Gradual Union Types
Complete Definition and Proofs

University of Chile
June 2017

Matías Toro and Éric Tanter
PLEIAD Laboratory
Computer Science Department (DCC)
University of Chile

Abstract. This report presents the complete definitions and proofs of GTFL\textsuperscript{⊕}, a gradual language that combines both gradual unions and the traditional, totally-unknown type. Gradual union types combine the benefits of both tagged and untagged unions, with added static flexibility backed by runtime checks. Compared to a standard gradually-typed language with only the totally-unknown type \?, the resulting design is stricter, allowing more blatantly wrong programs to be statically rejected. We also present a correct compilation scheme to GTFL\textsuperscript{⊕}, an internal language with support to threesomes, a space-efficient representation for casts.

Table of Contents

1 Overview ................................................................. 2
2 The Static Language: STFL ........................................... 2
3 GTFL\textsuperscript{⊕}: Definitions ....................................... 7
   3.1 Meaning of Gradual Unions ..................................... 7
      3.1.1 Step 1: The Classic Interpretation ....................... 7
      3.1.2 Step 2: The Classic Set Interpretation ............... 9
      3.1.3 Step 3: The Union Interpretation .................... 9
      3.1.4 Step 4: The Stratified Interpretation ............... 10
   3.2 Static Semantics of GTFL\textsuperscript{⊕} ......................... 11
      3.2.1 Consistent Predicates and Functions ................. 11
      3.2.2 Inductive definitions .................................. 14
      3.2.3 Examples of type derivations ....................... 15
   3.3 Dynamic Semantics of GTFL\textsuperscript{⊕} .................... 15
4 Properties of GTFL\textsuperscript{⊕} .................................. 17
   4.1 Static Gradual Guarantee .................................... 17
   4.2 Type Safety .................................................. 22
1 Overview

In this document we present the full definitions and proofs of the static language STFL, the gradual language GTFL and the intermediate language GTFL. Section 2 presents the full definition and proofs of the static language STFL: the static semantics, the dynamic semantics and its properties. Section 3 presents the full definition and proofs of GTFL; the Galois connections are presented in Section 3.1, the static semantics in Section 3.2 and the dynamic semantics in Section 3.3. Section 4 presents properties of GTFL and their proofs: the static gradual guarantee in Section 4.1, type safety in Section 4.2 and finally the dynamic gradual guarantee in Section 4.3. Section 5 presents the full definition and proofs of the compilation of GTFL to a threesome calculus. First we present the intermediate language GTFL in Section 5.1. Section 5.2 presents the cast insertion rules, and Section 5.3 presents the full formalization of the correctness of the translational semantics.

2 The Static Language: STFL

In this section we present the full definition of STFL. Figure 1 presents the syntax and type system, and Figure 2 presents the dynamic semantics. The rest of this section present the type safety proof of STFL.

Lemma 1 (Substitution). If \( \Gamma, x : T_1 \vdash t : T \) and \( \Gamma \vdash v : T'_1 \) such that \( T'_1 = T_1 \), then \( \Gamma \vdash [v/x]t : T' \) such that \( T' = T \).

Proof. By induction on the derivation of \( \Gamma, x : T_1 \vdash t : T \).

Proposition 1 (\( \rightarrow \) is well defined). If \( \Gamma \vdash t : T \), \( t \rightarrow t' \) then, \( \Gamma \vdash t' : T' \), where \( T' = T \).

Proof. Case (T+). Then \( t = b_1 + b_2 \) and

\[
\begin{align*}
(T+) \quad D_1 & \quad (T+) \quad D_2 \\
\Gamma \vdash n_1 : T_1 & \quad \Gamma \vdash n_2 : T_2 & \quad T_1 = \text{Int} & \quad T_2 = \text{Int}
\end{align*}
\]

Then

\( n_1 + n_2 \rightarrow (n_1 + n_2) \)

But \( \Gamma \vdash (n_1 + n_2) : \text{Int} \) and the result holds.
\[ T \in \text{TYPE}, \quad x \in \text{VAR}, \quad t \in \text{TERM}, \quad \Gamma \in \text{VAR}^{\text{fin}} \vdash \text{TYPE} \]
\[ T ::= \text{Bool} \mid \text{Int} \mid T \to T \quad \text{types} \]
\[ v ::= n \mid b \mid (\lambda x : T.t) \quad \text{values} \]
\[ t ::= v \mid x \mid t \mid t + t \mid \text{if } t \text{ then } t \text{ else } t \mid t :: T \quad \text{terms} \]
\[ (\text{Tx}) \frac{x : T \in \Gamma}{\Gamma \vdash x : T} \quad (\text{Tb}) \frac{\Gamma \vdash b : \text{Bool}}{\Gamma \vdash n : \text{Int}} \quad (\text{Tn}) \frac{\Gamma \vdash n : \text{Int}}{\Gamma : \text{INT}} \]
\[ (\text{Ta}) \frac{\Gamma, x : T_1 \vdash t : T_2}{\Gamma, \Sigma \vdash (\lambda x : T_1.t) : T_1 \to T_2} \quad (\text{Tt}) \frac{\Gamma \vdash t : T}{\Gamma : (t :: T) : T_1} \]
\[ (\text{Tapp}) \frac{\Gamma \vdash t_2 : T_2 \quad T_2 = \text{dom}(T_1)}{\Gamma \vdash t_1, t_2 : \text{cod}(T_1)} \quad (\text{Tf}) \frac{\Gamma \vdash t_1 : T_1 \quad T_1 = \text{Bool} \quad \Gamma \vdash t_2 : T_2 \quad \Gamma \vdash t_3 : T_3}{\Gamma \vdash \text{if } t_1 \text{ then } t_2 \text{ else } t_3 : \text{equate}(T_2, T_3)} \]

\[ \text{dom} : \text{TYPE} \to \text{TYPE} \quad \text{cod} : \text{TYPE} \to \text{TYPE} \quad \text{equate} : \text{TYPE}^2 \to \text{TYPE} \]
\[ \text{dom}(T_1 \to T_2) = T_1 \quad \text{cod}(T_1 \to T_2) = T_2 \quad \text{equate}(T, T) = T \]
\[ \text{dom}(T) \text{ undefined o.w.} \quad \text{cod}(T) \text{ undefined o.w.} \quad \text{equate}(T_1, T_2) \text{ undefined o.w.} \]

\textbf{Fig. 1. STFL: Syntax and Type System}

Case \( (\text{Tapp}) \). Then \( t = (\lambda x : T_{11}.t_1) v \), suppose \( \Gamma \vdash (\lambda x : T_{11}.t_1) : T_1 \), and \( \text{dom}(T_1) = T_{11} \) and \( \text{cod}(T_1) = T_{12} \). Therefore

\[ \frac{\qquad \frac{\Gamma, x : T_{11} \vdash t : T_{12}}{\Gamma \vdash (\lambda x : T_{11}.t_1) : T_{11} \to T_{12}}}{(\text{Ta})} \]
\[ \frac{\Gamma \vdash v : T_2}{\Gamma \vdash (\lambda x : T_{11}.t_1) v : T_{12}} \quad (\text{Tapp}) \]

Then

\[ (\lambda x : T_{11}.t_1) v \rightarrow [v/x]t_1 \]

By Lemma \[ \text{I} \] \( \Gamma \vdash [v/x]t_1 : T'_{12} \), where \( T'_{12} = T_{12} \), and the result holds.

Case \( (\text{Tif-true}) \). Then \( t = \text{if } \text{true} \text{ then } t_1 \text{ else } t_2 \) and

\[ \frac{\qquad \frac{\Gamma \vdash \text{true} : \text{Bool}}{\Gamma \vdash \text{if } \text{true} \text{ then } t_1 \text{ else } t_2 : \text{equate}(T_1, T_2)}}{\text{(Sif)}} \]

Then if

\[ \text{if } \text{true} \text{ then } t_1 \text{ else } t_2 \rightarrow t_1 \]
\[ v ::= n \mid \lambda x.t \mid \text{true} \mid \text{false} \mid v :: T \quad \text{(values)} \]
\[ f ::= □ + t \mid v + □ \mid □ t \mid v □ \mid □ :: T \quad \text{(frames)} \]

**Notions of Reduction**

\[ n_1 + n_2 \rightarrow n_3 \text{ where } n_3 = n_1 [+] n_2 \]
\[ (\lambda x.t) v \rightarrow ([v/x]t) \]
\[ \text{if true then } t_1 \text{ else } t_2 \rightarrow t_1 \]
\[ \text{if false then } t_1 \text{ else } t_2 \rightarrow t_2 \]
\[ v :: T \rightarrow v \]

**Reduction**

\[
\begin{array}{c}
\frac{t_1 \rightarrow t_2}{t_1 \mapsto \rightarrow t_2} \\
\frac{t_1 \rightarrow t_2}{f[t_1] \rightarrow f[t_2]}
\end{array}
\]

**Fig. 2.** STFL: Dynamic Semantics

But

\[
\frac{D_1}{Γ \vdash t_1 : T_1}
\]

and by definition of the \textit{equate} operator, \( T_1 = \text{equate}(T_1, T_2) \) and the result holds.

**Case (Tif-false).** Analogous to case (if-true).

**Case (T::).** Then \( t = v :: T \) and

\[
\frac{D}{Γ \vdash v : T_1} \quad \frac{T_1 = T}{Γ \vdash v :: T : T}
\]

Then

\[ v :: T \rightarrow v \]

But \( T_1 = T \) and the result holds.

**Proposition 2 (Canonical forms).** Consider a value \( v \) such that \( \cdot \vdash v : T \). Then:

1. If \( T = \text{Bool} \) then \( v = b \) for some \( b \).
2. If \( T = \text{Int} \) then \( v = n \) for some \( n \).
3. If \( T = T_1 \rightarrow T_2 \) then \( v = (\lambda x : T_1.t_2) \) for some \( t_2 \).

**Proof.** By inspection of the type derivation rules.
Lemma 2. Consider frame $f$, and term $t_1$, such as $\Gamma \vdash t_1 : T_1$ and $\Gamma \vdash f[t_1] : T$. Consider term $t'_1$, such that $\Gamma \vdash t'_1 : T'_1$ and $T'_1 = T_1$. Then $\Gamma \vdash f[t'_1] : T'$ such that $T' = T$.

Proof. By induction on the derivation of $f[t_1]$.

Case ($\square t$). Then $f = \square t_2$, $f[t_1] = t_1 t_2$ and

$$
\frac{
\Gamma \vdash t_1 : T_1 \quad \Gamma \vdash t_2 : T_2 \quad T_2 = \text{dom}(T_1)
}{
\Gamma \vdash t_1 t_2 : \text{cod}(T_1)
}(\text{Tapp})
$$

then $f[t'_1] = t'_1 t_2$. But as $T'_1 = T_1$ then $\text{cod}(T'_1) = \text{cod}(T_1)$ and $\text{dom}(T_1) = \text{dom}(T'_1)$. Therefore

$$
\frac{
\Gamma \vdash t_1 : T'_1 \quad \Gamma \vdash t_2 : T_2 \quad T_2 = \text{dom}(T'_1)
}{
\Gamma \vdash t'_1 t_2 : \text{cod}(T'_1)
}(\text{Tapp})
$$

and the result holds.

Case ($v \square, \square + t, v + \square$, if $\square$ then $t$ else $t$). Analogous to ($\square t$).

Proposition 3 ($\rightarrow$ is well defined). If $\Gamma \vdash t : T$, $t \rightarrow t'$ then, $\Gamma \vdash t' : T'$, where $T' = T$.

