdash_\wedge M : \rho \mid C^*$.

Proof. Proof by induction on the length of the derivation tree of $S_1(\Gamma) \vdash_\wedge M : \tau$.

4.2 Set Unification

Type inference for simple types relies in first-order unification. However, equality constraints between idempotent and commutative intersection types are not so easy to solve. Solving such constraints involves finding the correct association between instances in both sequences. If we consider sequences as sets, this problem is equivalent to solving a set unification problem [17,16].

According to [17], a set is an arbitrary, unordered collection of elements, i.e. the order and repetition of elements do not matter. Since we consider the intersection type operator $\wedge$ as idempotent and commutative, a sequence $\tau_1 \wedge \ldots \wedge \tau_n$ can be interpreted as a set $\{\tau_1, \ldots, \tau_n\}$, whose elements are the instances of the sequence. By definition 1, a sequence can have as instances base types B, type variables α, and arrows $\sigma \rightarrow \tau$. These are the building blocks of sequences, so we define their counterparts for sets:

Definition 14 (Individuals). *We define the set of individuals* $\mathcal{U}$ *in the following way:*

- *if* $B \in \mathcal{T}_{base}$ *then* $B \in \mathcal{U}$*;*
- *if* s, t *are abstract set terms, then* $\rightarrow (s, t) \in \mathcal{U}$*.*

Individuals are essentialy ground terms that make up our sets. Besides base types B, we also consider the arrow type as an individual, however, one with two arguments. We now define abstract set terms, according to [17]:

Definition 15 (Abstract Set Terms). *An abstract set term is a term of the form:*

$$\{X_1, \ldots, X_m, a_1, \ldots, a_n, s_1, \ldots, s_p\} \cup Y_1 \cup \ldots \cup Y_q \quad m, n, p, q \geq 0$$

where X_i, Y_i *are variables,* a_i *are individuals, and* s_i, t_i *are abstract set terms (distinct from variables).*

From the above definition, we can define the class of sets as follows: for $m \geq 0, n \geq 0, p \geq 0, q \geq 0$, the class $set(m, n, p, q)$ represents the collection of all abstract set terms $\{X_1, \ldots, X_{m'}, a_1, \ldots, a_{n'}, s_1, \ldots, s_{p'}\} \cup Y_1 \cup \ldots \cup Y_{q'}$ such that $0 \geq m' \geq m, 0 \geq n' \geq n, 0 \geq p' \geq p, 0 \geq q' \geq q$.

Even though a general definition of abstract set terms is presented, most of its expressive power won't be utilized when we translate sequences into sets. The language of types, as well as rank restrictions (definition 5), restricts the expressive power of sequences to be less than that of abstract set terms, i.e. abstract set terms represent a richer language than sequences. Due to rank restriction, we only consider rank 1 sequences, therefore sequences cannot contain other sequences as elements. This restriction means that abstract set terms s_i inside sets are not permitted. Furthermore, extra variables Y_i have no counterpart in our sequences. Therefore, we only need a restricted fragment of abstract set terms: the class $flat(0) = \bigcup_{m \geq 0, n \geq 0} \; set(m, n, 0, 0)$, which represents the collection of sets of the form $\{X_1, \ldots, X_m, a_1, \ldots, a_n\}$. Therefore, rank 1 sequence solving is equivalent to the Set Unification Decision [17] problem between two flat(0) sets.

The algorithm from [17,16] will allow us to solve equality constraints between sequences. However, we must first translate sequences to abstract set terms, which can be then passed onto the unification algorithm:

Definition 16 (Types as Abstract Set Terms). *We define our translation function* $(\!|.|\!)$ *according to the following rules:*

$$\frac{B \in \mathcal{T}_{base}}{(\!|B|\!) = B} \qquad \frac{}{(\!|\alpha|\!) = X} \qquad \frac{(\!|\sigma|\!) = s \qquad (\!|\upsilon|\!) = t}{(\!|\sigma \to \tau|\!) = \to (s, t)}$$

$$\frac{(\!|\tau_1|\!) = t_1 \;\ldots\; (\!|\tau_n|\!) = t_n}{(\!|\tau_1 \wedge \ldots \wedge \tau_n|\!) = \{t_1, \ldots, t_n\}}$$

The translation function is bijective, and we define its inverse as follows: assuming $(\!|\sigma|\!) = s$*, then we have that* $(\!|s|\!)^{inv} = \sigma$*.*

With an encoding of sequences as sets, we can unify two sets with algorithm `AbCl_unify` [17,16]. As two sets can be unified in several ways, this algorithm is non-deterministic, i.e. provides various solutions, albeit all correct. Therefore, by using `AbCl_unify`, our constraint solving algorithm will also be non-deterministic. We encapsulate the unification algorithm as well as the necessary translation, and define the sequence solving procedure $C \stackrel{s}{\Rightarrow} S$:

Definition 17 (Sequence Solving). *Let* $\sigma \doteq \upsilon$ *be an equality constraint between two rank 1 sequences* σ *and* υ*. The sequence solving procedure* $(\sigma \doteq \upsilon) \stackrel{s}{\Rightarrow} S_i$*, that non-deterministically returns a set of substitutions* $S_1, \ldots, S_n$*, is defined by the following steps.*

Let $(\sigma \doteq \upsilon) \stackrel{s}{\Rightarrow} S_i$*, such that:*

1. *let* t, s *be abstract set terms such that* $(\!|\sigma|\!) = t$ *and* $(\!|\upsilon|\!) = s$*;*
2. *choose an arbitrary solution* $\mathcal{E}_i$ *returned by* `AbCl_unify`$(\{t = s\})$*:*
   (a) *for every solved form equation* $X = t' \in \mathcal{E}_i$*, if* $(\!|X|\!)^{inv} = \alpha$ *and* $(\!|t'|\!)^{inv} = \sigma'$*, then* $[\alpha \mapsto \sigma'] \in S_i$

We transcribe the soundness and completeness result from [16], from which we can then derive our own:

Theorem 1 (Soundness and Completeness of `AbCl_unify` [16]). *Given a system $\mathcal{E}$, let $\mathcal{E}_1, \ldots, \mathcal{E}_n$ be all the systems in solved form produced by the unification algorithm. Then $Soln(\mathcal{E}) = Soln(\mathcal{E}_1)|_{vars(\mathcal{E})} \cup \ldots \cup Soln(\mathcal{E}_n)|_{vars(\mathcal{E})}$ where $Soln(X)$ is the set of all ground set-unifiers of X and $Soln(\mathcal{E}_i)|_{vars(\mathcal{E})}$ is $Soln(\mathcal{E}_i)$ restricted to the variables of $\mathcal{E}$.*

Lemma 3 (Soundness of Sequence Solving). *If $(\sigma \doteq \upsilon) \overset{s}{\Rightarrow} S$ then $S \models \sigma \doteq \upsilon$.*

Proof. If $(\sigma \doteq \upsilon) \overset{s}{\Rightarrow} S_i$, for all $i \in 1..n$, then by definition 17: $(\!|\sigma|\!) = t$ and $(\!|\upsilon|\!) = s$; `AbCl_unify`$(\{t = s\})$ returns solutions $\mathcal{E}_1, \ldots, \mathcal{E}_n$; and for every solved form equation $X = t' \in \mathcal{E}_i$, if $(\!|X|\!)^{inv} = \alpha$ and $(\!|t'|\!)^{inv} = \sigma'$, then $[\alpha \mapsto \sigma'] \in S_i$. By theorem 1, $Soln(\{t = s\}) = Soln(\mathcal{E}_1)|_{vars(\{t=s\})} \cup \ldots \cup Soln(\mathcal{E}_n)|_{vars(\{t=s\})}$. We then have that $\mathcal{E}_i$ is a solution for $\{t = s\}$. By definition 16, $(\!|t|\!)^{inv} = \sigma$ and $(\!|s|\!)^{inv} = \upsilon$. Therefore, S_i is a solution to $\sigma \doteq \upsilon$, or rather, $S_i(\sigma) = S_i(\upsilon)$. By definition 9, $S_i \models \sigma \doteq \upsilon$.

