Decidable, Tag-Based Semantic Subtyping for Nominal Types, Tuples, and Unions

Julia Belyakova
Northeastern University
belyakova.y@northeastern.edu

Abstract

Subtyping is utilized by many programming languages for static type checking and dynamic dispatch. *Semantic* subtyping enables simple, set-theoretical reasoning about types by interpreting a type as a set of its values. Previously, semantic subtyping has been studied primarily in the context of statically typed languages with structural typing. In this paper, we explore the applicability of semantic subtyping in the context of *dynamic* languages with *nominal* types. Instead of static type checking, such languages rely on run-time checking of type tags associated with values, so we propose using the tags for semantic interpretation. Namely, we present *tag-based semantic* subtyping for nominal types, tuples, and unions, where types are interpreted set-theoretically, as sets of type tags (instead of values). The proposed subtyping relation is shown to be decidable, and a corresponding syntax-directed definition is provided. The implications of using semantic subtyping for multiple dispatch in a dynamic language are also discussed.

Keywords semantic subtyping, type tags, multiple dynamic dispatch, nominal typing, distributivity, decidability

1 Introduction

Subtyping is utilized by many static type systems. Informally, a subtyping relation `T <: S` states that a value of type `T` can be safely used in the context that expects a value of type `S`. For example, if class `Rectangle` is a subtype of class `Shape`, then a function with an argument of type `Shape` can be called with an instance of `Rectangle`.

Subtyping can also be used for run-time dispatch of function calls, in particular, *multiple dynamic dispatch* (MDD) [4, 5]. It allows a function to have several implementations for different types of arguments, and the most suitable implementation for a particular call is picked dynamically, based on the run-time types of all arguments. For example, consider two implementations of addition, `+(Number, Number)` and `+(String, String)`, and the call `3+5`. In this case, a language run-time should pick the implementation for numbers because `Int <: Number` but `Int` $\not<:$ `String`.

It is often convenient to think of subtyping `T <: S` in terms of the set inclusion: "the elements of `T` are a subset of the elements of `S`" [13]. This intuition is not always correct, but, in the case of *semantic subtyping* [1, 7, 8], subtyping is defined exactly as the subset relation. Namely, types are interpreted as sets $[\![\tau]\!] = \{v \mid \vdash v : \tau\}$, and subtyping $\tau_1 <: \tau_2$ is defined as inclusion of the interpretations $[\![\tau_1]\!] \subseteq [\![\tau_2]\!]$.

While the semantic definition of subtyping intertwines with a static typing relation, subtyping is applicable in the context of *dynamically* typed languages. As mentioned before, subtyping can be used for multiple dynamic dispatch, and MDD is rather widespread among dynamic languages such as CLOS, Julia, Clojure. Unlike statically typed languages, which conservatively prevent type errors with static checking, dynamic languages detect type errors at run-time. Namely, whenever an operator is restricted to certain kinds of values, the language run-time checks the arguments of the operator before running it; often, such a check amounts to checking the *type tag* associated with the value argument.

A large number of dynamic languages provide support for object-oriented programming with classes, thus enabling user-defined hierarchies of nominal types. Nominal types are the main source of type tags: any class that can be instantiated induces a tag (the name of the class) that is used to tag all the instances. Abstract classes and interfaces, on the other hand, do not have instances, so do not induce tags.

In this paper, we are bridging the gap between *semantic* subtyping and *dynamically* typed languages with *nominal* types. Instead of directly interpreting types as sets of values, we interpret them as sets of *type tags* assuming each value is associated with a tag. Our contributions are as follows:

1. Tag-based semantic interpretation of types for a language with nominal types, tuples, and unions (Sec. 2).
2. Two syntactic definitions of subtyping, declarative and reductive, along with the Coq-mechanized proofs that the definitions are equivalent and coincide with the semantic interpretation (Sec. 3).
3. Proof of decidability of the reductive subtyping.
4. Discussion of the implications of using semantic subtyping for multiple dynamic dispatch (Sec. 5).

2 Semantic Subtyping in MiniJl

We base this work on a small language of types MiniJl, presented in Fig. 1. Types, denoted by $\tau \in$ Type, include pairs, unions, and nominal types: *cname* denotes *concrete* nominal types that can be instantiated, and *aname* denotes *abstract* nominal types.

FTfJP'19, July 15–19, 2019, London, United Kingdom
2019.

$$
\begin{array}{rcll}
\tau \in \textsc{Type} & ::= & & \textit{Types} \\
& | & \tau_1 \times \tau_2 & \text{covariant pair} \\
& | & \tau_1 \cup \tau_2 & \text{untagged union} \\
& | & \textit{cname} & \text{concrete nominal type} \\
& | & \textit{aname} & \text{abstract nominal type}
\end{array}
$$

$$
\begin{array}{rcl}
\textit{cname} & \in & \{\mathsf{Int}, \mathsf{Flt}, \mathsf{Cmplx}, \mathsf{Str}\} \\
\textit{aname} & \in & \{\mathsf{Real}, \mathsf{Num}\}
\end{array}
$$

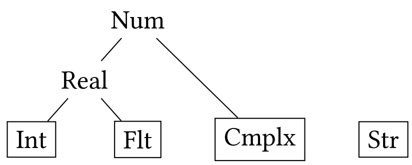

Figure 1. MiniJl: type grammar and nominal hierarchy

$$
\begin{array}{rcll}
v \in \textsc{ValType} & ::= & & \textit{Value Types} \\
& | & \textit{cname} & \text{concrete nominal type} \\
& | & v_1 \times v_2 & \text{pair of value types}
\end{array}
$$

Figure 2. Value types

To simplify the development, we work with a particular hierarchy of nominal types (presented in Fig. 1 as a tree) instead of a generic class table. There are four concrete, leaf types (depicted in rectangles) and two abstract types in the hierarchy. Formally, the hierarchy can be represented with a list of declarations $n_1 \rhd n_2$ read as "n_1 is a declared subtype of n_2" where n is either *cname* or *aname*. In the case of MiniJl, the hierarchy is defined as follows:

$$\mathsf{NomHrc} = [\mathsf{Real} \rhd \mathsf{Num}, \mathsf{Int} \rhd \mathsf{Real}, \mathsf{Flt} \rhd \mathsf{Real}, \mathsf{Cmplx} \rhd \mathsf{Num}].$$

Nominal hierarchies should not have cycles, and each type can have only one parent.

