

Types	$T$	$::=$	$\alpha$	Type variable
			$\perp$	Bottom type
			$A \rightarrow B$	Function type
			$\forall \alpha * B. A$	Universal quantification
			$A \cap B$	Intersection type
Expressions	$e$	$::=$	$x$	Variable
			$\lambda(x:A). e$	Lambda
			$e_1 e_2$	Application
			$\Lambda \alpha * A. e$	Big lambda
			$e A$	Type application
			$e_1, e_2$	Merge
Contexts	$\Gamma$	$::=$	$\epsilon$	
			$\Gamma, \alpha * A$	
			$\Gamma, x:A$	
Sugar	$\Lambda \alpha. e$	$\equiv$	$\Lambda \alpha * \perp. e$	
	$e : A$	$\equiv$	$(\lambda z : A. z) e$	

Figure 1. Syntax.

## 1. Introduction

Dundfield’s work showed how many language features can be encoded in terms of intersection types with a merge operator. However two important questions were left open by Dundfield:

1. How to allow coherent programs only?
2. If a restriction that allows coherent programs is in place, can all coherent programs conform to the restriction?

In other words question 1) asks whether we can find sufficient conditions to guarantee coherency; whereas question 2) asks whether those conditions are also necessary. In terms of technical lemmas that would correspond to:

1. Coherency theorem:  $\Gamma \vdash e : A \rightsquigarrow E_1 \wedge \Gamma \vdash e : A \rightsquigarrow E_2 \rightarrow E_1 = E_2$ .
2. Completeness of Coherency:  $(\Gamma \vdash_{\text{old}} e : A \rightsquigarrow E_1 \wedge \Gamma \vdash_{\text{old}} e : A \rightsquigarrow E_2 \rightarrow E_1 = E_2) \rightarrow \Gamma \vdash e : A$ .

For these theorems we assume two type systems. On liberal type system that ensures type-safety, but not coherence ( $\Gamma \vdash_{\text{old}} e : A$ ); and another one that is both type-safe and coherent ( $\Gamma \vdash e : A$ ). What needs to be shown for completeness is that if a coherent program type-checks in the liberal type system, then it also type-checks in the restricted system.

### 1.1 “Testsuite” of examples

1.  $\lambda(x : \text{Int} * \text{Int}). (\lambda(z : \text{Int}). z) x$ : This example should not type-check because it leads to an ambiguous choice in the body of the lambda. In the current system the well-formedness checks forbid such example.
2.  $\Lambda A. \Lambda B. \lambda(x : A). \lambda(y : B). (\lambda(z : A). z)(x, y)$ : This example should not type-check because it is not guaranteed that the instantiation of A and B produces a well-formed type. The TyMerge rule forbids it with the disjointness check.
3.  $\Lambda A. \Lambda B * A. \lambda(x : A). \lambda(y : B). (\lambda(z : A). z)(x, y)$ : This example should type-check because B is guaranteed to be disjoint with A. Therefore instantiation should produce a well-formed type.
4.  $(\lambda(z : \text{Int}). z)((1, 'c'), (2, \text{False}))$ : This example should not type-check, since it leads to an ambiguous lookup of integers (can either be 1 or 2). The definition of disjointness is crucial to

$$\begin{array}{c}
 \boxed{A <: B \hookrightarrow F} \\
 \hline
 \alpha <: \alpha \hookrightarrow \lambda(x:|\alpha|). x \quad \text{SUBVAR} \\
 \\
 \frac{\tau_3 <: \tau_1 \hookrightarrow C_1 \quad \tau_2 <: \tau_4 \hookrightarrow C_2}{\tau_1 \rightarrow \tau_2 <: \tau_3 \rightarrow \tau_4 \hookrightarrow \lambda(f:|\tau_1 \rightarrow \tau_2|). \lambda(x:|\tau_3|). C_2 (f (C_1 x)))} \text{SUBFUN} \\
 \\
 \frac{\tau_1 <: [\alpha_1/\alpha_2] \tau_2 \hookrightarrow C}{\forall \alpha_1 * \tau_3. \tau_1 <: \forall \alpha_2 * \tau_3. \tau_2 \hookrightarrow \lambda(f:|\forall \alpha_1 * \tau_3. \tau_1|). \Lambda \alpha. C (f \alpha)} \text{SUBFORALL} \\
 \\
 \frac{\tau_1 <: \tau_2 \hookrightarrow C_1 \quad \tau_1 <: \tau_3 \hookrightarrow C_2}{\tau_1 <: \tau_2 \cap \tau_3 \hookrightarrow \lambda(x:|\tau_1|). (C_1 x, C_2 x)} \text{SUBAND} \\
 \\
 \frac{\tau_1 <: \tau_3 \hookrightarrow C \quad \tau_3 \text{ atomic}}{\tau_1 \cap \tau_2 <: \tau_3 \hookrightarrow \lambda(x:|\tau_1 \cap \tau_2|). C (\text{proj}_1 x)} \text{SUBAND}_1 \\
 \\
 \frac{\tau_2 <: \tau_3 \hookrightarrow C \quad \tau_3 \text{ atomic}}{\tau_1 \cap \tau_2 <: \tau_3 \hookrightarrow \lambda(x:|\tau_1 \cap \tau_2|). C (\text{proj}_2 x)} \text{SUBAND}_2
 \end{array}$$