Lemma 4 (Completeness of Sequence Solving). *If $S_1 \models \sigma \doteq \upsilon$ then $\exists S, S_2$ s.t. $(\sigma \doteq \upsilon) \overset{s}{\Rightarrow} S_2$ and $S_1 = S \circ S_2$.*

Proof. If $S_1 \models \sigma \doteq \upsilon$, then by definition 16, (1) $(\!|\sigma|\!) = t$ and $(\!|\upsilon|\!) = s$. We then have that (2) `AbCl_unify`$(\{t = s\})$ returns solutions $\mathcal{E}_1, \ldots, \mathcal{E}_n$, with $i \in 1..n$. By theorem 1, we have that $Soln(\{t = s\}) = Soln(\mathcal{E}_1)|_{vars(\mathcal{E})} \cup \ldots \cup Soln(\mathcal{E}_n)|_{vars(\mathcal{E})}$. Therefore, the set of solved form equations of $\mathcal{E}_i$, for all $i \in 1..n$, represents all possible solutions of $\{t = s\}$, and each solution $\mathcal{E}_i$ is a minimal solution. (2a) For every solved form equation $X = t' \in \mathcal{E}_i$, if $(\!|X|\!)^{inv} = \alpha$ and $(\!|t'|\!)^{inv} = \sigma'$, then $[\alpha \mapsto \sigma'] \in S'_i$. By definition 17, since we have (1), (2), and (2a), then $(\sigma \doteq \upsilon) \overset{s}{\Rightarrow} S'_i$, non-deterministically for all $i \in 1..n$. One of these solutions S'_i agrees with S_1, and is a most general solution to $\sigma \doteq \upsilon$. Therefore, $\exists S, S'_i$ s.t. $S_1 = S \circ S'_i$.

4.3 Constraint Solving

We define the constraint solving rules in figure 2. Most rules are pretty straightforward, following standard formulations for type inference. Rule [S-Empty] allows the constraint solving to terminate: when no constraints are left, the algorithm can return the produced substitutions. Rule [S-Same] ignores equality constraints between the same types. Rule [S-Arrow] deconstructs an equality constraint between two arrows, by constraining both the domains to each other, and both the codomais to each other.

Rule [S-Seq] solves equality constraints between two sequences by calling the sequence solving algorithm $C \overset{s}{\Rightarrow} S'$, which in turn calls the solving algorithm `AbCl_unify` from [17,16]. Resulting substitutions are then applied to the remaining constraints, and solving proceeds as usual. Due to non-determinism of `AbCl_unify`, and consequently, $C \overset{s}{\Rightarrow} S'$, this rule introduces non-determinism in the constraint solving algorithm.

$$[\text{S-EMPTY}]\ \frac{}{\emptyset \Rightarrow \emptyset} \qquad [\text{S-SAME}]\ \frac{C^* \Rightarrow S}{\{\tau \doteq \tau\} \cup C^* \Rightarrow S}\ \tau \in \mathcal{T}_{base} \cup \mathcal{T}_{tvar}$$

$$[\text{S-ARROW}]\ \frac{\{\sigma \doteq \upsilon, \tau \doteq \rho\} \cup C^* \Rightarrow S}{\{\sigma \to \tau \doteq \upsilon \to \rho\} \cup C^* \Rightarrow S}$$

$$[\text{S-SEQ}]\ \frac{(\tau_1 \wedge \ldots \wedge \tau_n \doteq \rho_1 \wedge \ldots \wedge \rho_m) \overset{s}{\Rightarrow} S' \qquad S'(C^*) \Rightarrow S}{\{\tau_1 \wedge \ldots \wedge \tau_n \doteq \rho_1 \wedge \ldots \wedge \rho_m\} \cup C^* \Rightarrow S \circ S'}$$

$$[\text{S-TVARR}]\ \frac{\{\alpha \doteq \tau\} \cup C^* \Rightarrow S}{\{\tau \doteq \alpha\} \cup C^* \Rightarrow S}\ \tau \notin \mathcal{T}_{tvar}$$

$$[\text{S-TVARL}]\ \frac{[\alpha \mapsto \tau]C^* \Rightarrow S}{\{\alpha \doteq \tau\} \cup C^* \Rightarrow S \circ [\alpha \mapsto \tau]}\ \tau \in \mathcal{T}_0 \textit{ and } \alpha \notin tvars(\tau)$$

$$[\text{S-SVARR}]\ \frac{\{\phi \doteq \sigma\} \cup C^* \Rightarrow S}{\{\sigma \doteq \phi\} \cup C^* \Rightarrow S}\ \sigma \notin \mathcal{T}_{svar}$$

$$[\text{S-SVARL}]\ \frac{[\phi \mapsto \sigma]C^* \Rightarrow S}{\{\phi \doteq \sigma\} \cup C^* \Rightarrow S \circ [\phi \mapsto \sigma]}\ \sigma \in \mathcal{T}_1 \textit{ and } \phi \notin tvars(\sigma)$$

Fig. 3. Constraint Solving ($C^* \Rightarrow S$)

The remaining rules are standard rules to deal with type variables. Rules [S-TVarR] and [S-SVarR] apply when the type (and sequence) variables appear on the right side, swaping the positions of the constrained types. Rules [S-TVarL] and [S-SVarL] then produce a substitution between the type (and sequence) variable and the type on the right of the constraint.

We show our constraint solving algorithm is both sound and complete:

Lemma 5 (Soundness of Constraint Solving). *If $C^* \Rightarrow S$ then $S \models C^*$.*

Proof. Proof by induction on the length of the derivation tree of $C^* \Rightarrow S$.

Lemma 6 (Completeness of Constraint Solving). *If $S_1 \models C^*$ then $\exists S, S_2$ s.t. $C^* \Rightarrow S_2$ and $S_1 = S \circ S_2$.*

Proof. Proof by induction on the breakdown of constraint sets C^* by the solving rules.

4.4 Algorithm

Having defined both a generation and solving algorithm, we now include both in the main type inference algorithm. We also show our type inference is sound and complete.

Definition 18 (Type Inference). *The type inference procedure infer*$(M) \stackrel{def}{=} (\Gamma, \tau, S)$*, that given an expression* M*, non-deterministically returns a triple* (Γ, τ, S) *composed of a typing context* Γ*, type* τ *and substitutions* S*, is defined by the following steps:*

Let infer$(M) \stackrel{def}{=} (\Gamma, \tau, S)$*, such that:*

1. *let* Γ*,* τ *and* C^* *such that* $\Gamma \vdash_\wedge M : \tau \mid C^*$*;*
2. *let* S *such that* $C^* \Rightarrow S$*;*

Theorem 2 (Soundness). *If infer*$(M) = (\Gamma, \tau, S)$ *then* $S(\Gamma) \vdash_\wedge M : S(\tau)$*.*

Proof. By definition 18, we have Γ, τ and C^* such that $\Gamma \vdash_\wedge M : \tau \mid C^*$, and S such that $C^* \Rightarrow S$. By lemma 5, since $C^* \Rightarrow S$ then $S \models C^*$. By lemma 1, since $\Gamma \vdash_\wedge M : \tau \mid C^*$ and $S \models C^*$ then $S(\Gamma) \vdash_\wedge M : S(\tau)$.

Theorem 3 (Completeness). *If* $S_1(\Gamma) \vdash_\wedge M : \tau$ *then* $\exists S_2, \rho, S$ *s.t. infer*$(M) = (\Gamma, \rho, S_2)$ *and* $\tau = S \circ S_2(\rho)$*.*

Proof. If $S_1(\Gamma) \vdash_\wedge M : \tau$ then by lemma 2, $\Gamma \vdash_\wedge M : \rho \mid C^*$ and $\exists S_2$ s.t. S_2 agrees with S_1 except at χ, $S_2 \models C^*$ and $S_2(\rho) = \tau$, where χ are the fresh variables introduced in the derivation of $\Gamma \vdash_\wedge M : \rho \mid C^*$. By lemma 6, $\exists S, S_3$ s.t $C^* \Rightarrow S_3$ and $S_2 = S \circ S_3$. By definition 18, infer$(M) = (\Gamma, \rho, S_3)$. Then, we have that $\tau = S \circ S_3(\rho)$.

5 Conclusion and Future Work

In this paper we present a sound and complete unification-based type inference algorithm for rank-2 intersection types using set unification. One nice feature of this algorithm is its similarity with type inference for simple types, it is basically the same algorithm, replacing first-order unification by set unification.

5.1 Future Work

Using Set-Unification based Type Inference in Practice This work is carried out in the context of a larger research project, focused in the use of intersection types and gradual types for programming language design and implementation. This larger project assumes the implementation and evaluation of intersection gradual types in a functional programming language compiler. Several points need to be further developed to enable the use of the algorithm presented here in the overall project goals. Some important points to address are:

1. Extension of the term language with recursive definitions. This will enable to apply our algorithm to a more realistic language and will address the known problems related with decidability for recursive definitions [29,25].
2. Add support to let expressions and conditional expressions. Most likely, in the case of conditional expressions, this will mean extending the type language with union types.