Value Types Only types that can be instantiated induce type tags, and we call these types **value types**. Their formal definition is given in Fig. 2: value type $v \in \textsc{ValType}$ is either a concrete nominal type or a pair of value types. For example, Flt, $\mathsf{Int} \times \mathsf{Int}$, and $\mathsf{Str} \times (\mathsf{Int} \times \mathsf{Int})$ are all value types. Union types, just as abstract nominal types, are not value types. Even the type $\mathsf{Int} \cup \mathsf{Int}$ is not a value type, though it describes the same set of values as the value type Int. Note that each value type is a type.

2.1 Semantic Interpretation of Types

As mentioned in Sec. 1, we interpret types as sets of type tags (i.e. value types) instead of values, so we call this semantic interpretation *tag-based*. Formally, the interpretation is given by the function $[\![\cdot]\!]$ that maps a type $\tau \in \textsc{Type}$ into a set of value types $s \in \mathcal{P}(\textsc{ValType})$, as presented in Fig. 3.

$$
\begin{array}{rcl}
[\![\cdot]\!] : \textsc{Type} & \longrightarrow & \mathcal{P}(\textsc{ValType}) \\
{[\![\textit{cname}]\!]} & = & \{\textit{cname}\} \\
{[\![\mathsf{Real}]\!]} & = & \{\mathsf{Int}, \mathsf{Flt}\} \\
{[\![\mathsf{Num}]\!]} & = & \{\mathsf{Int}, \mathsf{Flt}, \mathsf{Cmplx}\} \\
{[\![\tau_1 \times \tau_2]\!]} & = & \{v_1 \times v_2 \mid v_1 \in [\![\tau_1]\!], v_2 \in [\![\tau_2]\!]\} \\
{[\![\tau_1 \cup \tau_2]\!]} & = & [\![\tau_1]\!] \cup [\![\tau_2]\!]
\end{array}
$$

Figure 3. Tag-based semantic interpretation of types

The interpretation of a type states what values constitute the type: $v \in [\![\tau]\!]$ means that values v tagged with v (i.e. instances of v) belong to τ. Thus, in MiniJl, a *concrete nominal* type *cname* is comprised only of its direct instances.[1] *Abstract nominal* types cannot be instantiated, but we want their interpretation to reflect the nominal hierarchy: for example, a Num value is either a concrete complex or a real number, which, in turn, is either a concrete integer or a floating point value. Therefore, the set of values of type Num is described by the set of value types $\{\mathsf{Cmplx}, \mathsf{Int}, \mathsf{Flt}\}$. More generally, the interpretation of an abstract nominal type *aname* can be given as follows:

$$[\![\textit{aname}]\!] = \{\textit{cname} \mid \textit{cname} \rhd^* \textit{aname}\},$$

where the relation $n_1 \rhd^* n_2$ means that n_1 is transitively a declared subtype of n_2:

$$\frac{n_1 \rhd n_2 \in \mathsf{NomHrc}}{n_1 \rhd^* n_2} \qquad \frac{n_1 \rhd^* n_2 \qquad n_2 \rhd^* n_3}{n_1 \rhd^* n_3}.$$

Finally, *pairs* and *unions* are interpreted set-theoretically.

Once we have the tag interpretation of types, we define **tag-based semantic subtyping** in a usual manner, as the subset relation:

$$\tau_1 \overset{\text{sem}}{<:} \tau_2 \quad \overset{\text{def}}{\equiv} \quad [\![\tau_1]\!] \subseteq [\![\tau_2]\!]. \tag{1}$$

3 Syntactic Definitions of Subtyping

While the semantic approach does enable intuitive reasoning about subtyping, we also need to be able to build the subtyping algorithm to compute subtypes. However, the semantic definition of subtyping (1) cannot be directly computed because of the quantification $\forall v$. Therefore, we provide a *syntactic* definition, equivalent to the semantic one, which is straightforward to implement.

We do this in two steps. First, we give an inductive definition, called *declarative*, that is handy to reason about; we prove it equivalent to the semantic definition. Second, we provide a *reductive*, syntax-directed definition of subtyping and prove it equivalent to the declarative one (and, hence, the semantic definition as well). We prove that the reductive subtyping is decidable, i.e. for any two types τ_1 and τ_2, it is possible to prove that either τ_1 is a subtype of τ_2, or it

[1] In the general case, the interpretation of a concrete nominal type would include itself and all its concrete subtypes.

is not. The proofs are mechanized in Coq, and since Coq logic is constructive, the decidability proof essentially gives a subtyping algorithm. However, it is also possible to devise an algorithm as a straightforward recursive function.

3.1 Declarative Subtyping

The declarative definition of subtyping is provided in Fig. 4. The definition is mostly comprised of the standard rules of syntactic subtyping for unions and pairs: namely, reflexivity and transitivity (SD-Refl and SD-Trans), subtyping of pairs (SD-Pairs), and subtyping of unions (SD-UnionL, SD-UnionR1, SD-UnionR2). Though SD-UnionR* rules are seemingly very strict (they require the left-hand side type to be syntactically equivalent to a part of the right-hand side type), transitivity allows us to derive judgments such as $\mathsf{Int} \leq (\mathsf{Str} \cup \mathsf{Real})$ via $\mathsf{Int} \leq \mathsf{Real}$ and $\mathsf{Real} \leq \mathsf{Str} \cup \mathsf{Real}$. Note that we do need the syntactic definition of subtyping to be *reflexive* and *transitive* because so is the subset relation, which is used to define semantic subtyping.