Proof. By induction on the structure of a derivation of $t \rightarrow t'$.

Case ($\rightarrow$). Then $t \rightarrow t'$. By well-definedness of $\rightarrow$ (Prop 1), $\Gamma \vdash t' : T'$, where $T' = T$, and the result holds immediately.

Case ($f\square$). Then $t = f[t_1]$, $\Gamma \vdash t_1 : T_1$ and $t_1 \rightarrow t_2$. By induction hypothesis $\Gamma \vdash t_2 : T_2$ where $T_2 = T_1$. By Lemma 2 $\Gamma \vdash f[t_2] : T'$ such that $T' = T$, and the result holds immediately.

Proposition 4 (Safety). If $\Gamma \vdash t : T$, then one of the following is true:

- $t$ is a value $v$;
- $t \rightarrow t'$, and $\Gamma \vdash t' : T'$ where $T' = T$.

Proof. By induction on the structure of $t$.

Case ($Tb, Tn, T\lambda, Tl$). $t$ is a value.

Case ($T+$). Then $t = t_1 + t_2$ and

$$
\frac{
\Gamma \vdash t_1 : T_1 \quad \Gamma \vdash t_2 : T_2 \quad T_1 = \text{int} \quad T_2 = \text{int}
}{
\Gamma \vdash t_1 + t_2 : \text{int}
}(T+)
$$

By induction hypotheses, one of the following holds:

1. $t_1$ is a value. Then by induction on $t_2$ one of the following holds:
By induction hypotheses, one of the following holds:

1. \( t_2 \) is a value. Then by Canonical Forms (Lemma 2)

\[
(R\rightarrow) \quad \frac{t \rightarrow t'}{t \rightarrow t'}
\]

and by Prop 1, \( \Gamma \vdash t' : T' \), where \( T' = T \), and therefore the result holds.

2. \( t_2 \rightarrow t_2' \). Then by induction hypothesis, \( \Gamma \vdash t_2 : T_2' \), where \( T_2' = T_2 \).

Then by (Tf), using \( f = v + \square \), \( t \mapsto t_1 + t_2' \) and by Lemma 2, \( \Gamma \vdash t_1 + t_2' : \text{Int} \) and the result holds.

Case (Sapp). Then \( t = t_1 \cdot t_2 \), \( T = T_{12} \) and

\[
(T\text{app}) \quad \frac{\Gamma \vdash t_1 : T_1 \quad \Gamma \vdash t_2 : T_2 \quad T_2 = dom(T_1)}{\Gamma \vdash t_1 \cdot t_2 : cod(T_1)}
\]

By induction hypotheses, one of the following holds:

1. \( t_1 \) is a value. Then by Canonical Forms (Lemma 2), and induction on \( t_2 \) one of the following holds:

   a) \( t_2 \) is a value. Then by Canonical Forms (Lemma 2)

   \[
   (R\rightarrow) \quad \frac{t \rightarrow t'}{t \rightarrow t'}
   \]

   and by Prop 1, \( \Gamma \vdash t' : T' \), where \( T' = T \), and therefore the result holds.

   b) \( t_2 \rightarrow t_2' \). Then by induction hypothesis, \( \Gamma \vdash t_2 : T_2' \), where \( T_2' = T_2 \).

   Then by (Tf), using \( f = v \cdot \square \), \( t \mapsto t_1 \cdot t_2' \) and by Lemma 2, \( \Gamma \vdash t_1 \cdot t_2' : T_{12} \)

   where \( T_{12} = cod(T_1) \) and the result holds.

2. \( t_1 \rightarrow t_1' \). Then by induction hypotheses, \( \Gamma' \vdash t_1' : T_{11} \rightarrow T_{12} \) where \( T_{11} \rightarrow T_{12} = T_1 \). Then by (Tf), using \( f = \square \cdot t_2 \), \( t \mapsto t_1' \cdot t_2 \) and by Lemma 2, \( \Gamma \vdash t_1' \cdot t_2 : T_{12} \)

   where \( T_{12} = cod(T_1) \) and the result holds.

Case (Tif). Then \( t = \text{if } t_1 \text{ then } t_2 \text{ else } t_3 \) and

\[
(T\text{if}) \quad \frac{\Gamma \vdash t_1 : T_1 \quad T_1 = \text{Bool} \quad \Gamma \vdash t_2 : T_2 \quad \Gamma \vdash t_3 : T_3}{\Gamma \vdash \text{if } t_1 \text{ then } t_2 \text{ else } t_3 : \text{equate}(T_2, T_3)}
\]

By induction hypotheses, one of the following holds:

1. \( t_1 \) is a value. Then by Canonical Forms (Lemma 2)

\[
(R\rightarrow) \quad \frac{t \rightarrow t'}{t \rightarrow t'}
\]

and by Prop 1, \( \Gamma \vdash t' : T' \), where \( T' = T \), and therefore the result holds.

2. \( t_1 \rightarrow t_1' \). Then by induction hypothesis, \( \Gamma \vdash t_1' : T_1' \), where \( T_1' = T_1 \).

Therefore \( T_1' = \text{Bool} \). Then by (Tf), using \( f = \text{if } \square \text{ then } t \text{ else } t, t \mapsto \text{if } t_1' \text{ then } t_2 \text{ else } t_3 \) and by Lemma 2, \( \Gamma \vdash \text{if } t_1' \text{ then } t_2 \text{ else } t_3 : T' \)

where \( T' = \text{equate}(T_2, T_3) \) and the result holds.
Case \((T::)\). Then \(t = t_1 :: T_2\) and
\[
\begin{align*}
(T::) & \quad \Gamma \vdash t_1 : T_1 \quad T_1 = T_2 \\
\Gamma & \vdash t_1 :: T_2 : T_2
\end{align*}
\]
By induction hypotheses, one of the following holds:

1. \(t_1\) is a value. Then
\[
\begin{align*}
(R\rightarrow) & \quad t \mapsto t' \\
\Gamma & \vdash t' \quad t \mapsto t'
\end{align*}
\]
and by Prop 1, \(\Gamma \vdash t' : T'\), where \(T' = T\), and therefore the result holds.

2. \(t_1 \mapsto t'_1\). Then by induction hypothesis, \(\Gamma \vdash t'_1 : T'_1\), where \(T'_1 = T_1\). Then
by \((Tf)\), using \(f = \Box :: T, t \mapsto t'_1 :: T_2\), but \(\Gamma \vdash t'_1 :: T_2 : T_2\) and the result holds.

3 GTFL\(^\oplus\): Definitions

Section 3.1 presents the Galois connections along its soundness and optimality proofs. Section 3.2 presents the static semantics of GTFL\(^\oplus\). Finally, Section 3.3 presents the dynamic semantics of GTFL\(^\oplus\).

3.1 Meaning of Gradual Unions

This section presents the different steps taken to derive the Galois connection. Section 3.1.1 presents the classic interpretation which interprets the unknown type \(?\). Section 3.1.2 presents the powerset lifting of the classic interpretation. Section 3.1.3 presents the union interpretation which add support for gradual unions among gradual types that include the unknown type. Finally in Section 3.1.4 we combine the classic set interpretation and the union interpretation, named the stratified interpretation.

3.1.1 Step 1: The Classic Interpretation We start by presenting the Galois connection for gradual types made up with the (nullary constructor) \(?\), here denoted GTYPE.

\[
\begin{align*}
G & \in \text{GTYPE} \\
G & ::= ? \mid \text{Bool} \mid \text{Int} \mid G \rightarrow G
\end{align*}
\]

The meaning of these gradual types is standard, and defined through concretization by Garcia et al. \cite{garcia2016} as follows:

Definition 1 (GTYPE Concretization). \(\gamma : \text{GTYPE} \rightarrow \mathcal{P}(\text{TYPE})\)

\[
\begin{align*}
\gamma(\text{Int}) & = \{ \text{Int} \} \\
\gamma(\text{Bool}) & = \{ \text{Bool} \} \\
\gamma(?) & = \text{TYPE} \\
\gamma(G_1 \rightarrow G_2) & = \{ T_1 \rightarrow T_2 \mid T_1 \in \gamma(G_1) \land T_2 \in \gamma(G_2) \}
\end{align*}
\]
Proof. We proceed by induction on the structure of $\gamma$.

Case $(\alpha \land \gamma)$. Proposition 5 ($\alpha \land \gamma$ if and only if $\gamma$).

Definition 3 (GType Abstraction). $\alpha : \mathcal{P}(\text{TYPE}) \rightarrow \text{GType}$

\[
\alpha_1(\{ T \}) = T \quad \alpha_2(\overrightarrow{T_1} \rightarrow \overrightarrow{T_2}) = \alpha_1(\overrightarrow{T_1}) \rightarrow \alpha_1(\overrightarrow{T_2}) \quad \alpha_1(\emptyset) = \text{undefined}
\]

$\alpha_1(\overrightarrow{T}) = ?$ otherwise.

Proposition 5 ($\alpha_1$ is Sound and Optimal). If $\overrightarrow{T}$ is not empty, then

(a) $\overrightarrow{T} \subseteq \gamma_1(\alpha_1(\overrightarrow{T}))$.  
(b) $\overrightarrow{T} \subseteq \gamma_1(G) \Rightarrow \alpha_1(\overrightarrow{T}) \subseteq G$.

Proof. We proceed by induction on the structure of $\overrightarrow{U}$. Let us start by proving a).

Case $(\{ \text{Int} \})$. Then $\alpha_1(\{ \text{Int} \}) = \text{Int}$. But $\gamma_1(\text{Int}) = \{ \text{Int} \}$ and the result holds.

Case $(\{ \text{Bool} \})$. Analogous to case $\{ \text{Int} \}$.

Case $(\overrightarrow{T_1} \rightarrow \overrightarrow{T_2})$. Then $\alpha_1(\overrightarrow{T_1} \rightarrow \overrightarrow{T_2}) = \alpha_1(\overrightarrow{T_1}) \rightarrow \alpha_1(\overrightarrow{T_2})$. But by definition of $\gamma_1$, $\gamma_1(\alpha_1(\overrightarrow{T_1}) \rightarrow \alpha_1(\overrightarrow{T_2})) = \gamma_1(\alpha_1(\overrightarrow{T_1})) \Rightarrow \gamma_1(\alpha_1(\overrightarrow{T_2}))$. By induction hypotheses, $\overrightarrow{T_1} \subseteq \gamma_1(\alpha_1(\overrightarrow{T_1}))$ and $\overrightarrow{T_2} \subseteq \gamma_1(\alpha_1(\overrightarrow{T_2}))$, therefore $\overrightarrow{T_1} \Rightarrow \overrightarrow{T_2} \subseteq \gamma_1(\alpha_1(\overrightarrow{T_1}) \rightarrow \alpha_1(\overrightarrow{T_2}))$ and the result holds.

Case $(\emptyset)$. This case cannot happen because $\alpha_1$ is restricted to non-empty sets of gradual intermediate types.

Case $(\overrightarrow{T})$. Then $\alpha_1(\overrightarrow{T}) = ?$ and therefore $\gamma_1(\alpha_1(\overrightarrow{T})) = \text{TYPE}$, but $\overrightarrow{T} \subseteq \text{TYPE}$ and the result holds.

Now let us prove b).

Case $(\text{Int})$. Trivial because $\gamma_1(\text{Int}) = \{ \text{Int} \}$, and $\alpha_1(\{ \text{Int} \}) = \text{Int}$.

Case $(\text{Bool})$. Analogous to case Int.