Theoretical Issues The work presented here inspires the following possible future work:

1. Types here use associative, commutative and idempotent intersections. In the last years non-idempotent intersections have been successfully used to obtain quantitative information of program behaviour [7,1,2]. We believe it is rather promising to use multiset unification (usually based on solving diophantine equations) in the same way we use set unification, to infer types in this particular setting.
2. Investigate the complexity of our type inference algorithm. Being exponential for sure, because this is the complexity of the type inference problem for rank-2 intersection types, we want to study the exact complexity of our type inference algorithm and investigate if using set-unification may have some impact on the overall efficiency of type inference.
3. Extension to higher rank intersection types. Here we use a simple form of set unification where there cannot be sets inside sets. We conjecture that using those nested sets limited to a fixed level of nesting will result on type inference algorithms for higher (but finite) rank intersection types.
4. Study the relation of our approach with β-unification [30] and other forms of unification. Unification theory is a wide research field and studying in detail the relations between different unification algorithms, which, in this case, are used for the same purpose may shed some light on their relations and also contribute to the area of unification theory.

Acknowledgements This work was partially financially supported by the portuguese Fundação para a Ciência e a Tecnologia, under the PhD grant number SFRH/BD/145183/2019 and by Base Funding - UIDB/00027/2020 of the Artificial Intelligence and Computer Science Laboratory – LIACC - funded by national funds through the FCT/MCTES (PIDDAC).

References

1. Accattoli, B., Graham-Lengrand, S., Kesner, D.: Tight typings and split bounds. Proc. ACM Program. Lang. **2**(ICFP), 94:1–94:30 (2018)
2. Alves, S., Kesner, D., Ventura, D.: A quantitative understanding of pattern matching. In: 25th International Conference on Types for Proofs and Programs, TYPES 2019, June 11-14, 2019, Oslo, Norway. LIPIcs, vol. 175, pp. 3:1–3:36. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2019)
3. Ângelo, P., Florido, M.: Type inference for rank 2 gradual intersection types. In: Bowman, W.J., Garcia, R. (eds.) Trends in Functional Programming. pp. 84–120. Springer International Publishing, Cham (2020). https://doi.org/10.1007/978-3-030-47147-7_5
4. Barendregt, H.P., Dekkers, W., Statman, R.: Lambda Calculus with Types. Perspectives in logic, Cambridge University Press (2013)
5. Barendregt, H., Coppo, M., Dezani-Ciancaglini, M.: A filter lambda model and the completeness of type assignment. Journal of Symbolic Logic **48**(4), 931–940 (1983). https://doi.org/10.2307/2273659

6. Bettini, L., Bono, V., Dezani-Ciancaglini, M., Giannini, P., Venneri, B.: Java & lambda: a featherweight story. Log. Methods Comput. Sci. **14**(3) (2018)
7. Bucciarelli, A., Kesner, D., Ventura, D.: Non-idempotent intersection types for the Lambda-Calculus. Logic Journal of the IGPL **25**(4), 431–464 (07 2017). `https://doi.org/10.1093/jigpal/jzx018`
8. Castagna, G., Lanvin, V.: Gradual typing with union and intersection types. Proc. ACM Program. Lang. **1**(ICFP), 41:1–41:28 (Aug 2017). `https://doi.org/10.1145/3110285`
9. Castagna, G., Lanvin, V., Petrucciani, T., Siek, J.G.: Gradual typing: A new perspective. Proc. ACM Program. Lang. **3**(POPL), 16:1–16:32 (Jan 2019). `https://doi.org/10.1145/3290329`
10. Coppo, M., Dezani-Ciancaglini, M.: An extension of the basic functionality theory for the λ-calculus. Notre Dame Journal of Formal Logic **21**(4), 685–693 (10 1980). `https://doi.org/10.1305/ndjfl/1093883253`
11. Coppo, M.: An extended polymorphic type system for applicative languages. In: Dembiński, P. (ed.) Mathematical Foundations of Computer Science 1980. pp. 194–204. Springer Berlin Heidelberg, Berlin, Heidelberg (1980)
12. Curry, H.B.: Functionality in Combinatory Logic. Proceedings of the National Academy of Science **20**(11), 584–590 (Nov 1934). `https://doi.org/10.1073/pnas.20.11.584`
13. Damas, L., Milner, R.: Principal type-schemes for functional programs. In: Proceedings of the 9th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages. pp. 207–212. POPL '82, ACM, New York, NY, USA (1982). `https://doi.org/10.1145/582153.582176`
14. Damiani, F.: Rank 2 intersection types for modules. In: Proceedings of the 5th ACM SIGPLAN International Conference on Principles and Practice of Declaritive Programming. p. 67–78. PPDP '03, Association for Computing Machinery, New York, NY, USA (2003). `https://doi.org/10.1145/888251.888259`
15. Damiani, F., Giannini, P.: A decidable intersection type system based on relevance. In: Hagiya, M., Mitchell, J.C. (eds.) Theoretical Aspects of Computer Software. pp. 707–725. Springer Berlin Heidelberg, Berlin, Heidelberg (1994)
16. Dovier, A., Omodeo, E., Pontelli, E., Rossi, G.: A language for programming in logic with finite sets. J. Log. Program. **28**, 1–44 (01 1996)
17. Dovier, A., Pontelli, E., Rossi, G.: Set unification. Theory and Practice of Logic Programming **6**(6), 645–701 (2006). `https://doi.org/10.1017/S1471068406002730`
18. Dunfield, J.: Elaborating intersection and union types. In: Proceedings of the 17th ACM SIGPLAN International Conference on Functional Programming. p. 17–28. ICFP '12, Association for Computing Machinery, New York, NY, USA (2012). `https://doi.org/10.1145/2364527.2364534`, `https://doi.org/10.1145/2364527.2364534`
19. Dunfield, J., Pfenning, F.: Type assignment for intersections and unions in call-by-value languages. In: Gordon, A.D. (ed.) Foundations of Software Science and Computation Structures. pp. 250–266. Springer Berlin Heidelberg, Berlin, Heidelberg (2003)
20. Florido, M., Damas, L.: Linearization of the lambda-calculus and its relation with intersection type systems. Journal of Functional Programming **14**(5), 519–546 (2004). `https://doi.org/10.1017/S0956796803004970`
21. Frankle, J., Osera, P.M., Walker, D., Zdancewic, S.: Example-directed synthesis: A type-theoretic interpretation. In: Proceedings of the 43rd Annual ACM

SIGPLAN-SIGACT Symposium on Principles of Programming Languages. p. 802–815. POPL '16, Association for Computing Machinery, New York, NY, USA (2016). https://doi.org/10.1145/2837614.2837629, https://doi.org/10.1145/2837614.2837629
22. Freeman, T., Pfenning, F.: Refinement types for ml. In: Proceedings of the ACM SIGPLAN 1991 Conference on Programming Language Design and Implementation. p. 268–277. PLDI '91, Association for Computing Machinery, New York, NY, USA (1991). https://doi.org/10.1145/113445.113468
23. Girard, J.Y.: Une extension de L'interpretation de gödel a L'analyse, et son application a L'elimination des coupures dans L'analyse et la theorie des types. In: Fenstad, J. (ed.) Proceedings of the Second Scandinavian Logic Symposium, Studies in Logic and the Foundations of Mathematics, vol. 63, pp. 63–92. Elsevier (1971). https://doi.org/https://doi.org/10.1016/S0049-237X(08)70843-7, https://www.sciencedirect.com/science/article/pii/S0049237X08708437
24. Girard, J.Y., Taylor, P., Lafont, Y.: Proofs and Types. Cambridge University Press, Cambridge (1989)
25. Henglein, F.: Type inference with polymorphic recursion. ACM Trans. Program. Lang. Syst. **15**(2), 253–289 (1993). https://doi.org/10.1145/169701.169692, https://doi.org/10.1145/169701.169692
26. Hindley, J.R.: Basic Simple Type Theory. Cambridge University Press (1997)
27. Jim, T.: Rank 2 type systems and recursive definitions. Tech. rep., Cambridge, MA, USA (1995)
28. Jim, T.: What are principal typings and what are they good for? In: Proceedings of the 23rd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages. pp. 42–53. POPL '96, ACM, New York, NY, USA (1996). https://doi.org/10.1145/237721.237728
29. Kfoury, A.J., Tiuryn, J., Urzyczyn, P.: Type reconstruction in the presence of polymorphic recursion. ACM Trans. Program. Lang. Syst. **15**(2), 290–311 (1993)
30. Kfoury, A.J., Wells, J.B.: Principality and decidable type inference for finite-rank intersection types. In: Proceedings of the 26th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages. pp. 161–174. POPL '99, ACM, New York, NY, USA (1999). https://doi.org/10.1145/292540.292556
31. Leivant, D.: Polymorphic type inference. In: Proceedings of the 10th ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages. p. 88–98. POPL '83, Association for Computing Machinery, New York, NY, USA (1983). https://doi.org/10.1145/567067.567077
32. PALSBERG, J., PAVLOPOULOU, C.: From polyvariant flow information to intersection and union types. Journal of Functional Programming **11**(3), 263–317 (2001). https://doi.org/10.1017/S095679680100394X
33. Pierce, B.C.: Types and Programming Languages. The MIT Press, 1st edn. (2002)
34. Pottinger, G.: A type assignment for the strongly normalizable lambda-terms. In: Hindley, J., Seldin, J. (eds.) To H. B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism, pp. 561–577. Academic Press (1980)
35. Reynolds, J.C.: Towards a theory of type structure. In: Programming Symposium, Proceedings Colloque Sur La Programmation. p. 408–423. Springer-Verlag, Berlin, Heidelberg (1974)
36. Reynolds, J.C.: Design of the Programming Language Forsythe, pp. 173–233. Birkhäuser Boston, Boston, MA (1997). https://doi.org/10.1007/978-1-4612-4118-8_9
37. Robinson, J.A.: A machine-oriented logic based on the resolution principle. J. ACM **12**(1), 23–41 (Jan 1965). https://doi.org/10.1145/321250.321253