Semantic subtyping also forces us to add rules for distributing pairs over unions, SD-Distr1 and SD-Distr2. For example, consider two types, $(\mathsf{Str} \times \mathsf{Int}) \cup (\mathsf{Str} \times \mathsf{Flt})$ and $\mathsf{Str} \times (\mathsf{Int} \cup \mathsf{Flt})$. They have the same semantic interpretation — $\{\mathsf{Str}{\times}\mathsf{Int}, \mathsf{Str}{\times}\mathsf{Flt}\}$ — so they are equivalent. Therefore, we should also be able to derive their equivalence using the declarative definition, i.e. declarative subtyping should hold in both directions. One direction is trivial:

$$\dfrac{\dfrac{\mathsf{Str} \leq \mathsf{Str} \qquad \mathsf{Int} \leq \mathsf{Int} \cup \mathsf{Flt}}{\mathsf{Str} \times \mathsf{Int} \leq \mathsf{Str} \times (\mathsf{Int} \cup \mathsf{Flt})} \qquad \dfrac{\ldots}{\mathsf{Str} \times \mathsf{Flt} \leq \ldots}}{(\mathsf{Str} \times \mathsf{Int}) \cup (\mathsf{Str} \times \mathsf{Flt}) \leq \mathsf{Str} \times (\mathsf{Int} \cup \mathsf{Flt})}\;.$$

But the other direction,

$$\mathsf{Str} \times (\mathsf{Int} \cup \mathsf{Flt}) \leq (\mathsf{Str} \times \mathsf{Int}) \cup (\mathsf{Str} \times \mathsf{Flt}),$$

cannot be derived without SD-Distr2 rule.

The novel part of the definition resides in subtyping of nominal types. There are four obvious rules coming directly from the nominal hierarchy, for instance, SD-RealNum mirrors the fact that $\mathsf{Real} \rhd \mathsf{Num} \in \mathsf{NomHrc}$. But the rules SD-RealUnion and SD-NumUnion (highlighted in Fig. 4) are new — they are dictated by semantic subtyping. Thus, SD-RealUnion allows us to prove the equivalence of types $\mathsf{Int} \cup \mathsf{Flt}$ and Real, which are both interpreted as $\{\mathsf{Int}, \mathsf{Flt}\}$.

3.2 Reductive Subtyping

The declarative definition is not syntax-directed. For one, it involves the SD-Trans rule, which requires "coming up" with a middle type τ_2. For instance, in order to show

$$\mathsf{Str} \times \mathsf{Real} \leq (\mathsf{Str} \times \mathsf{Int}) \cup (\mathsf{Str} \times \mathsf{Str}) \cup (\mathsf{Str} \times \mathsf{Flt}),$$

we need to apply transitivity several times, in particular, with the middle type $\mathsf{Str} \times (\mathsf{Int} \cup \mathsf{Flt})$.

$$\dfrac{}{\tau \leq \tau}\ \text{SD-Refl} \qquad \dfrac{\tau_1 \leq \tau_2 \qquad \tau_2 \leq \tau_3}{\tau_1 \leq \tau_3}\ \text{SD-Trans}$$

$$\dfrac{\text{SD-IntReal}}{\mathsf{Int} \leq \mathsf{Real}} \qquad \dfrac{\text{SD-FltReal}}{\mathsf{Flt} \leq \mathsf{Real}}$$

$$\dfrac{\text{SD-RealNum}}{\mathsf{Real} \leq \mathsf{Num}} \qquad \dfrac{\text{SD-CmplxNum}}{\mathsf{Cmplx} \leq \mathsf{Num}}$$

$$\dfrac{\text{SD-RealUnion}}{\mathsf{Real} \leq \mathsf{Int} \cup \mathsf{Flt}} \qquad \dfrac{\text{SD-NumUnion}}{\mathsf{Num} \leq \mathsf{Real} \cup \mathsf{Cmplx}}$$

$$\dfrac{\tau_1 \leq \tau_1' \qquad \tau_2 \leq \tau_2'}{\tau_1 \times \tau_2 \leq \tau_1' \times \tau_2'}\ \text{SD-Pair}$$

$$\dfrac{\tau_1 \leq \tau' \qquad \tau_2 \leq \tau'}{\tau_1 \cup \tau_2 \leq \tau'}\ \text{SD-UnionL}$$

$$\dfrac{\text{SD-UnionR1}}{\tau_1 \leq \tau_1 \cup \tau_2} \qquad \dfrac{\text{SD-UnionR2}}{\tau_2 \leq \tau_1 \cup \tau_2}$$

$$\dfrac{}{(\tau_{11} \cup \tau_{12}) \times \tau_2 \leq (\tau_{11} \times \tau_2) \cup (\tau_{12} \times \tau_2)}\ \text{SD-Distr1}$$

$$\dfrac{}{\tau_1 \times (\tau_{21} \cup \tau_{22}) \leq (\tau_1 \times \tau_{21}) \cup (\tau_1 \times \tau_{22})}\ \text{SD-Distr2}$$

Figure 4. Declarative subtyping for MiniJl

The syntax-directed reductive definition[2] of subtyping is presented in Fig. 5. Some of the inductive rules are similar to their declarative counterparts, e.g. subtyping of pairs (SR-Pair) and a union on the left (SR-UnionL). The differing rules are highlighted . The explicit reflexivity rule SR-BaseRefl now works only with concrete nominal types, which is enough for the definition to be reflexive. General transitivity is gone as well; instead, it gets incorporated into subtyping of nominal types (SR-IntNum, SR-FltNum) and a union on the right (SR-UnionR1, SR-UnionR2).