Case $(G_1 \rightarrow G_2)$. We have to prove that $\gamma_1(\alpha_1(\overrightarrow{T})) \subseteq \gamma_1(G_1 \rightarrow G_2)$. But we know that $\overrightarrow{T} \subseteq \gamma_1(G_1 \rightarrow G_2) = \gamma_1(G_1) \Rightarrow \gamma_1(G_2)$, therefore $\overrightarrow{T}$ has the form $\{ \overrightarrow{T_{i1}} \rightarrow \overrightarrow{T_{i2}} \}$, for some $\overrightarrow{T_{i1}} \subseteq \gamma_1(G_1)$ and $\overrightarrow{T_{i2}} \subseteq \gamma_1(G_2)$. But by definition of $\alpha_1$, $\alpha_1(\{ \overrightarrow{T_{i1}} \rightarrow \overrightarrow{T_{i2}} \}) = \alpha_1(\{ \overrightarrow{T_{i1}} \}) \rightarrow \alpha_1(\{ \overrightarrow{T_{i2}} \})$ and therefore $\gamma_1(\alpha_1(\{ \overrightarrow{T_{i1}} \}) \rightarrow \alpha_1(\{ \overrightarrow{T_{i2}} \})) = \gamma_1(\alpha_1(\{ \overrightarrow{T_{i1}} \})) \Rightarrow \gamma_1(\alpha_1(\{ \overrightarrow{T_{i2}} \}))$. But by induction hypotheses $\gamma_1(\alpha_1(\{ \overrightarrow{T_{i1}} \})) \subseteq \gamma_1(G_1) \rightarrow \gamma_1(\alpha_1(\{ \overrightarrow{T_{i2}} \})) \subseteq \gamma_1(G_2)$ and the result holds.

Case (?). Then we have to prove that $\gamma_1(\alpha_1(\overrightarrow{T})) \subseteq \gamma_1(?) = \text{TYPE}$, but this is always true and the result holds immediately.
### 3.1.2 Step 2: The Classic Set Interpretation

The powerset lifting of \( \gamma \), denoted \( \hat{\gamma} \), is simply the piecewise application of \( \gamma \):

**Definition 4 (Pfin(GType) Concretization).**

\[
\hat{\gamma}(\hat{G}) = \{ \gamma(G) \mid G \in \hat{G} \}
\]

Similarly, the powerset lifting of the abstraction function \( \alpha \), denoted \( \hat{\alpha} \), is the union of the piecewise application of \( \alpha \):

**Definition 5 (Pfin(GType) Abstraction).**

\[
\hat{\alpha}(\emptyset) = \text{undefined} \quad \hat{\alpha}(\hat{T}) = \bigcup_{\hat{T} \in \hat{T}} \alpha(\hat{T})
\]

**Proposition 6 (\( \hat{\alpha} \) is Sound and Optimal).** If \( \hat{T} \) is not empty, then

a) \( \hat{T} \subseteq \hat{\gamma}(\hat{\alpha}(\hat{T})) \).

b) \( \hat{T} \subseteq \hat{\gamma}(\hat{G}) \Rightarrow \hat{\alpha}(\hat{T}) \subseteq \hat{G} \).

*Proof.* We start proving a). By definition of \( \hat{\alpha} \), \( \hat{\gamma}(\hat{\alpha}(\hat{T})) = \bigcup_{\hat{T} \in \hat{T}} \alpha(\hat{T}) \). And by definition of \( \hat{\gamma} \), \( \hat{\gamma}(\hat{\alpha}(\hat{T})) = \{ \gamma(\alpha(\hat{T})) \mid \hat{T} \in \hat{T} \} \). We have to prove that \( \forall \hat{T} \in \hat{\gamma}(\hat{\alpha}(\hat{T})) \), \( \exists \hat{\alpha} \hat{T}' \in \hat{\gamma}(\hat{\alpha}(\hat{T})) \) such that \( \hat{T} \subseteq \hat{T}' \). But we now that \( \alpha \) is sound therefore \( \forall \hat{T} \in \hat{\gamma}(\hat{T}), \hat{T} \subseteq \gamma(\alpha(\hat{T})) \), and the result holds immediately.

Now we prove b). We know that \( \forall \hat{T} \in \hat{\gamma}(\hat{\alpha}(\hat{T})), \exists \hat{T}' \in \hat{\gamma}(\hat{\alpha}(\hat{T})) \) such that \( \hat{T} \subseteq \hat{T}' \). We have to prove that \( \hat{\gamma}(\hat{\alpha}(\hat{T})) \subseteq \hat{\gamma}(\hat{G}) \). But \( \hat{\gamma}(\hat{\alpha}(\hat{T})) = \{ \gamma(\alpha(\hat{T})) \mid \hat{T} \in \hat{T} \} \). But as \( \alpha \) is optimal, \( \forall \) non empty \( \hat{T} \), if \( \hat{T} \subseteq \hat{G} \) then \( \gamma(\alpha(\hat{T})) \subseteq \gamma(\hat{G}) \). Then we know that \( \forall \hat{T} \in \hat{\gamma}(\hat{T}), \gamma(\alpha(\hat{T})) \subseteq \hat{\gamma}(\hat{G}) \), and the result holds.

### 3.1.3 Step 3: The Union Interpretation

Now that we have defined the meaning of gradual types formed with the unknown type \( ? \), as well as the meaning of gradual types formed with gradual unions \( \oplus \), we turn to defining the meaning of gradual types in GTFL\( ^\oplus \), which combine both constructors, denoted UTYPE:

\[
\begin{align*}
U & \in \text{UTYPE} \\
U ::= ? | U \oplus U | \text{Bool} | \text{Int} | U \to U \quad \text{(gradual types)}
\end{align*}
\]

We define a Galois connection between UTYPE and \( P_{\text{fin}}(\text{GType}) \) as follows:

**Definition 6 (UType Concretization).**

\[
\begin{align*}
\gamma_\oplus(\text{Int}) &= \{ \text{Int} \} \\
\gamma_\oplus(\text{Bool}) &= \{ \text{Bool} \} \\
\gamma_\oplus(?) &= \{ ? \} \\
\gamma_\oplus(U_1 \to U_2) &= \{ T_1 \to T_2 \mid T_1 \in \gamma_\oplus(U_1) \land T_2 \in \gamma_\oplus(U_2) \} \\
\gamma_\oplus(U_1 \oplus U_2) &= \gamma_\oplus(U_1) \cup \gamma_\oplus(U_2)
\end{align*}
\]
Definition 7 (UType Abstraction). \( \alpha_{\oplus} : \mathcal{P}_{\text{fin}}(\text{GType}) \rightarrow \text{UType} \)

\[
\alpha_{\oplus}(\hat{G}) = \oplus_{\hat{G}} \quad \text{if } \hat{G} \neq \emptyset
\]

Proposition 7 (\( \alpha_{\oplus} \) is Sound and Optimal). If \( \hat{G} \) is not empty, then

\[
a) \ \hat{G} \subseteq \gamma_{\oplus}(\alpha_{\oplus}(\hat{G})). \quad \quad \quad \quad \quad \quad \quad b) \ \hat{G} \subseteq \gamma_{\oplus}(U) \Rightarrow \alpha_{\oplus}(\hat{G}) \subseteq U.
\]

Proof. We proceed by induction on the structure of \( U \). Let us start by proving a).

Case \( \{ \text{Int} \} \). Then \( \alpha_{\oplus}(\{ \text{Int} \}) = \text{Int} \). But \( \gamma_{\oplus}(\text{Int}) = \{ \text{Int} \} \) and the result holds.

Case \( \{ \text{Bool} \} \). Analogous to case \( \{ \text{Int} \} \).

Case \( \{ ? \} \). Analogous to case \( \{ \text{Int} \} \).

Case \( \emptyset \). This case cannot happen because \( \alpha_{\oplus} \) is restricted to non-empty sets of gradual intermediate types.

Case \( (T_1 \cup T_2) \). Then \( \alpha_{\oplus}(T_1 \cup T_2) = \alpha_{\oplus}(T_1) \oplus \alpha_{\oplus}(T_2) \). But by definition of \( \gamma_{\oplus} \),

\[
\gamma_{\oplus}(\alpha_{\oplus}(T_1) \oplus \alpha_{\oplus}(T_2)) = \gamma_{\oplus}(\alpha_{\oplus}(T_1)) \cup \gamma_{\oplus}(\alpha_{\oplus}(T_2)).
\]

By induction hypotheses, \( T_1 \subseteq \gamma_{\oplus}(\alpha_{\oplus}(T_1)) \) and \( T_2 \subseteq \gamma_{\oplus}(\alpha_{\oplus}(T_2)) \), therefore \( T_1 \cup T_2 \subseteq \gamma_{\oplus}(\alpha_{\oplus}(T_1) \oplus \alpha_{\oplus}(T_2)) \) and the result holds.

Now let us prove b).

Case \( \text{Int} \). Trivial because \( \gamma_{\oplus}(\text{Int}) = \{ \text{Int} \} \), and \( \alpha_{\oplus}(\{ \text{Int} \}) = \text{Int} \).

Case \( \text{Bool} \). Analogous to case \( \text{Int} \).

Case \( ? \). Analogous to case ?.

Case \( (U_1 \rightarrow U_2) \). We have to prove that \( \gamma_{\oplus}(\alpha_{\oplus}(\hat{G})) \subseteq \gamma_{\oplus}(U_1 \rightarrow U_2) \). But \( \gamma_{\oplus}(\alpha_{\oplus}(\hat{G})) = \gamma_{\oplus}(\oplus_{\hat{G}}) = \hat{G} \) and the result follows.

Case \( (U_1 \cup U_2) \). Then \( \gamma_{\oplus}(U_1 \cup U_2) = \gamma_{\oplus}(U_1) \cup \gamma_{\oplus}(U_2) \) and \( G = G_1 \cup G_2 \) for some \( G_1 \) and \( G_2 \) such that \( G_1 \subseteq \gamma_{\oplus}(U_1) \) and \( G_2 \subseteq \gamma_{\oplus}(U_2) \). By definition of \( \alpha_{\oplus} \),

\[
\alpha_{\oplus}(G) = \alpha_{\oplus}(G_1) \cup \alpha_{\oplus}(G_2).
\]

By induction hypotheses, \( \gamma_{\oplus}(\alpha_{\oplus}(G_1)) \subseteq \gamma_{\oplus}(U_1) \) and \( \gamma_{\oplus}(\alpha_{\oplus}(G_2)) \subseteq \gamma_{\oplus}(U_2) \), therefore \( \gamma_{\oplus}(G) = \gamma_{\oplus}(\alpha_{\oplus}(G_1)) \cup \gamma_{\oplus}(\alpha_{\oplus}(G_2)) \), then \( \gamma_{\oplus}(\alpha_{\oplus}(\hat{G})) \subseteq \gamma_{\oplus}(U_1) \cup \gamma_{\oplus}(U_2) = \gamma_{\oplus}(U) \) and the result holds.

3.1.4 Step 4: The Stratified Interpretation We can now compose the two Galois connections in order to define a stratified interpretation for UType in terms of sets of sets of static types.

Definition 8 (Concretization). \( \gamma : \text{UType} \rightarrow \mathcal{P}_{\text{fin}}(\mathcal{P}(\text{Type})) \), \( \gamma = \oplus_{\hat{G}} \circ \gamma_{\oplus} \)

Definition 9 (Abstraction). \( \alpha : \mathcal{P}_{\text{fin}}(\mathcal{P}(\text{Type})) \rightarrow \text{UType} \), \( \alpha = \alpha_{\oplus} \circ \alpha \).
Because the composition of two Galois connection is a Galois connection, the stratified interpretation \( \langle \gamma, \alpha \rangle \) is a Galois connection.