38. Urzyczyn, P.: The emptiness problem for intersection types. In: Proceedings Ninth Annual IEEE Symposium on Logic in Computer Science. pp. 300–309 (1994). https://doi.org/10.1109/LICS.1994.316059
39. Van Bakel, S.J.: Intersection type disciplines in lambda calculus and applicative term rewriting systems. Amsterdam: Mathematisch Centrum (1993)
40. Wand, M.: A simple algorithm and proof for type inference. Fundamenta Informaticae **10**(2), 115–121 (1987)

A Proofs

In this section, we present the full proofs for all the stated properties:

- Lemma 1 (Soundness of Constraint Generation) in A;
- Lemma 2 (Completeness of Constraint Generation) in A;
- Lemma 5 (Soundness of Constraint Solving) in A;
- Lemma 6 (Completeness of Constraint Solving) in A;

Lemma 1 (Soundness of Constraint Generation). *If $\Gamma \vdash_\wedge M : \tau \mid C^*$ and $S \models C^*$ then $S(\Gamma) \vdash_\wedge M : S(\tau)$.*

Proof. We proceed by induction on the length of the derivation tree of $\Gamma \vdash_\wedge M : \tau \mid C^*$.

Base case:

- Rule [G-Con]. If $\emptyset \vdash_\wedge k : B \mid \emptyset$ and $S \models \emptyset$, then k is a constant of base type B. Then, by rule [T-Con], $\emptyset \vdash_\wedge k : B$ holds. By definition 7, we have that $S(\emptyset) = \emptyset$ and $S(B) = B$. Therefore, $S(\emptyset) \vdash_\wedge k : S(B)$ holds.
- Rule [G-Var]. If $x : \alpha \vdash_\wedge x : \alpha \mid \emptyset$ and $S \models \emptyset$, then α is a fresh type variable. By definition 7, $S(\alpha) = \tau$ for any τ. By rule [T-Var], $x : \tau \vdash_\wedge x : \tau$. By definition 11, $x : S(\alpha) = S(x : \alpha)$. Therefore, $S(x : \alpha) \vdash_\wedge x : S(\alpha)$.

Induction step:

- Rule [G-AbsI]. If $\Gamma \vdash_\wedge \lambda x\ .\ M : \sigma \to \tau \mid C^*$ and $S \models C^*$ then by rule [G-AbsI], $\Gamma, x : \sigma \vdash_\wedge M : \tau \mid C^*$. By the induction hypothesis, $S(\Gamma, x : \sigma) \vdash_\wedge M : S(\tau)$. By definition 11, $S(\Gamma, x : \sigma) = S(\Gamma), x : S(\sigma)$, therefore $S(\Gamma), x : S(\sigma) \vdash_\wedge M : S(\tau)$. By rule [T-AbsI], $S(\Gamma) \vdash_\wedge \lambda x\ .\ M : S(\sigma) \to S(\tau)$, or rather, $S(\Gamma) \vdash_\wedge \lambda x\ .\ M : S(\sigma \to \tau)$.
- Rule [G-AbsK]. Assuming $x \notin fvars(M)$, if $\Gamma \vdash_\wedge \lambda x\ .\ M : \phi \to \tau \mid C^*$ and $S \models C^*$ then by rule [G-AbsK], $\Gamma \vdash_\wedge M : \tau \mid C^*$ and ϕ is a fresh sequence variable. By the induction hypothesis, $S(\Gamma) \vdash_\wedge M : S(\tau)$. By definition 7, $S(\phi) = \sigma$ for any σ. By rule [T-AbsK], $S(\Gamma) \vdash_\wedge \lambda x\ .\ M : \sigma \to S(\tau)$ holds, which means $S(\Gamma) \vdash_\wedge \lambda x\ .\ M : S(\phi \to \tau)$ also holds.
- Rule [G-App$\wedge$]. If $\Gamma_1 \wedge \Gamma_{21} \wedge \ldots \wedge \Gamma_{2n} \vdash_\wedge M\ N : \tau \mid C_1^* \cup C_{21}^* \cup \ldots \cup C_{2n}^* \cup C$ and $S \models C_1^* \cup C_{21}^* \cup \ldots \cup C_{2n}^* \cup C$ then by rule [G-App$\wedge$], $\Gamma_1 \vdash_\wedge M : \tau_1 \wedge \ldots \wedge \tau_n \to \tau \mid C_1^*$, $\Gamma_2 \vdash_\wedge N : \rho \mid C_2^*$ and $duplicate^n(\langle \Gamma_2, \rho, C_2^* \rangle) = \langle [\Gamma_{21}, \ldots, \Gamma_{2n}], [\rho_1, \ldots, \rho_n], [C_{21}^*, \ldots, C_{2n}^*] \rangle$, and by definition 9, $S \models C_1^*$, $S \models C_{21}^*$ and $\ldots$ and $S \models C_{2n}^*$ and $S \models \tau_1 \wedge \ldots \wedge \tau_n \doteq \rho_1 \wedge \ldots \wedge \rho_n$.

  By the induction hypothesis, $S(\Gamma_1) \vdash_\wedge M : S(\tau_1 \wedge \ldots \wedge \tau_n \to \tau)$. As we have that $\Gamma_2 \vdash_\wedge N : \rho \mid C_2^*$, we also have $\Gamma_{21} \vdash_\wedge N : \rho_1 \mid C_{21}^*$ and $\ldots$ and $\Gamma_{2n} \vdash_\wedge N : \rho_n \mid C_{2n}^*$, which are just renamings of variables. By the induction hypothesis, $S(\Gamma_{21}) \vdash_\wedge N : S(\rho_1)$ and $\ldots$ and $S(\Gamma_{2n}) \vdash_\wedge N : S(\rho_n)$. By definition 9, $S(\tau_1 \wedge \ldots \wedge \tau_n) = S(\rho_1 \wedge \ldots \wedge \rho_n)$. Therefore, $S(\Gamma_1) \vdash_\wedge M : S(\rho_1 \wedge \ldots \wedge \rho_n) \to S(\tau)$. By rule [T-App], $S(\Gamma_1) \wedge S(\Gamma_{21}) \wedge \ldots \wedge S(\Gamma_{2n}) \vdash_\wedge M\ N : S(\tau)$, or rather, $S(\Gamma_1 \wedge \Gamma_{21} \wedge \ldots \wedge \Gamma_{2n}) \vdash_\wedge M\ N : S(\tau)$.