The last rule of the definition, SR-NF, is the most important. It rewrites type τ into *disjunctive normal form* $\mathrm{NF}(\tau)$ before using other subtyping rules. This covers all useful applications of transitivity and distributivity that are possible in the declarative definition. The normalization function is presented in Fig. 6 (the auxiliary function `un_prs` can be found in Fig. 9, App. A). It produces a type of the form $v_1 \cup v_2 \cup \ldots \cup v_n$ (note that union is associative) by replacing

[2]The definition is not deterministic, though. For example, there are two ways to derive $\mathsf{Str} \times (\mathsf{Int} \cup \mathsf{Flt}) \leq_{\mathrm{R}} \mathsf{Str} \times (\mathsf{Int} \cup \mathsf{Flt})$: either by immediately applying SR-Pair, or by first normalizing the left-hand side with SR-NF.

$$\frac{}{\mathit{cname} \ \leq_{\mathrm{R}} \ \mathit{cname}} \ \textsc{SR-BaseRefl}$$

$$\textsc{SR-IntReal}\ \frac{}{\mathsf{Int} \ \leq_{\mathrm{R}} \ \mathsf{Real}} \qquad \textsc{SR-FltReal}\ \frac{}{\mathsf{Flt} \ \leq_{\mathrm{R}} \ \mathsf{Real}}$$

$$\textsc{SR-CmplxNum}\ \frac{}{\mathsf{Cmplx} \ \leq_{\mathrm{R}} \ \mathsf{Num}} \qquad \textsc{SR-IntNum}\ \frac{}{\mathsf{Int} \ \leq_{\mathrm{R}} \ \mathsf{Num}} \qquad \textsc{SR-FltNum}\ \frac{}{\mathsf{Flt} \ \leq_{\mathrm{R}} \ \mathsf{Num}}$$

$$\frac{\tau_1 \ \leq_{\mathrm{R}} \ \tau_1' \qquad \tau_2 \ \leq_{\mathrm{R}} \ \tau_2'}{\tau_1 \times \tau_2 \ \leq_{\mathrm{R}} \ \tau_1' \times \tau_2'} \ \textsc{SR-Pair}$$

$$\frac{\tau_1 \ \leq_{\mathrm{R}} \ \tau' \qquad \tau_2 \ \leq_{\mathrm{R}} \ \tau'}{\tau_1 \cup \tau_2 \ \leq_{\mathrm{R}} \ \tau'} \ \textsc{SR-UnionL}$$

$$\textsc{SR-UnionR1}\ \frac{\tau \ \leq_{\mathrm{R}} \ \tau_1'}{\tau \ \leq_{\mathrm{R}} \ \tau_1' \cup \tau_2'} \qquad \textsc{SR-UnionR2}\ \frac{\tau \ \leq_{\mathrm{R}} \ \tau_2'}{\tau \ \leq_{\mathrm{R}} \ \tau_1' \cup \tau_2'}$$

$$\frac{\mathrm{NF}(\tau) \ \leq_{\mathrm{R}} \ \tau'}{\tau \ \leq_{\mathrm{R}} \ \tau'} \ \textsc{SR-NF}$$

Figure 5. Reductive subtyping for MiniJl

$$\begin{array}{rcl}
\mathrm{NF} : \textsc{Type} & \longrightarrow & \textsc{Type} \\
\mathrm{NF}(\mathit{cname}) & = & \mathit{cname} \\
\mathrm{NF}\ (\mathsf{Real}) & = & \mathsf{Int} \cup \mathsf{Flt} \\
\mathrm{NF}\ (\mathsf{Num}) & = & \mathsf{Int} \cup \mathsf{Flt} \cup \mathsf{Cmplx} \\
\mathrm{NF}(\tau_1 \times \tau_2) & = & \mathsf{un_prs}(\mathrm{NF}(\tau_1),\ \mathrm{NF}(\tau_2)) \\
\mathrm{NF}(\tau_1 \cup \tau_2) & = & \mathrm{NF}(\tau_1) \cup \mathrm{NF}(\tau_2)
\end{array}$$

Figure 6. Computing normal form of MiniJl types

an abstract nominal type with the union of all its concrete subtypes, and a pair of unions with the union of pairs of value types, for instance:

$$\mathrm{NF}(\mathsf{Str} \times (\mathsf{Int} \cup \mathsf{Flt})) = (\mathsf{Str} \times \mathsf{Int}) \cup (\mathsf{Str} \times \mathsf{Flt}).$$

As we show in Sec. **??**, a type and its normal form are equivalent in the declarative definition, which is essential for reductive subtyping being equivalent to declarative subtyping.

4 Properties of Subtyping Relations

4.1 Correctness of Declarative Subtyping

In order to show that the declarative definition of subtyping is equivalent to the semantic definition, we need to prove that the former is sound and complete with respect to the latter, that is:

$$\forall \tau_1, \tau_2.\ (\tau_1 \ \leq \ \tau_2 \iff \tau_1 \overset{\text{sem}}{<:} \tau_2). \tag{2}$$

We find that instead of directly working with the semantic subtyping relation $\tau_1 \overset{\text{sem}}{<:} \tau_2 \overset{\text{def}}{\equiv} [\![\tau_1]\!] \subseteq [\![\tau_2]\!]$ (1), it is more convenient to use the following (equivalent) relation:

$$\tau_1 \ <: \ \tau_2 \quad \overset{\text{def}}{\equiv} \quad \forall v.\ (v \prec \tau_1 \implies v \prec \tau_2). \tag{3}$$

$$\frac{}{\mathit{cname} \prec \mathit{cname}} \ \textsc{MT-CName}$$

$$\textsc{MT-IntReal}\ \frac{}{\mathsf{Int} \prec \mathsf{Real}} \qquad \textsc{MT-FltReal}\ \frac{}{\mathsf{Flt} \prec \mathsf{Real}}$$

$$\textsc{MT-IntNum}\ \frac{}{\mathsf{Int} \prec \mathsf{Num}} \qquad \textsc{MT-FltNum}\ \frac{}{\mathsf{Flt} \prec \mathsf{Num}} \qquad \textsc{MT-CmplxNum}\ \frac{}{\mathsf{Cmplx} \prec \mathsf{Num}}$$

$$\frac{v_1 \prec \tau_1 \qquad v_2 \prec \tau_2}{v_1 \times v_2 \prec \tau_1 \times \tau_2} \ \textsc{MT-Pair}$$

$$\frac{v \prec \tau_1}{v \prec \tau_1 \cup \tau_2} \ \textsc{MT-Union1} \qquad \frac{v \prec \tau_2}{v \prec \tau_1 \cup \tau_2} \ \textsc{MT-Union2}$$