Figure 2. Subtyping.

$$\begin{array}{c}
 \boxed{\Gamma \vdash A * B} \\
 \\
 \frac{\alpha * B \in \Gamma}{\Gamma \vdash \alpha * B} \text{DISJOINTREFL} \quad \frac{\alpha * A \in \Gamma}{\Gamma \vdash A * \alpha} \text{DISJOINTSYM} \\
 \\
 \frac{\Gamma \vdash A * C \quad \Gamma \vdash B * C}{\Gamma \vdash A \& B * C} \text{DISJOINTSUB1} \\
 \\
 \frac{\Gamma \vdash A * B \quad \Gamma \vdash A * C}{\Gamma \vdash A * B \& C} \text{DISJOINTSUB2} \\
 \\
 \frac{\Gamma \vdash B * D}{\Gamma \vdash A \rightarrow B * C \rightarrow D} \text{DISJOINTFUN} \\
 \\
 \frac{\Gamma \vdash A * C}{\Gamma \vdash \forall \alpha * B. A * \forall \alpha * B. C} \text{DISJOINTFORALL} \\
 \\
 \frac{A \not\sim B}{\Gamma \vdash A * B} \text{DISJOINTATOMIC}
 \end{array}$$

$$\begin{array}{c}
 \boxed{A \not\sim B} \\
 \\
 \perp \not\sim A \rightarrow B \text{ NOTSIMBOT1} \quad \perp \not\sim \forall \alpha * B. A \text{ NOTSIMBOT2} \\
 \\
 A \rightarrow B \not\sim \forall \alpha * B. A \text{ NOTSIMFUNFORALL} \\
 \\
 \frac{B \not\sim A}{A \not\sim B} \text{ NOTSIMFUNFORALL}
 \end{array}$$

Figure 3. Disjointness.

$$\boxed{\Gamma \vdash \tau \text{ type}}$$

$$\frac{\alpha * A \in \Gamma}{\Gamma \vdash \alpha \text{ type}} \text{ WFFVAR} \quad \frac{}{\Gamma \vdash \perp \text{ type}} \text{ WFBOT}$$

$$\frac{\Gamma \vdash A \text{ type} \quad \Gamma \vdash B \text{ type}}{\Gamma \vdash A \rightarrow B \text{ type}} \text{ WFFUN}$$

$$\frac{\Gamma \vdash A \text{ type} \quad \Gamma, \alpha * A \vdash B \text{ type}}{\Gamma \vdash \forall \alpha * A. B \text{ type}} \text{ WFFORALL}$$

$$\frac{\Gamma \vdash A \text{ type} \quad \Gamma \vdash B \text{ type} \quad \Gamma \vdash A * B}{\Gamma \vdash A \cap B \text{ type}} \text{ WFINTE}$$

Figure 4. Well-formed types.