**Proposition 8 (\( \alpha \) is Sound and Optimal).** If \( \mathcal{T} \) is not empty, then

\[
\begin{align*}
(a) & \quad \mathcal{\widehat{T}} \subseteq \gamma(\mathcal{\widehat{T}}), \\
(b) & \quad \mathcal{\widehat{T}} \subseteq \gamma(U) \Rightarrow \alpha(\mathcal{\widehat{T}}) \subseteq U.
\end{align*}
\]

**Proof.** By propositions [7] and [8] and composition of sound and optimal abstractions.

### 3.2 Static Semantics of GTFL\(^\oplus\)

This section presents the full static semantics of GTFL\(^\oplus\) in Figure 3. Section 3.2.1 formally justifies the compositional lifting of predicates and functions. Section 3.2.2 presents the inductive definitions. Finally, Section 3.2.3 presents some type derivations examples.

#### 3.2.1 Consistent Predicates and Functions

We can base our liftings of predicates and types on inclusion and pointwise application that are extended to sets of sets.
Definition 10 (Predicate Lifting). \( \tilde{P}(U_1, U_2) \iff \exists \tilde{T}_1 \in \gamma(U_1), \tilde{T}_2 \in \gamma(U_2), P(T_1, T_2) \)
where \( \tilde{\ } \) is the existential lifting of \( \hat{\ } \) to powersets: \( T \in \hat{T} \iff \exists \hat{T} \in \tilde{T}, T \in \tilde{T} \)

Equivalently: \( \tilde{P}(U_1, U_2) \iff \exists \tilde{T}_1 \in \gamma(U_1), \exists \tilde{T}_2 \in \gamma(U_2), \exists T_1 \in \tilde{T}_1, \exists T_2 \in \tilde{T}_2, P(T_1, T_2) \)

The lifting of a predicate can also be defined in terms of each of the composed interpretations:

The lifting of a type function \( f \) uses the pointwise application of \( f \) to all elements of each subset of a powerset, which we note \( \widetilde{\ } \).

Definition 11 (Function Lifting). \( \widetilde{f} = \alpha \circ \hat{f} \circ \gamma \)

Definition 12 (Consistency). \( U_1 \sim U_2 \) if and only if \( \exists \tilde{T}_1 \in \gamma(U_1), \exists T_1 \in \tilde{T}_1, \exists T_2 \in \gamma(U_2), \exists T_2 \in \tilde{T}_2, P(T_1, T_2) \)

Proposition 9. \( \tilde{P}(U_1, U_2) \iff \exists G_1 \in \gamma_G(U_1), \exists G_2 \in \gamma_G(U_2), \tilde{P}(G_1, G_2) \)
where \( \tilde{P} \) is the predicate \( P \) lifted with \( \gamma \).

Proof. By definition of lifting predicates, \( \tilde{P}(U_1, U_2) = \exists \tilde{T}_1 \in \gamma(U_1), \exists T_1 \in \tilde{T}_1, \exists T_2 \in \gamma(U_2), \exists T_2 \in \tilde{T}_2, P(T_1, T_2) \).

If we unfold \( \tilde{P}(G_1, G_2) \), then \( \exists G_1 \in \gamma_G(U_1), \exists G_2 \in \gamma_G(U_2), \exists T_1 \in \gamma(G_1), \exists T_2 \in \gamma(G_2), P(T_1, T_2) \).

We start with direction \( \Rightarrow \). As \( \gamma = \tilde{\gamma} \circ \gamma_G \), then \( \gamma(U_1) = \tilde{\gamma}(G_1) \) and \( \gamma(U_2) = \tilde{\gamma}(G_2) \). As \( \tilde{T}_1 \in \tilde{\gamma}(G_1) \) then \( T_1 = \gamma(G_1) \) for some \( G_1 \in G_1 \), and also \( \tilde{T}_2 \in \tilde{\gamma}(G_2) \). Then we always choose \( G_1 = G_1 \) and \( G_2 = G_2 \).

Then we prove direction \( \Leftarrow \). As \( G_1 \in \gamma_G(U_1) \) and \( T_1 \in \gamma(G_1) \), then its easy to see that \( T_1 \in (\tilde{\gamma} \circ \gamma_G)(U_1) \) as we know that \( G_1 \in \gamma_G(U_1) \) and \( (\tilde{\gamma} \circ \gamma_G)(U_1) = \mathcal{P} \in \gamma_G(U_1) \bigcup\gamma(G) \). Analogous \( T_2 \in (\tilde{\gamma} \circ \gamma_G)(U_2) \), but \( \gamma = \tilde{\gamma} \circ \gamma_G \) and the result holds.

Proposition 10. \( U_1 \sim U_2 \iff \exists G_1 \in \gamma_G(U_1), \exists G_2 \in \gamma_G(U_2), G_1 \sim G_2 \) where \( \sim \) is the classic consistency operator defined in [2].

Proof. Direct by proposition 9.

When a function \( f \) receives more than one argument, then the lifting is the pointwise application of \( f \) to every combinations of elements of each set of each powerset. Formally:

Definition 13 (Lifting of type functions). Let \( f : \text{TYPE}^n \rightarrow \text{TYPE} \), then \( \tilde{f} : \text{UTYPE}^n \rightarrow \text{UTYPE} \) is defined as:

\[
\tilde{f}(U_1, ..., U_2) = \alpha( \bigcup_{G_1 \in \gamma_G(U_1)} \bigcup_{G_n \in \gamma_G(U_n)} \bigcup_{T_1 \in \gamma(G_1)} \bigcup_{T_n \in \gamma(G_n)} f(T_1, ..., T_n))
\]

\[
\tilde{f}(U_1, ..., U_2) = \alpha(\{ f(T_1, ..., T_n) \mid T_1 \in \gamma(G_1), ..., T_n \in \gamma(G_n) \})
\]

\[
\tilde{f}(U_1, ..., U_2) = \alpha(\{ f(T_1, ..., T_n) \mid T_1 \in \gamma(G_1), ..., T_n \in \gamma(G_n) \})
\]

\[
\tilde{f}(U_1, ..., U_2) = \alpha(\{ f(T_1, ..., T_n) \mid T_1 \in \gamma(G_1), ..., T_n \in \gamma(G_n) \})
\]

\[
\tilde{f}(U_1, ..., U_2) = \alpha(\{ f(T_1, ..., T_n) \mid T_1 \in \gamma(G_1), ..., T_n \in \gamma(G_n) \})
\]
Note that we can also define the lifting of a function using its intermediate lifting:

**Proposition 11.** Let \( \bar{f} : \text{UType}^n \to \text{UType} \) and \( \bar{f}_1 : \text{UType}^n \to \text{UType} \) then,

\[
\bar{f}(U_1, \ldots, U_2) \iff \alpha^n \circ \bar{f}_1 \circ \gamma_\alpha^\beta(U_1, \ldots, U_n) \equiv \alpha^n \{ \{ \bar{f}_1(G_1, \ldots, G_n) \mid G_1 \in \gamma_\beta(U_1), \ldots, G_n \in \gamma_\beta(U_n) \} \}
\]

where \( \bar{f}_1 \) is the pointwise application of \( \bar{f}_1 \), and \( \bar{f} \) is the lifting of \( f \) in the intermediate abstraction.

**Proof.** For simplicity, we will prove it for a function that receives one argument, the general case is analogous.

\[
\bar{f}(U) = \alpha \circ \bar{f} \circ \gamma(U)
\]

\[
= \alpha \circ \bar{f}_1 \circ \gamma \circ \gamma_\beta(U)
\]

\[
= \alpha \circ \bar{f}_1 \circ \bar{f} \circ \gamma(G \mid G \in \gamma_\beta(U))
\]

\[
= \alpha \circ \bar{f}_1 \circ \gamma_\gamma(\{ T \in \gamma(G) \mid G \in \gamma_\beta(U) \})
\]

\[
= \alpha \circ \bar{f}_1(\{ f(T) \in \gamma(G) \mid G \in \gamma_\beta(U) \})
\]

\[
= \alpha \circ \{ \gamma_\beta(U) \} \}
\]

\[
= \alpha \circ \bar{f}_1 \circ \gamma_\beta(U)
\]

**Proposition 12.** Let \( F : \text{TYPE} \to \text{TYPE} \) be a partial function, and define the predicate \( P(T_1, T_2) \equiv T_1 = F(T_2) \). Then \( \hat{P}(U_1, U_2) \) implies \( U_1 \sim \hat{F}(U_2) \).

**Proof.** Suppose \( \hat{P}(U_1, U_2) \). Then \( T_1 = F(T_2) \) for some \( T_1 \in T_1, \hat{T}_1 \in \gamma(U_1) \) and \( T_2 \in \hat{T_2}, \hat{T}_2 \in \gamma(U_2) \). Therefore \( F(T_2) \in \hat{T}_F, \hat{T}_F \in \hat{F}(\gamma(U_2)) \) and by Prop. \( \hat{F}(\gamma(U_2)) \subseteq \gamma(\alpha(\hat{F}(\gamma(U_2)))) \). But \( \hat{F}(U_2) = \alpha(\hat{F}(\gamma(U_2))) \), so \( F(T_2) \in \hat{T}_F, \hat{T}_F \in \gamma(\alpha(\hat{F}(\gamma(U_2)))) = \gamma(\hat{F}(U_2)) \). Then by definition of consistency, we can choose \( T_1, F(T_2) \in (\hat{T}_1, \hat{T}_F), (\hat{T}_1, \hat{T}_F), \in \gamma(U_1, \hat{F}(U_2)) \) such that \( T_1 = F(T_2) \), therefore \( U_1 \sim \hat{F}(U_2) \).

**Proposition 13.** Let \( P(T_1, T_2) \equiv T_1 = \text{dom}(T_2) \). Then \( \sim \text{dom}(U_2) \) implies \( \sim \hat{P}(U_1, U_2) \).

**Proof.** Suppose \( U_1 \sim \text{dom}(U_2) \). Then exists \( T_1 \in \hat{T}_1, \hat{T}_1 \in \gamma(U_1) \) and \( T_2 \in \hat{T}_2, \hat{T}_2 \in \gamma(\text{dom}(U_2)) \) such that \( T_1 = T_2 \), which implies that \( \exists T_2^2 \in \hat{T}_2^2, \hat{T}_2^2 \in \gamma(G_2) \), such that \( T_2 = \text{dom}(T_2^2) \), which is by definition \( \hat{P}(U_1, U_2) \).
Proposition 14. Let \( P(T_1, T_2) \equiv T_1 = \text{dom}(T_2) \). Then \( U_1 \sim \text{dom}(U_2) \) if and only if \( \hat{P}(U_1, U_2) \).


### 3.2.2 Inductive definitions

This section presents inductive definitions of some of the metafunctions presented in the paper.

#### Proposition 15.

<table>
<thead>
<tr>
<th>( U \sim U_1 )</th>
<th>( U \sim U_2 )</th>
<th>( U_1 \sim U )</th>
<th>( U_2 \sim U )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( U \sim U_1 \oplus U_2 )</td>
<td>( U \sim U_1 \oplus U_2 )</td>
<td>( U_1 \oplus U_2 \sim U )</td>
<td>( U_1 \oplus U_2 \sim U )</td>
</tr>
<tr>
<td>( U \sim U )</td>
<td>( ? \sim U )</td>
<td>( U_1 \sim U_1 \oplus U_2 )</td>
<td>( U_2 \sim U_1 \oplus U_2 )</td>
</tr>
</tbody>
</table>

Proof. Straightforward from the definition of consistency.