Figure 7. Matching relation in MiniJl

The relation $v \prec \tau$ (defined in Fig. 7), read "tag v matches type τ", we call **matching relation**. It is easy to show by induction on τ that the matching relation is equivalent to the belongs-to relation $v \in [\![\tau]\!]$. And the latter relation is used in the definition of semantic subtyping (we replace set inclusion $X \subseteq Y$ with its definition $\forall x.\ (x \in X \implies x \in Y)$):

$$\tau_1 \overset{\text{sem}}{<:} \tau_2 \overset{\text{def}}{\equiv} \forall v.\ (v \in [\![\tau_1]\!] \implies v \in [\![\tau_2]\!]). \tag{4}$$

The definitions (4) and (3) are equivalent because the relations $v \in [\![\tau]\!]$ and $v \prec \tau$ are equivalent. Therefore, instead of proving (2), we are going to prove that declarative subtyping $\tau_1 \ \leq \ \tau_2$ is equivalent to semantic subtyping $\tau_1 \ <: \ \tau_2$.

Theorem 1 (Correctness of Declarative Subtyping)**.**

$$\forall \tau_1, \tau_2.\ (\tau_1 \ \leq \ \tau_2 \iff \tau_1 \ <: \ \tau_2)$$

In order to prove the theorem, we need several auxiliary observations. First of all, subtyping a value type coincides with matching:

$$\forall v, \tau.\ (v \ \leq \ \tau \iff v \prec \tau). \tag{5}$$

Having that, it is easy to prove the *soundness* direction of Theorem 1.

Lemma 1 (Soundness of Declarative Subtyping)**.**

$$\forall \tau_1, \tau_2.\ [\tau_1 \ \leq \ \tau_2 \implies \forall v.\ (v \prec \tau_1 \implies v \prec \tau_2)]$$

Proof. We know $v \prec \tau_1$ and $\tau_1 \leq \tau_2$. We need to show that $v \prec \tau_2$. First, we apply (5) to $v \prec \tau_1$ and $v \prec \tau_2$. Now it suffices to show that $v \leq \tau_2$ follows from $v \leq \tau_1$ and $\tau_1 \leq \tau_2$, which is trivially true by SD-Trans. □

Lemma 2 (Completeness of Declarative Subtyping)**.**

$$\forall \tau_1, \tau_2. \, (\tau_1 \ <: \ \tau_2 \implies \tau_1 \leq \tau_2)$$

This direction of Theorem 1 is more challenging. The key observation here is that Lemma 2 can be shown for τ_1 of the form $v_1 \cup v_2 \cup \ldots \cup v_n$ (we omit parenthesis because union is associative). In this case, in the definition of $\tau_1 <: \tau_2$ the only vs that match τ_1 and τ_2 are v_i. By (5) we know that matching implies subtyping, so we also have $v_i \leq \tau_2$. From the latter, it is easy to show that $\tau_1 \leq \tau_2$ because τ_1 is just a union of value types, and subtyping of the left-hand side union amounts to subtyping its components, according to the SD-UnionL rule.

Normal Form We say that a type $\tau \equiv v_1 \cup v_2 \cup \ldots \cup v_n$ is in **normal form** and denote this fact by InNF(τ) (formal definition of InNF is given in Fig. 8, App. A). For each type τ, there is an equivalent normalized type that can be computed with the function NF defined in Fig. 6 (the auxiliary function `un_prs` can be found in Fig. 9, App. A). Note that abstract nominal types are unfolded into unions of all their value subtypes. A pairs gets rewritten into a union of value pairs, thus producing a type in the disjunctive normal form.

Using the fact that every type can be normalized, and that declarative subtyping is complete for normalized types, we can finally prove Lemma 2.

Lemma 3 (Properties of the Normal Form)**.**

$$\forall \tau. \, (\mathrm{InNF}(\mathrm{NF}(\tau)) \ \wedge \ \tau \leq \mathrm{NF}(\tau) \ \wedge \ \mathrm{NF}(\tau) \leq \tau)$$

Lemma 4 (Completeness for Normalized Types)**.**

$$\forall \tau_1, \tau_2 \mid \mathrm{InNF}(\tau_1). \, (\tau_1 \ <: \ \tau_2 \implies \tau_1 \leq \tau_2)$$

Lemma 5. $\forall \tau_1, \tau_2. \, (\tau_1 \ <: \ \tau_2 \implies \mathrm{NF}(\tau_1) \ <: \ \tau_2)$

Proof (Lemma 2). We know $\tau_1 <: \tau_2$, and we need to show $\tau_1 \leq \tau_2$. First, we apply Lemma 5 to $\tau_1 <: \tau_2$, and then Lemma 4, this gives us $\mathrm{NF}(\tau_1) \leq \tau_2$. Using Lemma 3 and SD-Trans, we can show $\tau_1 \leq \tau_2$. □

4.2 Reductive Subtyping

Theorem 2 (Correctness of Reductive Subtyping)**.**

$$\forall \tau_1, \tau_2. \, (\tau_1 \leq_{\mathrm{R}} \tau_2 \iff \tau_1 \leq \tau_2)$$

It is relatively easy to show by induction on a derivation of $\tau_1 \leq_{\mathrm{R}} \tau_2$ that the reductive subtyping is sound: for each case we build a corresponding derivation of $\tau_1 \leq \tau_2$. Most of the reductive rules have direct declarative counterparts. In the case of SR-*Num and SR-UnionR*, we need to additionally use transitivity. Finally, in the case of SR-NF, the induction hypothesis gives us $\mathrm{NF}(\tau_1) \leq \tau_2$, so we can use Lemma 3 and SD-Trans to derive $\tau_1 \leq \tau_2$.