– Rule [G-App]. If $\Gamma_1 \wedge \Gamma_2 \vdash_\wedge M\ N : \alpha \mid C_1^* \cup C_2^* \cup \{\tau \doteq \phi \to \alpha, \phi \doteq \rho\}$ and $S \models C_1^* \cup C_2^* \cup \{\tau \doteq \phi \to \alpha, \phi \doteq \rho\}$ then by rule [G-App], $\Gamma_1 \vdash_\wedge M : \tau \mid C_1^*$ and $\Gamma_2 \vdash_\wedge N : \rho \mid C_2^*$ and α and ϕ are fresh type (and sequence) variables, and by definition 9, $S \models C_1^*$, $S \models \cup C_2^*$, $S \models \tau \doteq \phi \to \alpha$ and $S \models \phi \doteq \rho$. By the induction hypothesis, $S(\Gamma_1) \vdash_\wedge M : S(\tau)$ and $S(\Gamma_2) \vdash_\wedge N : S(\rho)$. By definition 9, $S(\tau) = S(\phi \to \alpha)$ and $S(\phi) = S(\rho)$. Therefore, we have that $S(\Gamma_1) \vdash_\wedge M : S(\rho \to \alpha)$, or rather, $S(\Gamma_1) \vdash_\wedge M : S(\rho) \to S(\alpha)$. By rule [T-App], $S(\Gamma_1) \wedge S(\Gamma_2) \vdash_\wedge M\ N : S(\alpha)$. By definitions 6 and 7, we have that $S(\Gamma_1 \wedge \Gamma_2) \vdash_\wedge M\ N : S(\alpha)$ holds.
– Rule [G-Add]. If $\Gamma_1 \wedge \Gamma_2 \vdash_\wedge M + N : \mathit{Int} \mid C_1^* \cup \{\tau \doteq \mathit{Int}\} \cup C_2^* \cup \{\rho \doteq \mathit{Int}\}$ and $S \models C_1^* \cup \{\tau \doteq \mathit{Int}\} \cup C_2^* \cup \{\rho \doteq \mathit{Int}\}$, then by rule [G-Add], $\Gamma_1 \vdash_\wedge M : \tau \mid C_1^*$ and $\Gamma_2 \vdash_\wedge N : \rho \mid C_2^*$, and by definition 9, $S \models C_1^*$, $S \models \tau \doteq \mathit{Int}$, $S \models C_2^*$ and $S \models \rho \doteq \mathit{Int}$. By the induction hypothesis, $S(\Gamma_1) \vdash_\wedge M : S(\tau)$ and $S(\Gamma_2) \vdash_\wedge N : S(\rho)$. By definition 9, $S(\tau) = \mathit{Int}$ and $S(\rho) = \mathit{Int}$. Therefore, $S(\Gamma_1) \vdash_\wedge M : \mathit{Int}$ and $S(\Gamma_2) \vdash_\wedge N : \mathit{Int}$. By rule [T-Add], $S(\Gamma_1) \wedge S(\Gamma_2) \vdash_\wedge M + N : \mathit{Int}$. By definitions 6 and 7, we have that $S(\Gamma_1 \wedge \Gamma_2) \vdash_\wedge M + N : S(\mathit{Int})$ holds.

Lemma 2 (Completeness of Constraint Generation). *If $S_1(\Gamma) \vdash_\wedge M : \tau$ then $\Gamma \vdash_\wedge M : \rho \mid C^*$ s.t. the domain of S_1 is disjoint from χ, and $\exists S_2$ s.t. S_2 agrees with S_1 except at χ, $S_2 \models C^*$ and $S_2(\rho) = \tau$, where χ are the fresh variables introduced in the derivation of $\Gamma \vdash_\wedge M : \rho \mid C^*$.*

Proof. We proceed by induction on the length of the derivation tree of $S_1(\Gamma) \vdash_\wedge M : \tau$.

Base case:

– Rule [T-Con]. If $S_1(\emptyset) \vdash_\wedge k : B$ then by rule [T-Con], k is a constant of base type B. By rule [G-Con], $\emptyset \vdash_\wedge k : B \mid \emptyset$. We have that $S_1 \models \emptyset$, by definition 9, and that $S_1(B) = B$, by definition 7.
– Rule [T-Var]. If $S_1(x : \rho) \vdash_\wedge x : \tau$ then by definition 7, $S_1(\rho) = \tau$. By rule [G-Var], $x : \alpha \vdash_\wedge x : \alpha \mid \emptyset$. For a $S_2 = S_1 \circ [\alpha \mapsto \tau]$, then S_2 agrees with S_1 except at $\{\alpha\}$. By definition 9, $S_2 \models \emptyset$. By definition 7, $S_2(\alpha) = \tau$.

Induction step:

– Rule [T-AbsI]. If $S_1(\Gamma) \vdash_\wedge \lambda x\ .\ M : S_1(\sigma) \to \tau$ then by rule [T-AbsI], $S_1(\Gamma, x : \sigma) \vdash_\wedge M : \tau$. By the induction hypothesis, $\Gamma, x : \sigma \vdash_\wedge M : \rho \mid C^*$ s.t. the domain of S_1 is disjoint from χ, and $\exists S_2$ s.t. S_2 agrees with S_1 except at χ, $S_2 \models C^*$ and $S_2(\rho) = \tau$. By rule [G-AbsI], $\Gamma \vdash_\wedge \lambda x\ .\ M : \sigma \to \rho \mid C^*$. Since S_2 agrees with S_1 except at χ, then $S_2(\sigma) = S_1(\sigma)$. Therefore, by definition 7, $S_2(\sigma \to \rho) = S_1(\sigma) \to \tau$.
– Rule [T-AbsK]. If $S_1(\Gamma) \vdash_\wedge \lambda x\ .\ M : \sigma \to \tau$ then by rule [T-AbsK], $S_1(\Gamma) \vdash_\wedge M : \tau$. By the induction hypothesis, $\Gamma \vdash_\wedge M : \rho \mid C^*$ s.t. the domain of S_1 is disjoint from χ, and $\exists S_2$ s.t. S_2 agrees with S_1 except at χ, $S_2 \models C^*$ and $S_2(\rho) = \tau$. By rule [G-AbsK], $\Gamma \vdash_\wedge \lambda x\ .\ M : \phi \to \rho \mid C^*$. For an $S_3 = S_2 \circ [\phi \mapsto \sigma]$, then S_3 agrees with S_2 except at χ, where $\phi \in \chi$. By definition 9, $S_3 \models C^*$. By definition 7, $S_3(\phi \to \rho) = \sigma \to \tau$.

– Rule [T-APP]. If $S(\Gamma_0 \wedge \Gamma_1 \wedge \ldots \wedge \Gamma_n) \vdash_\wedge M\ N : \tau$ then by rule [T-APP], $S(\Gamma_0) \vdash_\wedge M : \tau_1 \wedge \ldots \wedge \tau_n \to \tau$ and $\forall i \in 1..n$. $S(\Gamma_i) \vdash_\wedge N : \tau_i$. By the induction hypothesis, $\Gamma_0 \vdash_\wedge M : \tau'' \mid C_0^*$ s.t. the domain of S is disjoint from χ_0 and $\exists S_0$ s.t. S_0 agrees with S except at χ_0, $S_0 \models C_0^*$ and $S_0(\tau'') = \tau_1 \wedge \ldots \wedge \tau_n \to \tau$. There are two possibilities:
  - $\tau'' = \tau_1' \wedge \ldots \wedge \tau_n' \to \tau'$. Therefore, $\Gamma_0 \vdash_\wedge M : \tau_1' \wedge \ldots \wedge \tau_n' \to \tau' \mid C_0^*$. By the induction hypothesis, $\forall i \in 1..n$, $\Gamma_i \vdash_\wedge N : \rho_i \mid C_i^*$ s.t. the domain of S is disjoint from χ_i and $\exists S_i$ s.t. S_i agrees with S except at χ_i, $S_i \models C_i^*$ and $S_i(\rho_i) = \tau_i$.

    We also have that $\forall i \in 1..n$, the derivations $\Gamma_i \vdash_\wedge N : \rho_i \mid C_i^*$ are just type variables renamings of each other. We can have an extra derivation $\Gamma' \vdash_\wedge N : \rho' \mid C'^*$ which is also just a type variable renaming of the previous. With a proper choice of variables, we have that $\mathit{duplicate}^n(\langle \Gamma', \rho', C'^* \rangle) = \langle [\Gamma_1, \ldots, \Gamma_n], [\rho_1, \ldots, \rho_n], [C_1^*, \ldots, C_n^*] \rangle$.