#### Definition 14 (Gradual Meet).

Let \( \sqcap : \text{UType} \to \text{UType} \) be defined as:

1. \( U \sqcap U = U \)
2. \( ? \sqcap U = U \sqcap ? = U \)
3. \( U \sqcap (U_1 \oplus U_2) = (U_1 \oplus U_2) \sqcap U = \begin{cases} U \sqcap U_1 & \text{if } U \sqcap U_2 \text{ is undefined} \\ U \sqcap U_2 & \text{if } U \sqcap U_1 \text{ is undefined} \\ (U \sqcap U_1) \oplus (U \sqcap U_2) & \text{otherwise} \end{cases} \)
4. \( (U_{11} \to U_{12}) \sqcap (U_{21} \to U_{22}) = (U_{11} \sqcap U_{21}) \to (U_{12} \sqcap U_{22}) \)
5. \( U_1 \sqcap U_2 \) is undefined otherwise.

#### Proposition 16.

\( \sqcap = \alpha \circ \hat{\text{equate}} \circ \gamma \)

Proof. Direct using induction and the definition of meet as intersection of sets of sets.

#### Proposition 17.

<table>
<thead>
<tr>
<th>( U \sqsubseteq U )</th>
<th>( ? \sqsubseteq U )</th>
<th>( U_1 \sqsubseteq U_3 )</th>
<th>( U_2 \sqsubseteq U_4 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( U_1 \sqsubseteq U_2 )</td>
<td>( U_1 \sqsubseteq U_3 )</td>
<td>( U_1 \sqsubseteq U_3 \oplus U_2 )</td>
<td>( U_2 \sqsubseteq U_3 \oplus U_2 \sqsubseteq U_3 )</td>
</tr>
<tr>
<td>( U_1 \sqsubseteq U_2 \oplus U_3 )</td>
<td>( U_1 \sqsubseteq U_3 \oplus U_2 \sqsubseteq U_3 )</td>
<td>( U_2 \sqsubseteq U_3 \oplus U_2 \sqsubseteq U_3 )</td>
<td></td>
</tr>
</tbody>
</table>

Proof. Direct using induction and the definition of the concretization function.
③ ⊢ \(x : \text{Int} \vdash x : \text{Int} \oplus \text{Bool}\)
③ ⊢ \(x : \text{Int} \vdash 1 : \text{Int} \oplus \text{Bool} \sim \text{Int} \sim \text{Int}\)
③ \(x : \text{Int} \vdash (x + 1) : \text{Int}\)
\[\vdash (\lambda x : (\text{Int} \vdash (x + 1)) : (\text{Int} \oplus \text{Bool}) \rightarrow \text{Int}\]

\[\bullet \vdash (\lambda x : (\text{Int} \vdash (x + 1)) : (\text{Int} \oplus \text{Bool}) \rightarrow \text{Int}\]
\[\vdash 1 : \text{Int} \sim \text{Int} \oplus \text{Bool}\]
\[\vdash \text{true} : \text{Bool}\]
\[\text{Bool} \sim \text{Int} \oplus \text{Bool}\]

\[\vdash ((\lambda x : (\text{Int} \vdash (x + 1))) \text{true}) : \text{Int}\]

\[\bullet \vdash (\lambda x : \text{Int} \vdash (x + 1)) : (\text{Int} \oplus \text{Bool}) \rightarrow \text{Int}\]
\[\vdash \text{true} : \text{Bool}\]
\[\text{Bool} \sim \text{Int} \oplus \text{Bool}\]

\[\vdash ((\lambda x : \text{Int} \vdash (x + 1))) \text{true} : \text{Int}\]

\[\vdash (\lambda x : \text{Bool} \vdash (\text{if } x \text{ then } (1 :: \text{Int} \oplus \text{Bool}) \text{ else } (\text{false} :: \text{Int} \oplus \text{Bool}))) : \text{Bool} \rightarrow (\text{Int} \oplus \text{Bool})\]

Fig. 4. Examples of intrinsic type derivations

3.2.3 Examples of type derivations

In this section we present some type derivations examples in Figure 4.

3.3 Dynamic Semantics of GTFL⊕

One of the salient features of the AGT methodology is that it provides a direct dynamic semantics for gradual programs [2], instead of the typical translational semantics through an intermediate cast calculus [5]. The key idea is to apply proof reduction on gradual typing derivations [3]; by the Curry-Howard correspondence, this gives a notion of relation for gradual terms. We call such semantics the reference semantics.

The main insight of AGT is that gradual typing derivations need to be augmented with evidence to support consistent judgments. Evidence reflects the justification of why a given consistent judgment holds. Therefore, the dynamic
semantics mirrors the type preservation argument of the static language, combining evidences at each reduction step in order to determine whether the program can reduce or should halt with a runtime error.

A consistency judgment $U_1 \sim U_2$ is supported by an evidence $\varepsilon$ that denotes the most precise knowledge about $U_1$ and $U_2$ gained by knowing that they are related by consistency. It is written $\varepsilon \vdash U_1 \sim U_2$. In the case of consistency, which is symmetric (as opposed to, say, consistent subtyping), evidence boils down to a single gradual type, i.e. $\varepsilon \in \text{UType}$, which is precisely the least upper bound of both types, i.e. $U_1 \sqcap U_2$ [2]. For instance, $\text{Int} \vdash \text{Int} \oplus \text{Bool} \sim \text{Int}$.

Consider the simple program: $(\lambda x : \text{Int} \oplus \text{Bool}. x + 1) \text{true}$. It is a well-typed gradual program, and its typing derivation includes two consistent judgments: $\text{Bool} \sim \text{Int} \oplus \text{Bool}$ to accept passing $\text{true}$ as argument, and $\text{Int} \oplus \text{Bool} \sim \text{Int}$ to accept using $x$ in the addition. When simplifying the typing derivation itself (replacing the use of the $x$ hypothesis with the typing derivation of the argument) it becomes necessary to combine the two consistent judgments in order to justify the reduction. In general, in the safety proof of the static language, this corresponds to a use of the fact that type equality is transitive. Here, transitivity demands that the respective evidences for the consistent judgments can be combined. In the example, $\text{Int}$ and $\text{Bool}$ cannot be combined (their meet is undefined), therefore the program halts with error.

To formalize this approach while avoiding writing down reduction rules on actual (bi-dimensional) derivation trees, Garcia et al. adopt intrinsic terms [1], which are a flat notation that is isomorphic to typing derivations. Specifically, the typing derivation for the judgment $\Gamma \vdash \bar{t} : U$ is represented by an intrinsic term $\hat{\bar{t}} \in \text{Term}_{U}$. (The reversed hat on $\hat{\bar{t}}$ is meant to suggest the derivation tree.)

To illustrate how intrinsic terms are formed, consider addition and ascription:

$$\begin{align*}
\hat{\bar{t}}_1 \in \text{Term}_{U_1}, & \quad \varepsilon_1 \vdash U_1 \sim \text{Int} \quad \hat{\bar{t}}_2 \in \text{Term}_{U_2}, \quad \varepsilon_2 \vdash U_2 \sim \text{Int} \\
\varepsilon_1 \hat{\bar{t}}_1 + \varepsilon_2 \hat{\bar{t}}_2 \in \text{Term}_{\text{Int}} \\
\hat{\bar{t}} \in \text{Term}_{U}, & \quad \varepsilon \vdash U \sim U' \\
\varepsilon \hat{\bar{t}} :: U' \in \text{Term}_{U'}
\end{align*}$$

The rules describe how a derivation tree for a compound expression is formed from the sub-derivations of the subterms together with the evidences that support the consistency judgments. Note how the involved evidences show up in the term representation. The syntax of intrinsic terms follows the same pattern as that illustrated with addition and ascription. Also, intrinsic values $\hat{\bar{v}}$ can either be simple values $\bar{u}$ or ascribed values $\varepsilon \bar{u} :: U$. With this notational device, the reduction rules on derivation trees can be written as reduction rules on intrinsic terms, possibly failing with an error when combining evidences, for instance:

$$\varepsilon_1 (\varepsilon_2 \bar{v} :: U) \rightarrow_c \begin{cases} (\varepsilon_2 \circ= \varepsilon_1) \bar{v} \\ \text{error} \quad \text{if } (\varepsilon_2 \circ= \varepsilon_1) \text{ is not defined} \end{cases}$$
The definition of consistent transitivity for a type predicate \( P \), \( \circ P \), is given by the abstract interpretation framework \([2]\); in particular, for type equality, \( \circ = \) corresponds to the meet of gradual types \( \sqcap \).

Notice that for convenience, from this point forward we use the notation \( t \in \text{Term}_U \) to refer to an intrinsic term \( \tilde{t} \in \text{Term}_U \), \( u \) to refer to an \( \tilde{u} \), \( v \) to refer to an \( \tilde{v} \), and finally we sometimes omit the type notation in \( t \) when the type is not important in that context. Figure 5 presents the gradual intrinsic terms of \( \text{GTFL}^\oplus \). Figures 6 and 7 present some intrinsic type derivations of the examples presented in Section 3.2.3. Figure 8 presents the syntax and notions of reductions. Figure 9 presents the intrinsic reduction of \( \text{GTFL}^\oplus \).

### 4 Properties of \( \text{GTFL}^\oplus \)

This section presents the proof of the static gradual guarantee in Section 2. Section 4.2 presents the proof of type safety. Finally, Section 4.3 presents the proof of the dynamic gradual guarantee.

#### 4.1 Static Gradual Guarantee

**Proposition 18** (Equivalence for fully-annotated terms).

For any \( t \in \text{Term} \), \( \vdash_S t : T \) if and only if \( \vdash t : T \).

**Proof.** By induction over the typing derivations. The proof is trivial because static types are given singleton meanings via concretization.
Lemma 3. If $\Gamma \vdash \overline{t} : U$ and $\Gamma \sqsubseteq \Gamma'$, then $\Gamma' \vdash \overline{t} : U'$ for some $U \subseteq U'$.

Proof. Simple induction on typing derivations.

Lemma 4. If $U_1 \sim U_2$ and $U_1 \sqsubseteq U_1'$ and $U_2 \sqsubseteq U_2'$ then $U_1' \sim U_2'$.
Proof. By definition of $\sim$, there exists $(T_1, T_2) \in (\tilde{T}_1, \tilde{T}_2) \in \gamma^2(U_1, U_2)$ such that $T_1 = T_2$. $U_1 \subseteq U_1'$ and $U_2 \subseteq U_2'$ mean that $\gamma(U_1) \subseteq \gamma(U_1')$ and $\gamma(U_2) \subseteq \gamma(U_2')$, therefore $(T_1, T_2) \in (\tilde{T}_1, \tilde{T}_2) \in \gamma^2(U_1, U_2)$.

Proposition 19 (Static gradual guarantee). If $\vdash \tilde{t}_1 : U_1$ and $\tilde{t}_1 \subseteq \tilde{t}_2$, then $\vdash \tilde{t}_2 : U_2$, for some $U_2$ such that $U_1 \subseteq U_2$.

Proof. We prove the property on opens terms instead of closed terms: If $\Gamma \vdash \tilde{t}_1 : U_1$ and $\tilde{t}_1 \subseteq \tilde{t}_2$ then $\Gamma \vdash \tilde{t}_2 : U_2$ and $U_1 \subseteq U_2$.

The proof proceed by induction on the typing derivation.

Case $(Ux, Ub)$. Trivial by definition of $\subseteq$ using $(Px), (Pb)$ respectively.

