

| | | | | |
|-------------|---------------------|----------|-----------------------------|--------------------------|
| Types | T | $::=$ | α | 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 | Γ | $::=$ | ϵ | |
| | | | $\Gamma, \alpha * A$ | |
| | | | $\Gamma, x:A$ | |
| Sugar | $\Lambda \alpha. e$ | \equiv | $\Lambda \alpha * \perp. e$ | |
| | $e : A$ | \equiv | $(\lambda z : A. z) e$ | |

Figure 1. Syntax.

| | |
|---|---------------------|
| $A <: B \hookrightarrow F$ | |
| $\alpha <: \alpha \hookrightarrow \lambda(x: \alpha). x$ | SUBVAR |
| $\tau_3 <: \tau_1 \hookrightarrow C_1 \quad \tau_2 <: \tau_4 \hookrightarrow C_2$ | |
| $\tau_1 \rightarrow \tau_2 <: \tau_3 \rightarrow \tau_4 \hookrightarrow \lambda(f: \tau_1 \rightarrow \tau_2). \lambda(x: \tau_3). C_2 (f (C_1 x))$ | SUBFUN |
| $\tau_1 <: [\alpha_1/\alpha_2] \tau_2 \hookrightarrow C$ | |
| $\forall \alpha_1 * \tau_3. \tau_1 <: \forall \alpha_2 * \tau_3. \tau_2 \hookrightarrow \lambda(f: \forall \alpha_1 * \tau_3. \tau_1). \Lambda \alpha. C (f \alpha)$ | SUBFORALL |
| $\tau_1 <: \tau_2 \hookrightarrow C_1 \quad \tau_1 <: \tau_3 \hookrightarrow C_2$ | |
| $\tau_1 <: \tau_2 \cap \tau_3 \hookrightarrow \lambda(x: \tau_1). (C_1 x, C_2 x)$ | SUBAND |
| $\tau_1 <: \tau_3 \hookrightarrow C$ | |
| $\tau_1 \cap \tau_2 <: \tau_3 \hookrightarrow \lambda(x: \tau_1 \cap \tau_2). C (\text{proj}_1 x)$ | SUBAND ₁ |
| $\tau_2 <: \tau_3 \hookrightarrow C$ | |
| $\tau_1 \cap \tau_2 <: \tau_3 \hookrightarrow \lambda(x: \tau_1 \cap \tau_2). C (\text{proj}_2 x)$ | SUBAND ₂ |

Figure 2. Subtyping.

0.1 “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.

| | | |
|----------------|--------------------------|--------------------------------|
| \perp atomic | $A \rightarrow B$ atomic | $\forall \alpha * B. A$ atomic |
|----------------|--------------------------|--------------------------------|

Figure 3. Atomic types.

| | |
|---|---|
| $\Gamma \vdash A \perp B$ | |
| $\frac{\alpha * B \in \Gamma}{\Gamma \vdash \alpha \perp B} \text{DISJOINTREFL}$ | $\frac{\alpha * A \in \Gamma}{\Gamma \vdash A \perp \alpha} \text{DISJOINTSYM}$ |
| $\frac{\Gamma \vdash A \perp C \quad \Gamma \vdash B \perp C}{\Gamma \vdash A \& B \perp C} \text{DISJOINTSUB1}$ | |
| $\frac{\Gamma \vdash A \perp B \quad \Gamma \vdash A \perp C}{\Gamma \vdash A \perp B \& C} \text{DISJOINTSUB2}$ | |
| $\frac{B \not<: A \quad A \not<: B \quad A \text{ atomic} \quad B \text{ atomic}}{\Gamma \vdash A \perp B} \text{DISJOINTATOMIC}$ | |

Figure 4. Disjointness.

| | |
|--|---|
| $\Gamma \vdash A \text{ type}$ | |
| $\Gamma \vdash \perp \text{ type WFBOT}$ | $\frac{\Gamma \vdash A \text{ type} \quad \Gamma \vdash B \text{ type}}{\Gamma \vdash A \rightarrow B \text{ type}} \text{WFFUN}$ |
| $\frac{\Gamma \vdash A \text{ type} \quad \Gamma \vdash B \text{ type}}{\Gamma \vdash \forall \alpha * B. A \text{ type}} \text{WFFORALL}$ | $\frac{\alpha * A \in \Gamma}{\Gamma \vdash \alpha \text{ type}} \text{WFVAR}$ |
| $\frac{\Gamma \vdash A \text{ type} \quad \Gamma \vdash B \text{ type} \quad \Gamma \vdash A \perp B}{\Gamma \vdash A \cap B \text{ type}} \text{WFINTER}$ | |

Figure 5. Well-formed types.

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 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.

0.2 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

$$\begin{array}{c}
\boxed{\Gamma \vdash e : A \hookrightarrow E} \\
\\
\frac{x : A \in \Gamma}{\Gamma \vdash x : A \hookrightarrow x} \text{TYVAR} \\
\\
\frac{\Gamma \vdash A \text{ type} \quad \Gamma, x : A \vdash e : B \hookrightarrow E}{\Gamma \vdash \lambda(x : A). e : A \rightarrow B \hookrightarrow \lambda(x : |A|). E} \text{TYLAM} \\
\\
\frac{\Gamma \vdash e_1 : A_1 \rightarrow A_2 \hookrightarrow E_1 \quad \Gamma \vdash e_2 : A_3 \hookrightarrow E_2 \quad A_3 <: A_1 \hookrightarrow C}{\Gamma \vdash e_1 e_2 : A_2 \hookrightarrow E_1 (C E_2)} \text{TYAPP} \\
\\
\frac{\Gamma, \alpha * B \vdash e : A \hookrightarrow E \quad \Gamma \vdash B \text{ type}}{\Gamma \vdash \Lambda \alpha * B. e : \forall \alpha * B. A \hookrightarrow \Lambda \alpha. E} \text{TYBLAM} \\
\\
\frac{\Gamma \vdash e : \forall \alpha * C. B \hookrightarrow E \quad \Gamma \vdash A \perp C \quad \Gamma \vdash A \text{ type}}{\Gamma \vdash e A : [A/\alpha]B \hookrightarrow E [A]} \text{TYTAPP} \\
\\
\frac{\Gamma \vdash e_1 : A \hookrightarrow E_1 \quad \Gamma \vdash e_2 : B \hookrightarrow E_2 \quad \Gamma \vdash A \perp B}{\Gamma \vdash e_1, e_2 : A \cap B \hookrightarrow (E_1, E_2)} \text{TYMERGE}
\end{array}$$

Figure 6. Typing.

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 $A <: B \rightsquigarrow C_1$ and $A <: B \rightsquigarrow C_2$ then $C_1 = C_2$

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 $A <: B \rightsquigarrow C_1$ and $A <: B \rightsquigarrow C_2$ and A, B well formed then $C_1 = C_2$

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

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

Definition 1. (Disjointness) Two sets S and T are *disjoint* if there does not exist an element x, such that $x \in S$ and $x \in T$.

Definition 2. (Disjointness) Two types A and B are *disjoint* if there does not exist an expression e, which is not a merge, such that $e \vdash e : A', e \vdash e : B', A' <: A$, and $B' <: B$.

Definition 3. (Disjointness) $A \perp B = \exists C. A <: C \wedge B <: C$

Two types A and B are *disjoint* if their least common supertype is \top .