    We must now introduce a substitution S' such that: (1) S' agrees with S except at $\chi_0 \cup \chi_1 \cup \ldots \cup \chi_n$, (2) $S' \models C_0^* \cup C_1^* \cup \ldots \cup C_n^* \cup \{\tau_1' \wedge \ldots \wedge \tau_n' \doteq \rho_1 \wedge \ldots \wedge \rho_n\}$ and (3) $S'(\tau') = \tau$. We define S' as follows:
    * $[\alpha \mapsto \tau_0] \in S'$ if $\alpha \notin \chi_0 \cup \chi_1 \cup \ldots \cup \chi_n$ and $[\alpha \mapsto \tau_0] \in S$;
    * $[\phi \mapsto \sigma_0] \in S'$ if $\phi \notin \chi_0 \cup \chi_1 \cup \ldots \cup \chi_n$ and $[\phi \mapsto \sigma_0] \in S$;
    * $\forall i \in 0..n$, then $[\alpha_i \mapsto \rho_i'] \in S'$ if $\alpha_i \in \chi_i$ and $[\alpha_i \mapsto \rho_i'] \in S_i$;
    * $\forall i \in 0..n$, then $[\phi_i \mapsto \sigma_i] \in S'$ if $\phi_i \in \chi_i$ and $[\phi_i \mapsto \sigma_i] \in S_i$;
    * a substitution S'' such that $S'' \models \tau_1' \wedge \ldots \wedge \tau_n' \doteq \rho_1 \wedge \ldots \wedge \rho_n$.

    Is it easy to check that conditions (1) hold. $S' \models C_0^* \cup C_1^* \cup \ldots \cup C_n^*$ because $\chi_0, \chi_1, \ldots, \chi_n$ are all disjoint from each other. Since $S'' \models \tau_1' \wedge \ldots \wedge \tau_n' \doteq \rho_1 \wedge \ldots \wedge \rho_n$, then also $S' \models \tau_1' \wedge \ldots \wedge \tau_n' \doteq \rho_1 \wedge \ldots \wedge \rho_n$. Therefore, condition (2) holds. Note that the domain of S_i is disjoint from χ_j, with $i \neq j$. Therefore, $S'(\tau_1' \wedge \ldots \wedge \tau_n' \to \tau') = S_0(\tau_1' \wedge \ldots \wedge \tau_n' \to \tau') = \tau_1 \wedge \ldots \wedge \tau_n \to \tau$. Therefore, $S'(\tau') = \tau$ and condition (3) holds. By rule [G-APP$\wedge$], $\Gamma_0 \wedge \Gamma_1 \wedge \ldots \wedge \Gamma_n \vdash_\wedge M\ N : \tau' \mid C_0^* \cup C_1^* \cup \ldots \cup C_n^* \cup \{\tau_1' \wedge \ldots \wedge \tau_n' \doteq \rho_1 \wedge \ldots \wedge \rho_n\}$ and S' fulfills the conditions.
  - τ'' is not an arrow type. Therefore $\Gamma_0 \vdash_\wedge M : \tau'' \mid C_0^*$. Also, according to definition 7, $S_0(\tau'') = \tau_1 \to \tau$, and then we have the single premise $S(\Gamma_1) \vdash_\wedge N : \tau_1$. By the induction hypothesis, $\Gamma_1 \vdash_\wedge N : \rho_1 \mid C_1^*$ s.t. the domain of S is disjoint from χ_1 and $\exists S_1$ s.t. S_1 agrees with S except at χ_1, $S_1 \models C_1^*$ and $S_1(\rho_1) = \tau_1$. We also have that χ_0 is disjoint from χ_1.

    We must now introduce a substitution S' such that: (1) S' agrees with S except at $\chi_0 \cup \chi_1 \cup \{\alpha\}$, (2) $S' \models C_0^* \cup C_1^* \cup \{\tau'' \doteq \rho_1 \to \alpha\}$ and (3) $S'(\alpha) = \tau$. We define S' as follows:
    * $[\alpha_0 \mapsto \tau_0] \in S'$ if $\alpha_0 \notin \chi_0 \cup \chi_1 \cup \alpha$ and $[\alpha_0 \mapsto \tau_0] \in S$;
    * $[\phi_0 \mapsto \sigma_0] \in S'$ if $\phi_0 \notin \chi_0 \cup \chi_1$ and $[\phi_0 \mapsto \sigma_0] \in S$;
    * $[\alpha_0 \mapsto \tau_0] \in S'$ if $\alpha_0 \in \chi_0 \cup \alpha$ and $[\alpha_0 \mapsto \tau_0] \in S_0$;
    * $[\phi_0 \mapsto \sigma_0] \in S'$ if $\phi_0 \in \chi_0$ and $[\phi_0 \mapsto \sigma_0] \in S_0$;

  * $[\alpha_0 \mapsto \tau_0] \in S'$ if $\alpha_0 \in \chi_1 \cup \alpha$ and $[\alpha_0 \mapsto \tau_0] \in S_1$;
  * $[\phi_0 \mapsto \sigma_0] \in S'$ if $\phi_0 \in \chi_1$ and $[\phi_0 \mapsto \sigma_0] \in S_1$;
  * $[\alpha \mapsto \tau] \in S'$;

  Is it easy to check that condition (1) and (3) hold. $S' \models C_0^* \cup C_1^*$ because χ_0 and χ_1 are disjoint. First note that the domain of S_0 is disjoint from χ_1, and the domain of S_1 is disjoint from χ_0. Therefore, $S'(\tau'') = S_0(\tau'') = \tau_1 \to \tau = S_1(\rho_1) \to S'(\alpha) = S'(\rho_1) \to S'(\alpha) = S'(\rho_1 \to \alpha)$. Therefore, $S' \models \{\tau'' \doteq \rho_1 \to \alpha\}$ and so (2) holds. By rule [G-App], $\Gamma_0 \wedge \Gamma_1 \vdash_\wedge M\ N : \alpha \mid C_0^* \cup C_1^* \cup \{\tau'' \doteq \rho_1 \to \alpha\}$ and S' fulfills the conditions.

– Rule [T-Add]. If $S(\Gamma_1 \wedge \Gamma_2) \vdash_\wedge M + N : \mathit{Int}$ then by rule [T-Add], $S(\Gamma_1) \vdash_\wedge M : \mathit{Int}$ and $S(\Gamma_2) \vdash_\wedge N : \mathit{Int}$. By the induction hypothesis, $\Gamma_1 \vdash_\wedge M : \tau \mid C_1^*$ s.t. the domain of S is disjoint from χ_1, and $\exists S_1$ s.t. S_1 agrees with S except at χ_1, $S_1 \models C_1^*$ and $S_1(\tau) = \mathit{Int}$; and $\Gamma_2 \vdash_\wedge M : \rho \mid C_2^*$ s.t. the domain of S is disjoint from χ_2, and $\exists S_2$ s.t. S_2 agrees with S except at χ_2, $S_2 \models C_2^*$ and $S_2(\rho) = \mathit{Int}$; and χ_1 is disjoint from χ_2.

  We must now introduce a substitution S' such that: (1) S' agrees with S except at $\chi_1 \cup \chi_2$, (2) $S' \models C_1^* \cup \{\tau \doteq \mathit{Int}\} \cup C_2^* \cup \{\rho \doteq \mathit{Int}\}$ and (3) $S'(\mathit{Int}) = \mathit{Int}$. We define S' as follows:
  - $[\alpha \mapsto \tau_0] \in S'$ if $\alpha \notin \chi_1 \cup \chi_2$ and $[\alpha \mapsto \tau_0] \in S$;
  - $[\phi \mapsto \sigma_0] \in S'$ if $\phi \notin \chi_1 \cup \chi_2$ and $[\phi \mapsto \sigma_0] \in S$;
  - $[\alpha_1 \mapsto \tau'] \in S'$ if $\alpha_1 \in \chi_1$ and $[\alpha_1 \mapsto \tau'] \in S_1$;
  - $[\phi_1 \mapsto \sigma_1] \in S'$ if $\phi_1 \in \chi_1$ and $[\phi_1 \mapsto \sigma_1] \in S_1$;
  - $[\alpha_2 \mapsto \rho'] \in S'$ if $\alpha_2 \in \chi_2$ and $[\alpha_2 \mapsto \rho'] \in S_2$;
  - $[\phi_2 \mapsto \sigma_2] \in S'$ if $\phi_2 \in \chi_2$ and $[\phi_2 \mapsto \sigma_2] \in S_2$.