Case $(U\lambda)$. Then $\tilde{t}_1 = (\lambda x : U_1, \tilde{t})$ and $U_1 = U_1' \to U_2'$. By $(U\lambda)$ we know that:

\[
\frac{\Gamma, x : U_1' \vdash \tilde{t} : U_2'}{\Gamma \vdash (\lambda x : U_1', \tilde{t}) : U_1' \to U_2'}
\]

(1)

Consider $\tilde{t}_2$ such that $\tilde{t}_1 \subseteq \tilde{t}_2$. By definition of term precision $\tilde{t}_2$ must have the form $\tilde{t}_2 = (\lambda x : U_1'', \tilde{t}'')$ and therefore

\[
\frac{\tilde{t} \subseteq \tilde{t}'' \quad U_1' \subseteq U_1''}{(\lambda x : U_1', \tilde{t}) \subseteq (\lambda x : U_1'', \tilde{t}'')}
\]

(2)

Using induction hypotheses on the premise of $1 \Gamma, x : U_1' \vdash \tilde{t} : U_2'$ with $U_2' \subseteq U_2''$. By Lemma $\frac{\exists \Gamma, x : U_1' \vdash \tilde{t} : U_2''}{U_2' \subseteq U_2''}$. Then we can use rule $(U\lambda)$ to derive:

\[
\frac{\Gamma, x : U_1'' : \vdash \tilde{t} : U_2''}{\Gamma \vdash (\lambda x : U_1', \tilde{t}'') : U_1'' \rightarrow U_2''}
\]

Where $U_2 \subseteq U_2''$. Using the premise of $2$ and the definition of type precision we can infer that

$U_1' \rightarrow U_1'' \subseteq U_1' \rightarrow U_2''$

and the result holds.

\[\text{Fig. 7. Examples of intrinsic type derivations (part 2)}\]
\[\varepsilon \in \text{Evidence}, \quad \text{et} \in \text{EvTerm}, \quad \text{ev} \in \text{EvValue}, \quad t \in \text{Term}, \]
\[v \in \text{Value}, \quad u \in \text{SimpleValue}, \quad g \in \text{EvFrame}, \quad f \in \text{TmFrame}\]

\[\text{et} ::= \varepsilon \text{t} \]
\[\text{ev} ::= \varepsilon \text{u} \]
\[u ::= x \mid n \mid b \mid \lambda x.t \]
\[\varepsilon \text{u} ::= \text{v} \mid \varepsilon \text{u} ::= \text{U} \]
\[\text{g} ::= \Box + \text{et} \mid \text{ev} + \Box \mid \Box @ \text{et} + \Box @ \Box ::= \text{U} \mid \text{if} \Box \text{then et else et} \]
\[f ::= g[\varepsilon \Box] \]

**Notions of Reduction**

\[\rightarrow_\varepsilon : \text{Term} \times (\text{Term} \cup \{\text{error}\}) \rightarrow \text{EvTerm} \times (\text{EvTerm} \cup \{\text{error}\}) \]

\[\varepsilon_1 n_1 + \varepsilon_2 n_2 \rightarrow n_3 \text{ where } n_3 = n_1 [+] n_2 \]
\[\varepsilon_1 (\lambda x^{U_{11}}.t) @^{U_1} \rightarrow^{U_2} \varepsilon_2 u \rightarrow \begin{cases} \text{icod}(\varepsilon_1) \text{(((} \varepsilon_2 \circ^m \text{idom}(\varepsilon_1) ) u ::= U_{11}) / x^{U_{11}} ) t :: U_2 \\ \text{error} \quad \text{if not defined} \end{cases} \]
\[\text{if } \varepsilon_1 \text{b then } \varepsilon_2 t^{U_2} \text{ else } \varepsilon_3 t^{U_3} \rightarrow \begin{cases} \varepsilon_2 t^{U_2} :: U_2 \cap U_3 \quad \text{b = true} \\ \varepsilon_3 t^{U_3} :: U_2 \cap U_3 \quad \text{b = false} \end{cases} \]
\[\varepsilon_1 (\varepsilon_2 u ::= \text{U}) \rightarrow_c \begin{cases} \varepsilon_2 \circ^m \varepsilon_1 u \\ \text{error} \quad \text{if not defined} \end{cases} \]

**Fig. 8.** Syntax and notions of Reduction

**Case (U+).** Then \( \tilde{t}_1 = \tilde{t}_1^\prime + \tilde{t}_2^\prime \) and \( U_1 = \text{Int} \). By \((U+)\) we know that:
\[
\begin{array}{c}
\Gamma \vdash \tilde{t}_1 : U_1 \\
\Gamma \vdash \tilde{t}_2 : U_2 \\
U_1 \sim \text{Int} \\
U_2 \sim \text{Int}
\end{array}
\]

\[
\Gamma \vdash \tilde{t}_1 + \tilde{t}_2 : \text{Int}
\]

Consider \( \tilde{t}_2 \) such that \( \tilde{t}_1 \subseteq \tilde{t}_2 \). By definition of term precision \( \tilde{t}_2 \) must have the form \( \tilde{t}_2 = \tilde{t}_1^\prime + \tilde{t}_2^\prime \) and therefore
\[
\begin{array}{c}
\tilde{t}_1^\prime \subseteq \tilde{t}_1^\prime \\
\tilde{t}_2^\prime \subseteq \tilde{t}_2^\prime \\
\tilde{t}_1^\prime + \tilde{t}_2^\prime \subseteq \tilde{t}_1^\prime + \tilde{t}_2^\prime
\end{array}
\]

Using induction hypotheses on the premises of \[[B] \Gamma \vdash \tilde{t}_1^\prime : U_1^\prime \) and \( \Gamma \vdash \tilde{t}_2^\prime : U_2^\prime \), where \( U_1 \subseteq U_1^\prime \) and \( U_2 \subseteq U_2^\prime \). By Lemma \[[C] U_1^\prime \sim \text{Int} \) and \( U_2^\prime \sim \text{Int} \). Therefore we can use rule \((U+)\) to derive:
\[
\begin{array}{c}
\Gamma \vdash \tilde{t}_1^\prime : U_1^\prime \\
\Gamma \vdash \tilde{t}_2^\prime : U_2^\prime \\
U_1^\prime \sim \text{Int} \\
U_2^\prime \sim \text{Int}
\end{array}
\]

\[
\Gamma \vdash \tilde{t}_1^\prime + \tilde{t}_2^\prime : \text{Int}
\]

and the result holds.
\[
\begin{align*}
\text{Reduction} & \quad \text{TERM}_U \times (\text{TERM}_U \cup \{\text{error}\}) \\
(R) & \quad t^U \to r \quad r \in (\text{TERM}_U \cup \{\text{error}\}) \\
(Rr) & \quad t^U \to r \\
(Rg) & \quad g[et] \to g[et'] \\
(Rf) & \quad t^U_1 \to t^U_2 \quad f[t^U_1] \to f[t^U_2] \\
(Rerr) & \quad t^U_1 \to \text{error} \\
\end{align*}
\]

Case (Uapp). Then \(\bar{t}_1 = \bar{t}'_1 \bar{t}'_2\) and \(U_1 = U_{12}\). By (Uapp) we know that:

\[
\text{(Uapp)} & \quad \frac{\Gamma \vdash \bar{t}'_1 : U'_1 \quad \Gamma \vdash \bar{t}'_2 : U'_2 \quad U_2 \sim \text{dom}(U'_1)}{\Gamma \vdash \bar{t}_1 \bar{t}_2 : \text{cod}(U'_1)}
\]

Consider \(\bar{t}_2\) such that \(\bar{t}_1 \subseteq \bar{t}_2\). By definition of term precision \(\bar{t}_2\) must have the form \(\bar{t}_2 = t''_1 \bar{t}''_2\) and therefore

\[
\text{(Papp)} & \quad \frac{\bar{t}'_1 \subseteq \bar{t}''_1 \quad \bar{t}'_2 \subseteq \bar{t}''_2 \quad \bar{t}_1' \bar{t}_2' \subseteq \bar{t}_1'' \bar{t}_2''}{t''_1 t''_2 \subseteq \bar{t}''_1 \bar{t}''_2}
\]

Using induction hypotheses on the premises of (Uapp) \(\Gamma \vdash \bar{t}'_1 : U'_1\) and \(\Gamma \vdash \bar{t}'_2 : U'_2\), where \(U'_1 \subseteq U''_1\) and \(U'_2 \subseteq U''_2\). By definition precision (Def. 2) and the definition of \(\text{dom}\), \(\text{dom}(U'_1) \subseteq \text{dom}(U''_1)\) and, therefore by Lemma 4 \(U''_2 \sim \text{dom}(U''_1)\). Also, by the previous argument \(\text{cod}(U'_1) \subseteq \text{cod}(U''_1)\) Then we can use rule (Uapp) to derive:

\[
\text{(Uapp)} & \quad \frac{\Gamma \vdash \bar{t}'_1 : U'_1 \quad \Gamma \vdash \bar{t}'_2 : U'_2 \quad U_2 \sim \text{dom}(U'_1)}{\Gamma \vdash \bar{t}_1 \bar{t}_2 : \text{cod}(U''_1)}
\]

and the result holds.

Case (Uif). Then \(\bar{t}_1 = \text{if } \bar{t}_1' \text{ then } \bar{t}_2' \text{ else } \bar{t}_3'\) and \(U_1 = (U'_2 \cap U'_3)\). By (Uif) we know that:

\[
\text{(Uif)} & \quad \frac{\Gamma \vdash \bar{t}_1' : U'_1 \quad \Gamma \vdash \bar{t}_2' : U'_2 \quad \Gamma \vdash \bar{t}_3' : U'_3}{\Gamma \vdash \text{if } \bar{t}_1' \text{ then } \bar{t}_2' \text{ else } \bar{t}_3' : (U'_2 \cap U'_3)}
\]

Consider \(\bar{t}_2\) such that \(\bar{t}_1 \subseteq \bar{t}_2\). By definition of term precision \(\bar{t}_2\) must have the form \(\bar{t}_2 = t''_1 \bar{t}''_2\) and therefore

\[
\text{(Pif)} & \quad \frac{\bar{t}_1' \subseteq \bar{t}''_1 \quad \bar{t}_1' \subseteq \bar{t}''_1 \quad \bar{t}_2' \subseteq \bar{t}''_2 \quad \bar{t}_2' \subseteq \bar{t}''_2}{\text{if } \bar{t}_1' \text{ then } \bar{t}_2' \text{ else } \bar{t}_1' \text{ else } \bar{t}_2'}
\]
Then we can use induction hypotheses on the premises of [7] and derive:

\[
\frac{\Gamma \vdash \overline{t}_{1}' : U_{1}' \quad \Gamma \vdash \overline{t}_{2}' : U_{2}' \quad \Gamma \vdash \overline{t}_{3}' : U_{3}'}{
\Gamma \vdash \text{if } \overline{t}_{1}' \text{ then } \overline{t}_{2}' \text{ else } \overline{t}_{3}' : (U_{1}' \sqcap U_{2}')} \tag{U\text{if)}
\]

Where \(U_{1}' \sqsubseteq U_{1}''\) and \(U_{2}' \sqsubseteq U_{2}''\). Using the definition of type precision (Def. 2) we can infer that

\[
(U_{1}' \sqcap U_{2}') \sqsubseteq (U_{1}'' \sqcap U_{2}'')
\]

and the result holds.