The challenging part of the proof is to show completeness. For this, we need to prove that the reductive definition is *reflexive*, *transitive*, and *distributive*. To prove transitivity and distributivity, we need several auxiliary statements:

1. $\tau \leq_{\mathrm{R}} \tau' \implies \mathrm{NF}(\tau) \leq_{\mathrm{R}} \tau'$,
2. $\mathrm{NF}(\tau_1) \leq_{\mathrm{R}} \mathrm{NF}(\tau_2) \ \wedge \ \mathrm{NF}(\tau_2) \leq_{\mathrm{R}} \tau_3 \implies \mathrm{NF}(\tau_1) \leq_{\mathrm{R}} \tau_3$,
3. $\mathrm{NF}(\tau) \leq_{\mathrm{R}} \mathrm{NF}(\tau') \implies \tau \leq_{\mathrm{R}} \tau'$.

Having all the facts, we can prove completeness by induction on a derivation of $\mathrm{NF}(\tau_1) \leq \tau_2$. For details, the reader can refer to the full Coq-proof.

Theorem 3 (Decidability of Reductive Subtyping)**.**

$$\forall \tau_1, \tau_2. \, (\tau_1 \leq_{\mathrm{R}} \tau_2 \quad \vee \quad \neg \tau_1 \leq_{\mathrm{R}} \tau_2)$$

The Coq-proof is available.

5 Semantic Subtyping and Multiple Dynamic Dispatch

In this section, we describe in more detail how subtyping can be used to implement multiple dynamic dispatch, and also discuss implications of using *semantic* subtyping.

As an example, consider the following methods[3] of the addition function (we assume that function `flt` converts its argument to a float):

```
+(x::Int, y::Int) = prim_add_int(x, y)
+(x::Flt, y::Flt) = prim_add_flt(x, y)
+(x::Int∪Flt, y::Int∪Flt) = prim_add_flt(flt(x), ..)
```

and the function call `3 + 5`. How exactly does dispatch work?

One approach, adopted by some languages such as Julia [2], is to use subtyping on tuples [10]. Namely, method signatures and function calls are interpreted as tuple types, and then subtyping is used to determine applicable methods as well as pick one of them. In the example above, the three methods are interpreted as the following types (from top to bottom):

```
mII ≡ Int × Int
mFF ≡ Flt × Flt
mUU ≡ (Int∪Flt) × (Int∪Flt)
```

and the call as having type `cII ≡ Int × Int`. To resolve the call, the language run-time ought to perform two steps.

1. Find applicable methods (if any). For this, we check subtyping between the type of the call, `cII`, and the method signatures. Since `cII <: mII` and `cII <: mUU` but `cII` $\not<:$ `mFF`, only two methods are applicable, `mII` for integers and `mUU` for mixed-type numbers.
2. Pick the most specific of the applicable methods (if there is one). For this, we check subtyping relations between all applicable methods. In this example, naturally, we would like `mII` to be called for the addition

[3]In the context of MDD, different implementations of the same function are usually called *methods*, and the set of all methods is called a *generic function*.

of integers. And indeed, since `mII <: mUU`, the integer addition is considered the most specific.

Let us also consider the call `3.14 + 5`. Its type is `Flt × Int`, and there is only one applicable method `mUU` that is a supertype of the call type, so it should be called.

It is important to understand what happens if the programmer defines several implementations with the same argument types. In the case of a static language, an error can be reported. In the case of a dynamic language, however, the second implementation simply replaces the earlier one, in the same way as reassignment to a variable replaces its previous value.

For instance, consider a program that contains the three implementations of `(+)` from above and also the following:

```
+(x::Real, y::Real) = ... # mRR
print(3.14 + 5)
```

According to the semantic subtyping relation, type `Real` is equivalent to `Int∪Flt` in MiniJl. Therefore, implementation of `mRR` will replace `mUU`, and the call `3.14 + 5` will be dispatched to `mRR`.

There is a problem with using semantic subtyping for MDD: the semantics of the program above is not stable. If the programmer adds a new type into the nominal hierarchy, e.g. `Int8 <: Real`, type `Real` is not equivalent to `Int∪Flt` anymore. Therefore, if the program is run again, types of `mUU` and `mRR` will be different, and so the implementation of `mRR` will not replace `mUU`. Since `mUU <: mRR`, the call `3.14 + 5` will be dispatched to `mUU`, not `mRR` as before.

We can gain stability by removing the rules that equate abstract nominal types with the union of their subtypes, i.e. SD-RealUnion and SD-NumUnion in the declarative definition.[4] To fix the discrepancy between this definition and the semantic interpretation, we can change the latter by accounting for "future nominal types", e.g. $[\![\mathsf{Real}]\!] = \{\mathsf{Int}, \mathsf{Flt}, X\}$. It needs to be understood whether such an interpretation provides us with a useful intuition about subtyping.

6 Related Work

Semantic subtyping has been studied primarily in the context of *statically typed* languages with *structural* typing. For example, Hosoya and Pierce [8] defined a semantic type system for XML that incorporated unions, products, and recursive types, with a subtyping algorithm based on tree automata [9]. Frisch et al. [7] presented decidable semantic subtyping for a language with functions, products, and boolean combinators (union, intersection, negation); the decision procedure for $\tau_1 <: \tau_2$ is based on checking the emptiness of $\tau_1 \setminus \tau_2$. Dardha et al. [6] adopted semantic subtyping to objects with structural types, and Ancona and Corradi [1] proposed decidable semantic subtyping for mutable records. Unlike these works, we are interested in applying semantic reasoning to a *dynamic* language with *nominal* types.