$$\boxed{\Gamma \vdash e : A \hookrightarrow E}$$

$$\frac{x : A \in \Gamma}{\Gamma \vdash x : A \hookrightarrow x} \text{ TYVAR}$$

$$\frac{\Gamma \vdash A \text{ type} \quad \Gamma, x : A \vdash e : B \hookrightarrow E}{\Gamma \vdash \lambda(x:A). e : A \rightarrow B \hookrightarrow \lambda(x:A). E} \text{ TYLAM}$$

$$\frac{\Gamma \vdash e_1 : A_1 \hookrightarrow E_1 \quad \Gamma \vdash e_2 : A_2 \hookrightarrow E_2 \quad A_3 <: A_1 \hookrightarrow C}{\Gamma \vdash e_1 \ e_2 : A_2 \hookrightarrow E_1 \ (C \ E_2)} \text{ TYAPP}$$

$$\frac{\Gamma, \alpha * B \vdash e : A \hookrightarrow E \quad \Gamma \vdash B \text{ type}}{\Gamma \vdash \Lambda \alpha * B. e : \forall \alpha * B. A \hookrightarrow \Lambda \alpha. E} \text{ TYBLAM}$$

$$\frac{\Gamma \vdash e : \forall \alpha * B. C \hookrightarrow E \quad \Gamma \vdash A \text{ type} \quad \Gamma \vdash A * B}{\Gamma \vdash e A : [A/\alpha] C \hookrightarrow E [A]} \text{ TYTAPP}$$

$$\frac{\Gamma \vdash e_1 : A \hookrightarrow E_1 \quad \Gamma \vdash e_2 : B \hookrightarrow E_2 \quad \Gamma \vdash A * B}{\Gamma \vdash e_1, e_2 : A \cap B \hookrightarrow (E_1, E_2)} \text{ TYMERGE}$$

Figure 5. Typing.

prevent this example from type-checking. When type-checking the large merge, the disjointness predicate will detect that more than one integer exists in the merge.

5.  $(\lambda(f : \text{Int} \rightarrow \text{Int} \& \text{Bool}). \lambda(g : \text{Int} \rightarrow \text{Char} \& \text{Bool}). ((f, g) : \text{Int} \rightarrow \text{Bool}))$ : This example should not type-check, since it leads to an ambiguous lookup of functions. It shows that in order to check disjointness of functions we must also check disjointness of the subcomponents.
6.  $(\lambda(f : \text{Int} \rightarrow \text{Int}). \lambda(g : \text{Bool} \rightarrow \text{Int}). ((f, g) : \text{Bool} \& \text{Int} \rightarrow \text{Int}))$ : This example shows that whenever the return types overlap, so does the function type: we can always find a common subtype for the argument types.

## 1.2 Achieving coherence

The crucial challenge lies in the generation of coercions, which can lead to different results due to multiple possible choices in the rules that can be used. In particular the rules SubAnd1 and SubAnd2

overlap and can result in coercions that are not equivalent. A simple example is:

$(\lambda(x : \text{Int}). x)(1, 2)$

The result of this program can be either 1 or 2 depending on whether we chose SubAnd1 or SubAnd2.

Therefore the challenge of coherence lies in ensuring that, for any given types A and B, the result of  $A <: B$  always leads to the same (or semantically equivalent) coercions.

It is clear that, in general, the following does not hold:

if  $A <: B \rightsquigarrow C1$  and  $A <: B \rightsquigarrow C2$  then  $C1 = C2$

We can see this with the example above. There are two possible coercions:

$(\text{Int} \& \text{Int}) <: \text{Int} \rightsquigarrow \lambda(x, y). x$   
 $(\text{Int} \& \text{Int}) <: \text{Int} \rightsquigarrow \lambda(x, y). y$

However  $\lambda(x, y). x$  and  $\lambda(x, y). y$  are not semantically equivalent.

One simple observation is that the use of the subtyping relation on the example uses an ill-formed type  $(\text{Int} \& \text{Int})$ . Since the type system can prevent such bad uses of ill-formed types, it could be that if we only allow well-formed types then the uses of the subtyping relation do produce equivalent coercions. Therefore we postulate the following conjecture:

if  $A <: B \rightsquigarrow C1$  and  $A <: B \rightsquigarrow C2$  and A, B well formed then  $C1 = C2$

If the following conjecture does hold then it should be easy to prove that the translation is coherent.

$$e \vdash 1, 2 : (\text{Int} * \text{Int}) \Rightarrow \text{Int} \cap \text{Int}$$

We say two types are *disjoint* if they do not share a common supertype.

**Definition 1** (Disjointness).  $A \perp B = \neg \exists C. A <: C \wedge B <: C$

We require the types of two terms in a merge  $e_1, e_2$  to be disjoint. Why do we require this? That is because if both terms can be assigned some type C, both of them can be chosen as the meaning of the merge, which leads to multiple meaning of a term, known as incoherence.