**Case (U::).** Then \(\overline{t}_{1} = \overline{t} :: U_{1}\). By (U::) we know that:

\[
\frac{\Gamma \vdash \overline{t} : U_{1}' \quad U_{1}' \sim U_{1}}{
\Gamma \vdash \overline{t} :: U_{1}} \tag{9}
\]

Consider \(\overline{t}_{2}\) such that \(\overline{t}_{1} \sqsubseteq \overline{t}_{2}\). By definition of term precision \(\overline{t}_{2}\) must have the form \(\overline{t}_{2} = \overline{t}' :: U_{2}\) and therefore

\[
\frac{\overline{t} \sqsubseteq \overline{t}' \quad U_{1} \sqsubseteq U_{2}}{
\overline{t} :: U_{1} \sqsubseteq \overline{t}' :: U_{2}} \tag{P::)
\]

Using induction hypotheses on the premises of [9] \(\Gamma \vdash \overline{t}' : U_{2}'\) where \(U_{1}' \sqsubseteq U_{2}'\). We can use rule (U::) and Lemma 4 to derive:

\[
\frac{\Gamma \vdash \overline{t}' : U_{2}' \quad U_{2}' \sim U_{2}}{
\Gamma \vdash \overline{t} :: U_{2}} \tag{9}
\]

Where \(U_{1} \sqsubseteq U_{2}\) and the result holds.

### 4.2 Type Safety

In this section we present the proof of type safety for GTFL."
Proof. By induction on the derivation of $t^U$.

**Proposition 20** ($\rightarrow$ is well defined). If $t^U \rightarrow r$, then $r \in \text{CONF}_U \cup \{\text{error}\}$.

Proof. By induction on the structure of a derivation of $t^U \rightarrow r$, considering the last rule used in the derivation.

**Case (I\text{U}+)\.** Then $t^U = \epsilon_1 n_1 + \epsilon_2 n_2$. Then

$$\frac{n_1 \in \text{TERM}_{\text{Int}}}{(\text{I}U^+) \quad \epsilon_1 \vdash \text{Int} \sim \text{Int} \quad n_2 \in \text{TERM}_{\text{Int}} \quad \epsilon_2 \vdash \text{Int} \sim \text{Int}} \quad \epsilon_1 n_1 + \epsilon_2 n_2 \in \text{TERM}_{\text{Int}}$$

Therefore

$$\epsilon_1 n_1 + \epsilon_2 n_2 \rightarrow n_3 \text{ where } n_3 = n_1 \left[+\right] n_2$$

But $n_3 \in \text{TERM}_{\text{Int}}$ and the result holds.

**Case (I\text{U}app)\.** Then $t^U = \epsilon_1 (\lambda x^{U_1} t_1^{U_1}) @^{U_1 \rightarrow U_2} (\epsilon_2 u)$ and $U = U_2$. Then

$$\frac{t_1^{U_1} \in \text{TERM}_{U_1_2}}{(\lambda x^{U_1} t_1^{U_1}) \in \text{TERM}_{U_11 \rightarrow U_12}} \quad \frac{t_2^{U_2} \in \text{TERM}_{U_12}}{\epsilon_1 \vdash U_{11} \rightarrow U_{12} \sim U_1 \rightarrow U_2} \quad \epsilon_2 \vdash U'_2 \sim U_1$$

(lapp)

$$\frac{(\lambda x^{U_1} t_1^{U_1}) @^{U_1 \rightarrow U_2} \epsilon_2 u \in \text{TERM}_{U_2}}{\epsilon_1 (\lambda x^{U_1} t_1^{U_1}) @^{U_1 \rightarrow U_2} \epsilon_2 u \in \text{TERM}_{U_2}}$$

If $\epsilon' = (\epsilon_2 \circ \text{idom}(\epsilon_1))$ is not defined, then $t^U \rightarrow \text{error}$, and then the result holds immediately. Suppose that consistent transitivity does hold, then

$$\epsilon_1 (\lambda x^{U_1} t_1^{U_1}) @^{U_1 \rightarrow U_2} \epsilon_2 u \in \text{TERM}_{U_2} \rightarrow \text{idom}(\epsilon_1) \left(\left[\left(\epsilon' u :: U_{11}\right)/x^{U_1}\right] t\right) :: U_2$$

As $\epsilon_2 \vdash U'_2 \sim U_1$ and by inversion lemma $\text{idom}(\epsilon_1) \vdash U_{11} \sim U_{11}$, then $\epsilon' \vdash U'_2 \sim U_{11}$. Therefore $\epsilon' u :: U_{11} \in \text{TERM}_{U_{11}}$, and by Lemma 6, $t^{U_12} = \left[\left(\epsilon' u :: U_{11}\right)/x^{U_1}\right] U_{12} \in \text{TERM}_{U_{12}}$.

Then

$$\frac{t^{U_{12}} \in \text{TERM}_{U_{12}}}{\text{idom}(\epsilon_1) \vdash U_{12} \sim U_2} \quad \frac{\epsilon_1 \vdash U_{12} \sim U_2}{\epsilon_1 t^{U_{12}} :: U_2 \in \text{TERM}_{U_2}}$$

and the result holds.

**Case (I\text{U}if-true)\.** Then $t^U = \text{if } \epsilon_1 b \text{ then } \epsilon_2 t^{U_2} \text{ else } \epsilon_3 t^{U_3}, U = U_2 \sqcap U_3$ and

$$\frac{b \in \text{TERM}_{U_1}}{\epsilon_1 \vdash U_1 \sim \text{Bool} \quad U = (U_2 \sqcap U_3)} \quad \frac{t_2^{U_2} \in \text{TERM}_{U_2}}{\epsilon_2 \vdash U_2 \sim U} \quad \frac{t_3^{U_3} \in \text{TERM}_{U_3}}{\epsilon_3 \vdash U_3 \sim U}$$

(I\text{Uif})

$$\frac{\text{if } \epsilon_1 b \text{ then } \epsilon_2 t^{U_2} \text{ else } \epsilon_3 t^{U_3} \in \text{TERM}_{U}}{\text{if } \epsilon_1 b \text{ then } \epsilon_2 t^{U_2} \text{ else } \epsilon_3 t^{U_3} \rightarrow \epsilon_2 t^{U_2} :: U_2 \sqcap U_3}$$

Therefore

$$\text{if } \epsilon_1 b \text{ then } \epsilon_2 t^{U_2} \text{ else } \epsilon_3 t^{U_3} \rightarrow \epsilon_2 t^{U_2} :: U_2 \sqcap U_3$$
But
\[
(U::) \quad t^{U_2} \in \text{TERM}_{U_2} \quad \varepsilon_1 \vdash U_2 \sim U_2 \cap U_3 \\
\varepsilon_2 t^{U_2} :: U_2 \cap U_3 \in \text{TERM}_{U_2} \cap U_3
\]
and the result holds.

**Case (IU if-false).** Analogous to case (if-true).

**Proposition 21 (\(\rightarrow\) is well defined).** If \(t^U \rightarrow r\), then \(r \in \text{CONFIG}_U \cup \{\text{error}\}\).

**Proof.** By induction on the structure of a derivation of \(t^U \rightarrow r\).

**Case (R\(\rightarrow\)).** \(t^U \rightarrow r\). By well-definedness of \(\rightarrow\) (Prop 20), \(r \in \text{CONFIG}_U \cup \{\text{error}\}\).

**Case (Rf).** \(t^U = f[t^U_1], f[t^U] \in \text{TERM}_U, t^U_1 \rightarrow t^U_2, t^{U_2} \in \text{TERM}_U, \) and \(f : \text{TERM}_U \rightarrow \text{TERM}_U\). By induction hypothesis, \(t^{U_2} \in \text{TERM}_U\), so \(f[t^{U_2}] \in \text{TERM}_U\).

**Case (Rferr, Rgerr).** \(r = \text{error}\).

**Case (Rg).** \(t^U = g[et], g[t^U] \in \text{TERM}_U, \) and \(g : \text{EvTERM} \rightarrow \text{TERM}_U, \) and \(et \rightarrow e et'\). Then there exists \(U_e, U_x\) such that \(et = e et'\) and \(e \vdash U_e \sim U_x\).

Also, \(t_e = e_v :: U_e, \) with \(v \in \text{TERM}_U\), and \(e_v \vdash U_v \sim U_e\).

We know that \(e_v = e_v \circ^e e_e\) is defined, and \(et = e_v t_e \rightarrow e_v e_v = et'\). By definition of \(\circ^e\) we have \(e_v \vdash U_v \sim U_x\), so \(g[et'] \in \text{TERM}_U\).

Now we can establish type safety: programs do not get stuck, though they may terminate with cast errors. Also the store of a program is well typed.

**Proposition 22 (Type Safety).** If \(t^U \in \text{TERM}_U\) then either \(t^U\) is a value \(v\); \(t^U \rightarrow \text{error}\); or \(t^U \rightarrow t'\) for some term \(t' \in \text{TERM}_U\).

**Proof.** By induction on the structure of \(t^U\).

**Case (Iu,In, Ib, Ix, I\(\lambda\)).** \(t^U\) is a value.

**Case (I::).** \(t^U = \varepsilon_1 t^{U_1} :: U_2, \) and
\[
(I::) \quad t^{U_1} \in \text{TERM}_{U_1} \quad \varepsilon_1 \vdash U_1 \sim U_2 \\
\varepsilon_1 t^{U_1} :: U_2 \in \text{TERM}_{U_2}
\]
By induction hypothesis on \(t^{U_1}\), one of the following holds:

1. \(t^{U_1}\) is a value, in which case \(t^U\) is also a value.
2. \(t^{U_1} \rightarrow r_1\) for some \(r_1 \in \text{TERM}_{U_1} \cup \{\text{error}\}\). Hence \(t^U \rightarrow r\) for some \(r \in \text{CONFIG}_U \cup \{\text{error}\}\) by Prop 21 and either (Rf), or (Rferr).
Case (I/\text{if}). \( t^U = \text{if} \, \varepsilon_1 t^{U_1} \, \text{then} \, \varepsilon_2 t^{U_2} \, \text{else} \, \varepsilon_3 t^{U_3} \) and

\[
\begin{align*}
&\varepsilon_1 t^{U_1} \in \text{TERM}_{U_1} & \varepsilon_1 \vdash U_1 \sim \text{Bool} & U = (U_2 \cap U_3) \\
&\varepsilon_2 t^{U_2} \in \text{TERM}_{U_2} & \varepsilon_2 \vdash U_2 \sim U \\
&\varepsilon_3 t^{U_3} \in \text{TERM}_{U_3} & \varepsilon_3 \vdash U_3 \sim U \\
\text{(I/\text{if})} & \text{if } \varepsilon_1 t^{U_1} \text{ then } \varepsilon_2 t^{U_2} \text{ else } \varepsilon_3 t^{U_3} \in \text{TERM}_{U}
\end{align*}
\]

By induction hypothesis on \( t^{U_1} \), one of the following holds:

1. \( t^{U_1} \) is a value \( u \), then by (R\rightarrow), \( t^U \rightarrow r \) and \( r \in \text{CONFIG}_U \cup \{ \text{error} \} \) by Prop \textbf{21}.
2. \( t^{U_1} \) is an ascribed value \( v \), then, \( \varepsilon_1 t^{U_1} \rightarrow_c et' \) for some \( et' \in \text{EvTERM} \cup \{ \text{error} \} \). Hence \( t^U \rightarrow r \) for some \( r \in \text{CONFIG}_U \cup \{ \text{error} \} \) by Prop \textbf{21} and either (Rg), or (Rgerr).
3. \( t^{U_1} \rightarrow r_1 \) for some \( r_1 \in \text{TERM}_{U_1} \cup \{ \text{error} \} \). Hence \( t^U \rightarrow r \) for some \( r \in \text{CONFIG}_U \cup \{ \text{error} \} \) by Prop \textbf{21} and either (Rf), or (Rferr).