Though *multiple dispatch* is more often found in dynamic languages, there has been research on safe integration of dynamic dispatch into statically typed languages [3–5, 12]. There, subtyping is used for both static type checking and dynamic method resolution. In the realm of dynamic languages, Bezanson [2] employed subtyping for multiple dynamic dispatch in the Julia language. Julia has a rich language of type annotations (including, but not limited to nominal types, tuples, and unions) and a complex subtyping relation [14]. However, it is not clear whether the subtyping relation is decidable or even transitive, and transitivity of subtyping is important for correct implementation of method resolution. In this paper, while we work with only a subset of Julia types, subtyping is transitive and decidable.

Recently, a framework for building transitive, distributive, and decidable subtyping of union and intersection types was proposed by Muehlboeck and Tate [11]. Our language of types does not have intersection types but features pair types that distribute over unions in a similar fashion.

7 Conclusion and Future Work

We have presented decidable subtyping of nominal types, tuples, and unions, that has the advantages of semantic subtyping, such as simple set-theoretic reasoning, yet can be used in the context of dynamically typed languages. Namely, we interpret types in terms of type tags, which are typical for dynamic languages, and provide a decidable syntactic subtyping relation that is equivalent to the subset relation on the interpretations (aka tag-based semantic subtyping).

We found that the proposed subtyping relation, if used for multiple dynamic dispatch, would make the semantics of dynamically typed programs unstable due to an interaction of abstract nominal types and unions. We expect that a different semantic interpretation of nominal types can fix the issue, and would like to further explore the alternative.

In future work, we plan to extend tag-based semantic subtyping to invariant type constructors, e.g. `Ref`:

$$\begin{array}{rcl} \tau \in \textsc{Type} & ::= & \ldots \mid \mathsf{Ref}[\tau] \\ v \in \textsc{ValType} & ::= & \ldots \mid \mathsf{Ref}[\tau] \end{array}$$

As usual for invariant constructors, we would like to consider types such as $\mathsf{Ref}[\mathsf{Int}]$ and $\mathsf{Ref}[\mathsf{Int} \cup \mathsf{Int}]$ to be equivalent because Int and $\mathsf{Int} \cup \mathsf{Int}$ are equivalent. However, a naive interpretation of invariant types below is not well defined:

$$[\![\mathsf{Ref}[\tau]]\!] = \{\mathsf{Ref}[\tau'] \mid v \in [\![\tau]\!] \iff v \in [\![\tau']\!]\}.$$

Our plan is to introduce an indexed interpretation,

$$[\![\mathsf{Ref}[\tau]]\!]_{k+1} = \{\mathsf{Ref}[\tau'] \mid v \in [\![\tau]\!]_k \iff v \in [\![\tau']\!]_k\},$$

and define semantic subtyping as:

$$\tau_1 \overset{\text{sem}}{<:} \tau_2 \quad \overset{\text{def}}{\equiv} \quad \forall k.\ ([\![\tau_1]\!]_k \subseteq [\![\tau_2]\!]_k).$$

[4] To get an equivalent reductive subtyping, we need to change the SR-NF rule: replace normalization function NF with $\mathrm{NF_{at}}$ (Fig. 11, App. A).

References

[1] Davide Ancona and Andrea Corradi. 2016. Semantic Subtyping for Imperative Object-oriented Languages. In *Proceedings of the 2016 ACM SIGPLAN International Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA 2016)*. ACM, New York, NY, USA, 568–587. https://doi.org/10.1145/2983990.2983992

[2] Jeff Bezanson. 2015. Abstraction in technical computing.

[3] Giuseppe Castagna, Giorgio Ghelli, and Giuseppe Longo. 1992. A Calculus for Overloaded Functions with Subtyping. In *Proceedings of the 1992 ACM Conference on LISP and Functional Programming (LFP '92)*. ACM, New York, NY, USA, 182–192. https://doi.org/10.1145/141471.141537

[4] Craig Chambers. 1992. Object-Oriented Multi-Methods in Cecil. In *Proceedings of the European Conference on Object-Oriented Programming (ECOOP '92)*. Springer-Verlag, Berlin, Heidelberg, 33–56. http://dl.acm.org/citation.cfm?id=646150.679216

[5] Curtis Clifton, Gary T. Leavens, Craig Chambers, and Todd Millstein. 2000. MultiJava: Modular Open Classes and Symmetric Multiple Dispatch for Java. In *Proceedings of the 15th ACM SIGPLAN Conference on Object-oriented Programming, Systems, Languages, and Applications (OOPSLA '00)*. ACM, New York, NY, USA, 130–145. https://doi.org/10.1145/353171.353181

[6] Ornela Dardha, Daniele Gorla, and Daniele Varacca. 2013. Semantic Subtyping for Objects and Classes. In *Formal Techniques for Distributed Systems*, Dirk Beyer and Michele Boreale (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 66–82.