## 2. Polymorphism with disjoint constraint

With a subtyping relation in a type system, bounded polymorphism extends the universal quantifier by confining the polymorphic type to be a subtype of a given type. In our type system, the forall binder also extends the parametric polymorphism, but in a different vein: the polymorphic type can only be disjoint with a given type.

- **Bounded polymorphism**—the instantiation can only be the descendant of a given type
- **Polymorphism with disjoint constraint**—the instantiation cannot share a common ancestor with a given type

The intuition can be found in figure ....

## 3. Intuition for the disjoint rules

The problem with the definition of disjointness is that it is a search problem. In this section, we are going to convert it that into an algorithm.

Let  $\mathbb{U}_0$  be the universe of  $\tau$  types. Let  $\mathbb{U}$  be the quotient set of  $\mathbb{U}_0$  by  $\approx$ , where  $\approx$  is defined by ....

Let  $\uparrow$  be the “common supertype” function, and  $\downarrow$  be the “common subtype” function. For example, assume Int and Char share no common supertype. Then the fact can be expressed by

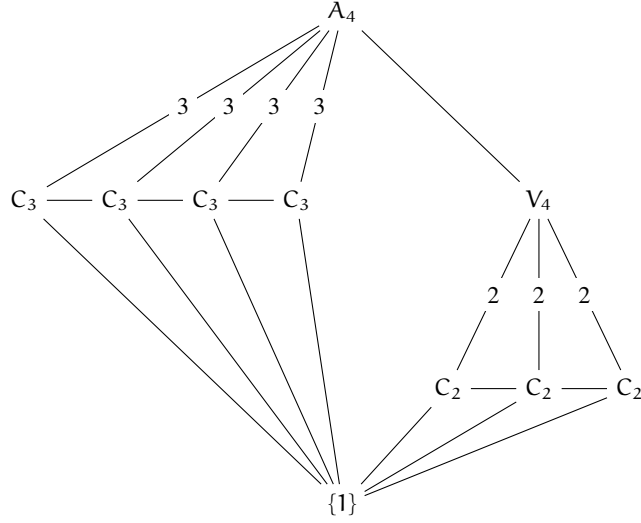


Figure 6. Untergruppenverband

$\uparrow (\text{Int}, \text{Char}) = \emptyset$ . Formally,

$$\uparrow : \mathbb{U} \times \mathbb{U} \rightarrow \mathcal{P}(\mathbb{U})$$

$$\downarrow : \mathbb{U} \times \mathbb{U} \rightarrow \mathcal{P}(\mathbb{U})$$

which, given two types, computes the set of their common super-types. ( $\mathcal{P}(S)$  denotes the power set of  $S$ , that is, the set of all subsets of  $S$ .)

$$\uparrow (\alpha, \alpha) = \{\alpha\}$$

$$\uparrow (\perp, \perp) = \{\perp\}$$

$$\uparrow (\tau_1 \rightarrow \tau_2, \tau_3 \rightarrow \tau_4) = \downarrow (\tau_1, \tau_3) \rightarrow \uparrow (\tau_2, \tau_4)$$

Notation. We use  $\downarrow (\tau_1, \tau_3) \rightarrow \uparrow (\tau_2, \tau_4)$  as a shorthand for  $\{s \rightarrow t \mid s \in \downarrow (\tau_1, \tau_3), t \in \uparrow (\tau_2, \tau_4)\}$ . Therefore, the problem of determining if  $\downarrow (\tau_1, \tau_3) \rightarrow \uparrow (\tau_2, \tau_4)$  is empty reduces to the problem of determining if  $\uparrow (\tau_2, \tau_4)$  is empty.

Note that there always exists a common subtype of any two given types (case disjoint / case nondisjoint).

## 4. Proof

### 4.1 Sketch of the proof

**Lemma 1** (Unique subtype contributor). *If  $A \cap B <: C$ , where  $A \cap B$  and  $C$  are well-formed types, then it is not possible that the following hold at the same time:*

1.  $A <: C$
2.  $B <: C$

If  $A \cap B <: C$ , then either  $A$  or  $B$  contributes to that subtyping relation, but not both. The implication of this lemma is that during the derivation, it is not possible that two rules are applicable.