  Is it easy to check that conditions (1) and (3) hold. $S' \models C_1^* \cup C_2^*$ because χ_1 and χ_2 are disjoint. First note that the domain of S_1 is disjoint from χ_2, and the domain of S_2 is disjoint from χ_1. Therefore, $S'(\tau) = S_1(\tau) = \mathit{Int}$ and $S'(\rho) = S_2(\rho) = \mathit{Int}$, and $S' \models \{\tau \doteq \mathit{Int}, \rho \doteq \mathit{Int}\}$. We have that (2) holds. By rule [G-Add], $\Gamma_1 \wedge \Gamma_2 \vdash_\wedge M + N : \mathit{Int} \mid C_1^* \cup \{\tau \doteq \mathit{Int}\} \cup C_2^* \cup \{\rho \doteq \mathit{Int}\}$ and S' fulfills the conditions.

Lemma 5 (Soundness of Constraint Solving). *If $C^* \Rightarrow S$ then $S \models C^*$.*

Proof. We proceed by induction on the length of the derivation tree of $C^* \Rightarrow S$.

Base case:

– Rule [S-Empty]. By definition 9, $\emptyset \models \emptyset$ holds.

Induction step:

– Rule [S-Same]. Assuming $\tau \in \mathcal{T}_{base} \cup \mathcal{T}_{tvar}$, if $\{\tau \doteq \tau\} \cup C^* \Rightarrow S$, then by rule [S-Same], $C^* \Rightarrow S$. By the induction hypothesis, $S \models C^*$. By definition 7, we have that $S(\tau) = S(\tau)$, so by definition 9, we have that $S \models \tau \doteq \tau$. Therefore, $S \models \{\tau \doteq \tau\} \cup C^*$.

– Rule [S-Arrow]. If $\{\sigma \to \tau \doteq \upsilon \to \rho\} \cup C^* \Rightarrow S$ then by rule [S-Arrow], $\{\sigma \doteq \upsilon, \tau \doteq \rho\} \cup C^* \Rightarrow S$. By the induction hypothesis, $S \models \{\sigma \doteq \upsilon, \tau \doteq \rho\} \cup C^*$. By definition 9, $S(\sigma) = S(\upsilon)$, $S(\tau) = S(\rho)$ and $S \models C^*$. By definition 7, $S(\sigma) \to S(\tau) = S(\upsilon) \to S(\rho)$, or rather, $S(\sigma \to \tau) = S(\upsilon \to \rho)$. Therefore, $S \models \{\sigma \to \tau \doteq \upsilon \to \rho\} \cup C^*$.
– Rule [S-Seq]. If $\{\tau_1 \wedge \ldots \wedge \tau_n \doteq \rho_1 \wedge \ldots \wedge \rho_m\} \cup C^* \Rightarrow S \circ S'$ then by rule [S-Seq], $(\tau_1 \wedge \ldots \wedge \tau_n \doteq \rho_1 \wedge \ldots \wedge \rho_m) \overset{s}{\Rightarrow} S'$ and $S'(C^*) \Rightarrow S$. By lemma 3, $S' \models \tau_1 \wedge \ldots \wedge \tau_n \doteq \rho_1 \wedge \ldots \wedge \rho_m$, and thus, by definition 9, $S'(\tau_1 \wedge \ldots \wedge \tau_n) = S'(\rho_1 \wedge \ldots \wedge \rho_m)$. By definition 7, $S \circ S'(\tau_1 \wedge \ldots \wedge \tau_n) = S \circ S'(\rho_1 \wedge \ldots \wedge \rho_m)$. Therefore, by definition 9, $S \circ S' \models \tau_1 \wedge \ldots \wedge \tau_n \doteq \rho_1 \wedge \ldots \wedge \rho_m$.

  By the induction hypothesis, $S \models S'(C^*)$. By definition 9, $S \circ S' \models C^*$. Therefore, by definition 9, $S \circ S' \models \{\tau_1 \wedge \ldots \wedge \tau_n \doteq \rho_1 \wedge \ldots \wedge \rho_m\} \cup C^*$.
– Rule [S-TVarR]. Assuming $\tau \notin \mathcal{T}_{tvar}$, if $\{\tau \doteq \alpha\} \cup C^* \Rightarrow S$ then by rule [S-TVarR], $\{\alpha \doteq \tau\} \cup C^* \Rightarrow S$. By the induction hypothesis, $S \models \{\alpha \doteq \tau\} \cup C^*$. By definition 9, $S(\alpha) = S(\tau)$, or rather, $S(\tau) = S(\alpha)$. By definition 9, $S \models \{\tau \doteq \alpha\} \cup C^*$.
– Rule [S-TVarL]. Assuming $\tau \in \mathcal{T}_0$ and $\alpha \notin tvars(\tau)$, if $\{\alpha \doteq \tau\} \cup C^* \Rightarrow S \circ [\alpha \mapsto \tau]$ then by rule [S-TVarL], $[\alpha \mapsto \tau]C^* \Rightarrow S$. By the induction hypothesis, $S \models [\alpha \mapsto \tau]C^*$.

  We show that if $S \models [\alpha \mapsto \tau]C^*$ then $S \circ [\alpha \mapsto \tau] \models C^*$. We proceed by showing that, for all $C \in C^*$, if $S \models [\alpha \mapsto \tau]C$ then $S \circ [\alpha \mapsto \tau] \models C$. There is only one possibility:
  • $C = \sigma \doteq \upsilon$. We have that $S \models [\alpha \mapsto \tau](\sigma \doteq \upsilon)$. By definition 11, $[\alpha \mapsto \tau](\sigma \doteq \upsilon) = ([\alpha \mapsto \tau]\sigma) \doteq ([\alpha \mapsto \tau]\upsilon)$. Therefore, $S \models ([\alpha \mapsto \tau]\sigma) \doteq ([\alpha \mapsto \tau]\upsilon)$. By definition 9, $S([\alpha \mapsto \tau]\sigma) = S([\alpha \mapsto \tau]\upsilon)$, or rather, $S \circ [\alpha \mapsto \tau](\sigma) = S \circ [\alpha \mapsto \tau](\upsilon)$. By definition 9, $S \circ [\alpha \mapsto \tau] \models \sigma \doteq \upsilon$.

  By definition 7, $S \circ [\alpha \mapsto \tau](\alpha) = S \circ [\alpha \mapsto \tau](\tau)$. Therefore, by definition 9, $S \circ [\alpha \mapsto \tau] \models \{\alpha \doteq \tau\}$. By definition 9, $S \circ [\alpha \mapsto \tau] \models \{\alpha \doteq \tau\} \cup C^*$.
– Rule [S-SVarR]. Assuming $\sigma \notin \mathcal{T}_{svar}$, if $\{\sigma \doteq \phi\} \cup C^* \Rightarrow S$ then by rule [S-SVarR], $\{\phi \doteq \sigma\} \cup C^* \Rightarrow S$. By the induction hypothesis, $S \models \{\phi \doteq \sigma\} \cup C^*$. By definition 9, $S(\phi) = S(\sigma)$, or rather, $S(\sigma) = S(\phi)$. By definition 9, $S \models \{\sigma \doteq \phi\} \cup C^*$.
– Rule [S-SVarL]. Assuming $\sigma \in \mathcal{T}_1$ and $\phi \notin tvars(\sigma)$, if $\{\phi \doteq \sigma\} \cup C^* \Rightarrow S \circ [\phi \mapsto \sigma]$ then by rule [S-SVarL], $[\phi \mapsto \sigma]C^* \Rightarrow S$. By the induction hypothesis, $S \models [\phi \mapsto \sigma]C^*$.

  We show that if $S \models [\phi \mapsto \sigma]C^*$ then $S \circ [\phi \mapsto \sigma] \models C^*$. We proceed by showing that, for all $C \in C^*$, if $S \models [\phi \mapsto \sigma]C$ then $S \circ [\phi \mapsto \sigma] \models C$. There is only one possibility:
  • $C = \upsilon_1 \doteq \upsilon_2$. We have that $S \models [\phi \mapsto \sigma](\upsilon_1 \doteq \upsilon_2)$. By definition 11, $[\phi \mapsto \sigma](\upsilon_1 \doteq \upsilon_2) = ([\phi \mapsto \sigma]\upsilon_1) \doteq ([\phi \mapsto \sigma]\upsilon_2)$. Therefore, $S \models ([\phi \mapsto \sigma]\upsilon_1) \doteq ([\phi \mapsto \sigma]\upsilon_2)$. By definition 9, $S([\phi \mapsto \sigma]\upsilon_1) = S([\phi \mapsto \sigma]\upsilon_2)$, or rather, $S \circ [\phi \mapsto \sigma](\upsilon_1) = S \circ [\phi \mapsto \sigma](\upsilon_2)$. By definition

9, $S \circ [\phi \mapsto \sigma] \models \upsilon_1 \doteq \upsilon_2$.