[7] Alain Frisch, Giuseppe Castagna, and Véronique Benzaken. 2008. Semantic Subtyping: Dealing Set-theoretically with Function, Union, Intersection, and Negation Types. *J. ACM* 55, 4, Article 19 (Sept. 2008), 64 pages. https://doi.org/10.1145/1391289.1391293

[8] Haruo Hosoya and Benjamin C. Pierce. 2003. XDuce: A Statically Typed XML Processing Language. *ACM Trans. Internet Technol.* 3, 2 (May 2003), 117–148. https://doi.org/10.1145/767193.767195

[9] Haruo Hosoya, Jérôme Vouillon, and Benjamin C. Pierce. 2005. Regular Expression Types for XML. *ACM Trans. Program. Lang. Syst.* 27, 1 (Jan. 2005), 46–90. https://doi.org/10.1145/1053468.1053470

[10] Gary T. Leavens and Todd D. Millstein. 1998. Multiple Dispatch As Dispatch on Tuples. In *Proceedings of the 13th ACM SIGPLAN Conference on Object-oriented Programming, Systems, Languages, and Applications (OOPSLA '98)*. ACM, New York, NY, USA, 374–387. https://doi.org/10.1145/286936.286977

[11] Fabian Muehlboeck and Ross Tate. 2018. Empowering Union and Intersection Types with Integrated Subtyping. *Proc. ACM Program. Lang.* 2, OOPSLA, Article 112 (Oct. 2018), 29 pages. https://doi.org/10.1145/3276482

[12] Gyunghee Park, Jaemin Hong, Guy L. Steele Jr., and Sukyoung Ryu. 2019. Polymorphic Symmetric Multiple Dispatch with Variance. *Proc. ACM Program. Lang.* 3, POPL, Article 11 (Jan. 2019), 28 pages. https://doi.org/10.1145/3290324

[13] Benjamin C. Pierce. 2002. *Types and Programming Languages* (1st ed.). The MIT Press.

[14] Francesco Zappa Nardelli, Julia Belyakova, Artem Pelenitsyn, Benjamin Chung, Jeff Bezanson, and Jan Vitek. 2018. Julia Subtyping: A Rational Reconstruction. *Proc. ACM Program. Lang.* 2, OOPSLA, Article 113 (Oct. 2018), 27 pages. https://doi.org/10.1145/3276483

$$\frac{}{\mathrm{InNF}(v)}\ \textsc{NF-ValType} \qquad \frac{\mathrm{InNF}(\tau_1) \qquad \mathrm{InNF}(\tau_2)}{\mathrm{InNF}(\tau_1 \cup \tau_2)}\ \textsc{NF-Union}$$

Figure 8. Normal form of types in MiniJl

$$\begin{array}{rcl}
\mathrm{NF} : \textsc{Type} & \to & \textsc{Type} \\
\mathrm{NF}(\mathit{cname}) & = & \mathit{cname} \\
\mathrm{NF}(\mathsf{Real}) & = & \mathsf{Int} \cup \mathsf{Flt} \\
\mathrm{NF}(\mathsf{Num}) & = & \mathsf{Int} \cup \mathsf{Flt} \cup \mathsf{Cmplx} \\
\mathrm{NF}(\tau_1 \times \tau_2) & = & \mathtt{un_prs}(\mathrm{NF}(\tau_1), \mathrm{NF}(\tau_2)) \\
\mathrm{NF}(\tau_1 \cup \tau_2) & = & \mathrm{NF}(\tau_1) \cup \mathrm{NF}(\tau_2)
\end{array}$$

$$\begin{array}{rcl}
\mathtt{un_prs} : \textsc{Type} \times \textsc{Type} & \to & \textsc{Type} \\
\mathtt{un_prs}(\tau_{11} \cup \tau_{12},\ \tau_2) & = & \mathtt{un_prs}(\tau_{11}, \tau_2) \cup \mathtt{un_prs}(\tau_{12}, \tau_2) \\
\mathtt{un_prs}(\tau_1,\ \tau_{21} \cup \tau_{22}) & = & \mathtt{un_prs}(\tau_1, \tau_{21}) \cup \mathtt{un_prs}(\tau_1, \tau_{22}) \\
\mathtt{un_prs}(\tau_1,\ \tau_2) & = & \tau_1 \times \tau_2
\end{array}$$

Figure 9. Computing normal form of MiniJl types

$$\frac{\textsc{Atom-CName}}{\mathrm{Atom}(\mathit{cname})} \qquad \frac{\textsc{Atom-AName}}{\mathrm{Atom}(\mathit{aname})}$$

$$\frac{\mathrm{Atom}(\tau)}{\mathrm{InNF}_{\mathrm{at}}(\tau)}\ \textsc{NFAt-Atom}$$

$$\frac{\mathrm{InNF}_{\mathrm{at}}(\tau_1) \qquad \mathrm{InNF}_{\mathrm{at}}(\tau_2)}{\mathrm{InNF}_{\mathrm{at}}(\tau_1 \cup \tau_2)}\ \textsc{AtNF-Union}$$

Figure 10. Atomic normal form of types in MiniJl

$$\begin{array}{rcl}
\mathrm{NF}_{\mathrm{at}} : \textsc{Type} & \to & \textsc{Type} \\
\mathrm{NF}_{\mathrm{at}}(\mathit{cname}) & = & \mathit{cname} \\
\mathrm{NF}_{\mathrm{at}}(\mathit{aname}) & = & \mathit{aname} \\
\mathrm{NF}_{\mathrm{at}}(\tau_1 \times \tau_2) & = & \mathtt{un_prs}(\mathrm{NF}_{\mathrm{at}}(\tau_1), \mathrm{NF}_{\mathrm{at}}(\tau_2)) \\
\mathrm{NF}_{\mathrm{at}}(\tau_1 \cup \tau_2) & = & \mathrm{NF}_{\mathrm{at}}(\tau_1) \cup \mathrm{NF}_{\mathrm{at}}(\tau_2)
\end{array}$$

Figure 11. Computing atomic normal form of MiniJl types

A Appendix: Normal Forms

Fig. 8 defines the predicate $\mathrm{InNF}(\tau)$, which states that type τ is in normal form. Fig. 9 contains the full definition of $\mathrm{NF}(\tau)$ function, which computes the normal form of a type.

Fig. 10 and Fig. 11 present "atomic normal form", which can be used to define reductive subtyping that disables derivations such as $\mathsf{Real} \ \leq_{\mathrm{R}} \ \mathsf{Int} \cup \mathsf{Flt}$.