*Proof.* Since  $A \cap B$  is well-formed,  $A * B$  by the formation rule of intersection types WINTER. Then by the definition of disjointness, there does not exist a type  $C$  such that  $A <: C$  and  $B <: C$ . It follows that  $A <: C$  and  $B <: C$  cannot hold simultaneously.  $\square$

The coercion of a subtyping relation  $A <: B$  is uniquely determined.

**Lemma 2** (Unique coercion). *If  $A <: B \hookrightarrow C_1$  and  $A <: B \hookrightarrow C_2$ , where  $A$  and  $B$  are well-formed types, then  $C_1 \equiv C_2$*

*Proof.* The set of rules for generating coercions is syntax-directed except for the three rules that involve intersection types in the conclusion. Therefore it suffices to show that if well-formed types  $A$  and  $B$  satisfy  $A <: B$ , where  $A$  or  $B$  is an intersection type, then at most one of the three rules applies. In the following, we do a case analysis on the shape of  $A$  and  $B$ :

- **Case  $A \neq A_1 \cap A_2$  and  $B = B_1 \cap B_2$ :** Clearly only SUBAND can apply.
- **Case  $A = A_1 \cap A_2$  and  $B \neq B_1 \cap B_2$ :** Only two rules can apply, SUBAND1 and SUBAND2. Further, by the unique subtype contributor lemma, it is not possible that  $A_1 <: B$  and that  $A_2 <: B$ . Thus we are certain that at most one rule of SUBAND1 and SUBAND2 will apply.
- **Case  $A = A_1 \cap A_2$  and  $B = B_1 \cap B_2$ :**<sup>2</sup> Since  $B$  is not atomic, only (SUBAND) apply.

$\square$

In general, disjointness judgements are not invariant with respect to free-variable substitution. In other words, a careless substitution can violate the disjoint constraint in the context. For example, in the context  $\alpha * \text{Int}$ ,  $\alpha$  and  $\text{Int}$  are disjoint:

$$\alpha * \text{Int} \vdash \alpha * \text{Int}$$

But after the substitution of  $\text{Int}$  for  $\alpha$  on the two types, the sentence

$$\alpha * \text{Int} \vdash \text{Int} * \text{Int}$$

is longer true since  $\text{Int}$  is clearly not disjoint with itself.

**Lemma 3.** *Invariance of disjointness* If  $\Gamma \vdash A * B$  and the  $\Gamma \vdash \beta * R$ , then  $\Gamma \vdash [R/\beta] A * [R/\beta] B$ .

*Proof.*

$\square$

**Lemma 4.** *Substitution* If  $\Gamma \vdash R$  type,  $\Gamma \vdash S$  type, and  $\Gamma \vdash \beta * R$ , then  $\Gamma \vdash [R/\beta] S$  type.

*Proof.* By induction on the derivation of  $\Gamma \vdash [R/\beta] S$  type.

- Case

$$\frac{\alpha * A \in \Gamma}{\Gamma \vdash \alpha \text{ type}} \text{WFVAR}$$

If  $\alpha$  happens to be the same as  $\beta$ , then by the def. of substitution  $[R/\beta] \alpha = R$ . Since  $\Gamma \vdash R$  type, we have  $\Gamma \vdash [R/\beta] \alpha$  type; On the other hand, if not, then by the def. of substitution  $[R/\beta] S = S$ . Since  $\Gamma \vdash S$  type, we also have  $\Gamma \vdash [R/\beta] \alpha$  type.

- Case

$$\frac{}{\Gamma \vdash \perp \text{ type}} \text{WFBOT}$$

Trivial.

- Case

$$\frac{\Gamma \vdash A \text{ type} \quad \Gamma \vdash B \text{ type}}{\Gamma \vdash A \rightarrow B \text{ type}} \text{WFFUN}$$

By i.h.,  $\Gamma \vdash [R/\beta] A$  type and  $\Gamma \vdash [R/\beta] B$  type. By the def. of substitution,  $\Gamma \vdash [R/\beta] A \rightarrow B$  type.

<sup>2</sup> An example of this case is:

$$(\text{Int} \cap \text{Bool}) \cap \text{Char} <: \text{Bool} \cap \text{Char}$$

- Case

$$\frac{\Gamma \vdash A \text{ type} \quad \Gamma, \alpha * A \vdash B \text{ type}}{\Gamma \vdash \forall \alpha * A. B \text{ type}} \text{ WFFORALL}$$

By the premise and the i.h.,

$$\Gamma, \alpha * A \vdash [R/\beta] B \text{ type}$$

which by (WFFORALL) implies

$$\Gamma \vdash \forall \alpha * A. [R/\beta] B \text{ type}$$

By the def. of substitution,  $\Gamma \vdash [R/\beta] \forall \alpha * A. B \text{ type}$ .