By definition 7, $S \circ [\phi \mapsto \sigma](\phi) = S \circ [\phi \mapsto \sigma](\sigma)$. Therefore, by definition 9, $S \circ [\phi \mapsto \sigma] \models \{\phi \doteq \sigma\}$. By definition 9, $S \circ [\phi \mapsto \sigma] \models \{\phi \doteq \sigma\} \cup C^*$.

Lemma 6 (Completeness of Constraint Solving). *If $S_1 \models C^*$ then $\exists S, S_2$ s.t. $C^* \Rightarrow S_2$ and $S_1 = S \circ S_2$.*

Proof. We proceed by induction on the breakdown of constraint sets C^* by the solving rules.

Base case:

- Rule for $\emptyset \Rightarrow \emptyset$. If $S_1 \models \emptyset$ then by rule [S-Empty], $\emptyset \Rightarrow \emptyset$. For an $S = S_1$, then $S_1 = S \circ \emptyset$.

Induction step:

- Rule for $\{\tau \doteq \tau\} \cup C^* \Rightarrow S$. If $S_1 \models \{\tau \doteq \tau\} \cup C^*$, then by definition 9, $S_1 \models \tau \doteq \tau$ and $S_1 \models C^*$. By the induction hypothesis, $\exists S, S_2$ s.t. $C^* \Rightarrow S_2$ and $S_1 = S \circ S_2$. By rule [S-Same], $\{\tau \doteq \tau\} \cup C^* \Rightarrow S_2$.
- Rule for $\{\sigma \rightarrow \tau \doteq \upsilon \rightarrow \rho\} \cup C^* \Rightarrow S$. If $S_1 \models \{\sigma \rightarrow \tau \doteq \upsilon \rightarrow \rho\} \cup C^*$, then by definition 9, $S_1(\sigma \rightarrow \tau) = S_1(\upsilon \rightarrow \rho)$, or rather, $S_1(\sigma) = S_1(\upsilon)$ and $S_1(\tau) = S_1(\rho)$. By definition 9, $S_1 \models \{\sigma \doteq \upsilon, \tau \doteq \rho\} \cup C^*$. By the induction hypothesis, $\exists S, S_2$ s.t. $\{\sigma \doteq \upsilon, \tau \doteq \rho\} \cup C^* \Rightarrow S_2$ and $S_1 = S \circ S_2$. By rule [S-Arrow], $\{\sigma \rightarrow \tau \doteq \upsilon \rightarrow \rho\} \cup C^* \Rightarrow S_2$.
- Rule for $\{\tau_1 \wedge \ldots \wedge \tau_n \doteq \rho_1 \wedge \ldots \wedge \rho_m\} \cup C^* \Rightarrow S \circ S'$. If $S_1 \models \{\tau_1 \wedge \ldots \wedge \tau_n \doteq \rho_1 \wedge \ldots \wedge \rho_m\} \cup C^*$ then $S_1 \models \tau_1 \wedge \ldots \wedge \tau_n \doteq \rho_1 \wedge \ldots \wedge \rho_m$ and $S_1 \models C^*$. By lemma 4, $\exists S, S_2$ s.t. $(\tau_1 \wedge \ldots \wedge \tau_n \doteq \rho_1 \wedge \ldots \wedge \rho_m) \stackrel{s}{\Rightarrow} S_2$ and $S_1 = S \circ S_2$. Therefore, $S \circ S_2 \models C^*$, and by definition 9, $S \models S_2(C^*)$. By the induction hypothesis, $\exists S', S_3$ s.t. $S_2(C^*) \Rightarrow S_3$ and $S = S' \circ S_3$. By rule [S-Seq], $\{\tau_1 \wedge \ldots \wedge \tau_n \doteq \rho_1 \wedge \ldots \wedge \rho_m\} \cup C^* \Rightarrow S_3 \circ S_2$. Since $S_1 = S \circ S_2$ and $S = S' \circ S_3$ then $S_1 = S' \circ S_3 \circ S_2$.
- Rule for $\{\tau \doteq \alpha\} \cup C^* \Rightarrow S$. If $S_1 \models \{\tau \doteq \alpha\} \cup C^*$, then by definition 9, $S_1(\tau) = S_1(\alpha)$, or rather $S_1(\alpha) = S_1(\tau)$. By definition 9, $S_1 \models \{\alpha \doteq \tau\} \cup C^*$. By the induction hypothesis, $\exists S, S_2$ s.t. $\{\alpha \doteq \tau\} \cup C^* \Rightarrow S_2$ and $S_1 = S \circ S_2$. By rule [S-TVarR], $\{\tau \doteq \alpha\} \cup C^* \Rightarrow S_2$.
- Rule for $\{\alpha \doteq \tau\} \cup C^* \Rightarrow S \circ [\alpha \mapsto \tau]$. If $S_1 \models \{\alpha \doteq \sigma\} \cup C^*$ then by definition 9, $S_1(\alpha) = S_1(\sigma)$ and $S_1 \models C^*$. Therefore, for each constraint $\sigma_1 \doteq \sigma_2 \in C^*$, $S_1 \circ [\alpha \mapsto \sigma](\sigma_1) = S_1 \circ [\alpha \mapsto \sigma](\sigma_2)$, which by definition 7, is the same as $S_1([\alpha \mapsto \sigma]\sigma_1) = S_1([\alpha \mapsto \sigma]\sigma_2)$. By definition 9, $S_1 \models [\alpha \mapsto \sigma]\sigma_1 \doteq [\alpha \mapsto \sigma]\sigma_2$, and by definition 11, $S_1 \models [\alpha \mapsto \sigma](\sigma_1 \doteq \sigma_2)$. By definition 9, $S_1 \models [\alpha \mapsto \sigma]C^*$. By the induction hypothesis, $\exists S, S_2$ s.t. $[\alpha \mapsto \sigma]C^* \Rightarrow S_2$ and $S_1 = S \circ S_2$. By rule [S-TVarL], $\{\alpha \doteq \sigma\} \cup C^* \Rightarrow S_2 \circ [\alpha \mapsto \sigma]$. Since $S_1(\alpha) = S_1(\sigma)$, then $S_1 = S \circ S_2 \circ [\alpha \mapsto \sigma]$.
- Rule for $\{\sigma \doteq \phi\} \cup C^* \Rightarrow S$. If $S_1 \models \{\sigma \doteq \phi\} \cup C^*$, then by definition 9, $S_1(\sigma) = S_1(\phi)$, or rather $S_1(\phi) = S_1(\sigma)$. By definition 9, $S_1 \models \{\phi \doteq \sigma\} \cup C^*$. By the induction hypothesis, $\exists S, S_2$ s.t. $\{\phi \doteq \sigma\} \cup C^* \Rightarrow S_2$ and $S_1 = S \circ S_2$. By rule [S-TVarR], $\{\sigma \doteq \phi\} \cup C^* \Rightarrow S_2$.

– Rule for $\{\phi \doteq \sigma\} \cup C^* \Rightarrow S \circ [\phi \mapsto \sigma]$. If $S_1 \models \{\phi \doteq \sigma\} \cup C^*$ then by definition 9, $S_1(\phi) = S_1(\sigma)$ and $S_1 \models C^*$. Therefore, for each constraint $\sigma_1 \doteq \sigma_2 \in C^*$, $S_1 \circ [\phi \mapsto \sigma](\sigma_1) = S_1 \circ [\phi \mapsto \sigma](\sigma_2)$, which by definition 7, is the same as $S_1([\phi \mapsto \sigma]\sigma_1) = S_1([\phi \mapsto \sigma]\sigma_2)$. By definition 9, $S_1 \models [\phi \mapsto \sigma]\sigma_1 \doteq [\phi \mapsto \sigma]\sigma_2$, and by definition 11, $S_1 \models [\phi \mapsto \sigma](\sigma_1 \doteq \sigma_2)$. By definition 9, $S_1 \models [\phi \mapsto \sigma]C^*$. By the induction hypothesis, $\exists S, S_2$ s.t. $[\phi \mapsto \sigma]C^* \Rightarrow S_2$ and $S_1 = S \circ S_2$. By rule [S-SVarL], $\{\phi \doteq \sigma\} \cup C^* \Rightarrow S_2 \circ [\phi \mapsto \sigma]$. Since $S_1(\phi) = S_1(\sigma)$, then $S_1 = S \circ S_2 \circ [\phi \mapsto \sigma]$.