- Case

$$\frac{\Gamma \vdash A \text{ type} \quad \Gamma \vdash B \text{ type} \quad \Gamma \vdash A * B}{\Gamma \vdash A \cap B \text{ type}} \text{ WFINTE}$$

By i.h.,  $\Gamma \vdash [R/\beta] A \text{ type}$  and  $\Gamma \vdash [R/\beta] B \text{ type}$ . By some magic lemma, we also have  $\Gamma \vdash [R/\beta] A * [R/\beta] B$ . Therefore by (WFINTE),  $\Gamma \vdash [R/\beta] A \cap B \text{ type}$ .

□

**Lemma 5. Instantiation** If  $\Gamma \vdash \forall \alpha * B. C \text{ type}$ ,  $\Gamma \vdash A \text{ type}$ ,  $\Gamma \vdash A * B$ , then  $\Gamma \vdash [A/\alpha] C \text{ type}$ .

Instantiating a “forall” type results in a well-formed type if the type provided satisfies the disjoint constraint.

*Proof.* Since

$$\Gamma \vdash \forall \alpha * B. C \text{ type}$$

by (WFFORALL) we have

$$\Gamma \vdash B \text{ type}$$

$$\Gamma, \alpha * B \vdash C \text{ type}$$

Next we do a case analysis on the shape of  $C$ . The interesting case is when  $C$  is an intersection type.

$$\frac{\Gamma \vdash A \text{ type} \quad \Gamma \vdash B \text{ type} \quad \Gamma \vdash A * B}{\Gamma \vdash A \cap B \text{ type}} \text{ WFINTE}$$

Let  $C = C_1 \cap C_2$ . We know  $\Gamma \vdash C_1 \cap C_2 \text{ type}$  and need to show

$$\Gamma \vdash [A/\alpha] C_1 \cap C_2 \text{ type}$$

which is just

$$\Gamma \vdash [A/\alpha] C_1 \cap [A/\alpha] C_2 \text{ type}$$

by the definition of the substitution function. □

**Lemma 6. Well-formed typing** If  $\Gamma \vdash e : A$ , then  $\Gamma \vdash e \text{ type}$ .

Typing always produces a well-formed type.

*Proof.* By induction on the derivation of  $\Gamma \vdash e : A$ . The case of (TYTAPP) needs special attention

$$\frac{\Gamma \vdash e : \forall \alpha * B. C \hookrightarrow E \quad \Gamma \vdash A \text{ type} \quad \Gamma \vdash A * B}{\Gamma \vdash e A : [A/\alpha] C \hookrightarrow E [A]} \text{ TYTAPP}$$

because we need to show that the result of substitution ( $[A/\alpha] C$ ) is well-formed, which is evident by Lemma 5. □

**Theorem 1 (Unique elaboration).** If  $\Gamma \vdash e : A_1 \hookrightarrow E_1$  and  $\Gamma \vdash e : A_2 \hookrightarrow E_2$ , then  $E_1 \equiv E_2$ .

Given a source expression  $e$ , elaboration always produces the same target expression  $E$ .

*Proof.* The typing rules are syntax-directed. The case of (TYAPP) needs special attention since we still need to show that the generated coercion  $C$  is unique.

$$\frac{\Gamma \vdash e_1 : A_1 \rightarrow A_2 \hookrightarrow E_1 \quad \Gamma \vdash e_2 : A_3 \hookrightarrow E_2 \quad A_3 <: A_1 \hookrightarrow C}{\Gamma \vdash e_1 e_2 : A_2 \hookrightarrow E_1 (C E_2)} \text{ TYAPP}$$

By Lemma 6, we have  $\Gamma \vdash A_1 \text{ type}$  and  $\Gamma \vdash A_3 \text{ type}$ . Therefore we are able to apply Lemma 2 and conclude that  $C$  is unique. □

## 5. Application of the theory

### 5.1 Systems without subtyping

### 5.2 Systems with a top type

In type systems with a top type (such as `Object` in some OO languages), the definition of disjointness can be modified to:

We say two types are *disjoint* if their only common supertype is the top type.