Case (I/\text{app}). \( t^U = (\varepsilon_1 t^{U_1} \, \circ \, U_1 \rightarrow U_2 \, (\varepsilon_2 t^{U_2}) \)

\[
\begin{align*}
&\varepsilon_1 t^{U_1} \in \text{TERM}_{U_1} & \varepsilon_1 \vdash U_1 \rightarrow U_2 \\
&\varepsilon_2 t^{U_2} \in \text{TERM}_{U_2} & \varepsilon_2 \vdash U_2 \sim U_1 \\
\text{(I/\text{app})} & (\varepsilon_1 t^{U_1} \, \circ \, U_1 \rightarrow U_2 \, (\varepsilon_2 t^{U_2}) \in \text{TERM}_{U_2})
\end{align*}
\]

By induction hypothesis on \( t^{U_1} \), one of the following holds:

1. \( t^{U_1} \) is a value \( (\lambda x^{U_1}, t^{U_2}) \) (by canonical forms Lemma \textbf{5}), posing \( U_1 = U'_1 \rightarrow U'_2 \).

Then by induction hypothesis on \( t^{U_2} \), one of the following holds:

(a) \( t^{U_2} \) is a value \( u \), then by (R\rightarrow), \( t^U \rightarrow r \) and \( r \in \text{CONFIG}_U \cup \{ \text{error} \} \) by Prop \textbf{21}.

(b) \( t^{U_2} \) is an ascribed value \( v \), then, \( \varepsilon_2 t^{U_2} \rightarrow_c et' \) for some \( et' \in \text{EvTERM} \cup \{ \text{error} \} \). Hence \( t^U \rightarrow r \) for some \( r \in \text{CONFIG}_U \cup \{ \text{error} \} \) by Prop \textbf{21} and either (Rg), or (Rgerr).

(c) \( t^{U_2} \rightarrow r_2 \) for some \( r_2 \in \text{CONFIG}_U \cup \{ \text{error} \} \). Hence \( t^U \rightarrow r \) for some \( r \in \text{CONFIG}_U \cup \{ \text{error} \} \) by Prop \textbf{21} and either (Rf), or (Rferr).

2. \( t^{U_1} \) is an ascribed value \( v \), then, \( \varepsilon_1 t^{U_1} \rightarrow_c et' \) for some \( et' \in \text{EvTERM} \cup \{ \text{error} \} \). Hence \( t^U \rightarrow r \) for some \( r \in \text{CONFIG}_U \cup \{ \text{error} \} \) by Prop \textbf{21} and either (Rg), or (Rgerr).

3. \( t^{U_1} \rightarrow r_1 \) for some \( r_1 \in \text{CONFIG}_U \cup \{ \text{error} \} \). Hence \( t^U \rightarrow r \) for some \( r \in \text{CONFIG}_U \cup \{ \text{error} \} \) by Prop \textbf{21} and either (Rf), or (Rferr).

Case (I/\text{+}). Similar case to (I/\text{app})

4.3 Dynamic Gradual Guarantee

In this section we present the proof the Dynamic Gradual Guarantee for GTFL\textsuperscript{®}. 
Definition 18 (Intrinsic term precision). Let \( \Omega \in \mathcal{P}(\text{VAR}_* \times \text{VAR}_*) \) be defined as \( \Omega := \{ x^{U_{i1}} \subseteq x^{U_{i2}} \} \) We define an ordering relation \( (\cdot \vdash \cdot \subseteq \cdot) \in (\mathcal{P}(\text{VAR}_* \times \text{VAR}_*) \times \text{TERM}_* \times \text{TERM}_* \) shown in Figure 10.

Definition 19 (Well Formedness of \( \Omega \)). We say that \( \Omega \) is well formed iff \( \forall \{ x^{G_{i1}} \subseteq x^{G_{i2}} \} \in \Omega, G_{i1} \subseteq G_{i2} \)

Before proving the gradual guarantee, we first establish some auxiliary properties of precision. For the following propositions, we assume Well Formedness of \( \Omega \) (Definition 19).

Proposition 23. If \( \Omega \vdash t^{U_1} \subseteq t^{U_2} \) for some \( \Omega \in \mathcal{P}(\text{VAR}_* \times \text{VAR}_*) \), then \( U_1 \subseteq U_2 \).

Proof. Straightforward induction on \( \Omega \vdash t^{U_1} \subseteq t^{U_2} \), since the corresponding precision on types is systematically a premise (either directly or transitively).

Proposition 24. Let \( g_1, g_2 \in \text{EvFrame} \) such that \( g[e_{11}t^{U_{11}}] \in \text{TERM}_{U_{11}'}, g[e_{21}t^{U_{12}}] \in \text{TERM}_{U_{12}'} \), with \( U_{11}' \subseteq U_{12}' \). Then if \( g_1[e_{11}t^{U_{11}}] \subseteq g_2[e_{21}t^{U_{12}}], e_{12} \subseteq e_{22} \) and \( t^{U_1} \subseteq t^{U_2} \), then \( g_1[e_{12}t^{U_{12}}] \subseteq g_2[e_{22}t^{U_{22}}] \)

Proof. We proceed by case analysis on \( g_i \).
Case \(\square @^{U′} et\). Then for \(i \in \{1, 2\}\) \(g_i\) must have the form \(\square @^{U″} ε_{i′} t^{U″}\) for some \(U″_i, ε_{i′}\) and \(t^{U″}\). As \(g_1[ε_{1t^{U_i}}] ⊑ \square_{APP} ε_1 ⊑ ε_2, ε_{i′} ⊑ ε′_2, U″_1 ⊑ U″_2\) and \(t^{U″_1} ⊑ t^{U″_2}\).

As \(ε_1 \sqsubseteq ε_2\) and \(t^{U_1} ⊑ t^{U_2}\), then by \(\square_{APP} ε_{12t^{U_1}} @^{U″_1} ε_{1′} t^{U″_1} ⊑ ε_{22t^{U_2}} @^{U″_2} ε′_2 t^{U″_2}\), and the result holds.

Case \(\square + et, ev + □, ev @^{U′} □, □ :: U, if \square then et else et\). Straightforward using similar argument to the previous case.

**Proposition 25.** Let \(g_1, g_2 \in \text{EvFrame} such that \(g_1[ε_{1t^{U_i}}] \in \text{TERM}_{U′}, g_2[ε_{2t^{U_2}}] \in \text{TERM}_{U′_2}\), with \(U_i' ⊑ U_2'\). Then if \(g_1[ε_{1t^{U_1}}] ⊑ g_2[ε_{2t^{U_2}}]\) then \(t^{U_1} ⊑ t^{U_2}\) and \(ε_1 \sqsubseteq ε_2\).

**Proof.** We proceed by case analysis on \(g_i\).

Case \(\square @^{U′} et\). Then there must exist some \(U″_i, ε_{i′}\) and \(t^{U″}\) such that \(g[ε_{1t^{U_i}}] = ε_{1t^{U_i}} @^{U″_1} ε_{1′} t^{U″_1}\) and \(g[ε_{2t^{U_2}}] = ε_{2t^{U_2}} @^{U″_2} ε′_2 t^{U″_2}\). Then by the hypothesis and the premises of \(\square_{APP}\), \(t^{U_1} ⊑ t^{U_2}\) and \(ε_1 \sqsubseteq ε_2\), and the result holds immediately.

**Proposition 26.** Let \(f_1, f_2 \in \text{EvFrame} such that \(f_1[ε_{1t^{U_1}}] \in \text{TERM}_{U′_1}, f_2[ε_{2t^{U_2}}] \in \text{TERM}_{U′_2}\), with \(U_i' ⊑ U_2'\). Then if \(f_1[ε_{1t^{U_1}}] ⊑ f_2[ε_{2t^{U_2}}]\) and \(t^{U_1} ⊑ t^{U_2}\), then \(f_1[ε_{1t^{U_1}}] ⊑ f_2[ε_{2t^{U_2}}]\)

**Proof.** Suppose \(f_i[ε_{t^{U_i}}] = f_i[ε_{1t^{U_i}}].\) We know that \(g_1[ε_{1t^{U_i}}] \in \text{TERM}_{U′_1}, g_2[ε_{2t^{U_2}}] \in \text{TERM}_{U′_2}\), and \(U_i' ⊑ U_2'\). Therefore if \(g_1[ε_{1t^{U_1}}] \sqsubseteq g_2[ε_{2t^{U_2}}]\), by Prop 25 \(ε_1 \sqsubseteq ε_2\). Finally by Prop 24 we conclude that \(g_1[ε_{1t^{U_1}}] ⊑ g_1[ε_{2t^{U_2}}]\).

**Proposition 27.** Let \(f_1, f_2 \in \text{EvFrame} such that \(f_1[ε_{1t^{U_1}}] \in \text{TERM}_{U′_1}, f_2[ε_{2t^{U_2}}] \in \text{TERM}_{U′_2}\), with \(U_i' ⊑ U_2'\). Then if \(f_1[ε_{1t^{U_1}}] ⊑ f_2[ε_{2t^{U_2}}]\) then \(t^{U_1} ⊑ t^{U_2}\).

**Proof.** Suppose \(f_i[ε_{t^{U_i}}] = f_i[ε_{1t^{U_i}}].\) We know that \(g_1[ε_{1t^{U_i}}] \in \text{TERM}_{U′_1}, g_2[ε_{2t^{U_2}}] \in \text{TERM}_{U′_2}\), and \(U_i' ⊑ U_2'\). Therefore if \(g_1[ε_{1t^{U_1}}] \sqsubseteq g_2[ε_{2t^{U_2}}]\), then using Prop 25 we conclude that \(t^{U_1} ⊑ t^{U_2}\).

**Proposition 28 (Substitution preserves precision).** If \(Ω ∪ \{x^{U_3} ⊑ x^{U_4}\} \vdash t^{U_1} ⊑ t^{U_2} \text{ and } Ω ⊢ t^{U_3} ⊑ t^{U_4}\), then \(Ω ⊢ [t^{U_3/x^{U_3}}] t^{U_1} \sqsubseteq [t^{U_4/x^{U_4}}] t^{U_2}\).

**Proof.** By induction on the derivation of \(t^{U_1} ⊑ t^{U_2}\), and case analysis of the last rule used in the derivation. All cases follow either trivially (no premises) or by the induction hypotheses.
Proposition 29 (Monotone precision for $\circ^\text{=}$. If $\varepsilon_1 \subseteq \varepsilon_2$ and $\varepsilon_3 \subseteq \varepsilon_4$ then $\varepsilon_1 \circ^\text{=} \varepsilon_3 \subseteq \varepsilon_2 \circ^\text{=} \varepsilon_4$.

Proof. By definition of consistent transitivity for $=$ and the definition of precision.

Proposition 30. If $U_{11} \subseteq U_{12}$ and $U_{21} \subseteq U_{22}$ then $U_{11} \cap U_{21} \subseteq U_{12} \cap U_{22}$.

Proof. By induction on the type derivation of the types and meet.

Proposition 31 (Dynamic guarantee for $\rightarrow$). Suppose $\Omega \vdash t_{1}^{U_1} \sqsubseteq t_{2}^{U_2}$. If $t_{1}^{U_1} \rightarrow t_{1}^{U_1'}$ then $t_{1}^{U_1'} \rightarrow t_{2}^{U_2'}$, where $\Omega' \vdash t_{1}^{U_1'} \sqsubseteq t_{2}^{U_2'}$ for some $\Omega' \supseteq \Omega$.

Proof. By induction on the structure of $t_{1}^{U_1} \sqsubseteq t_{2}^{U_2}$. For simplicity we omit the $\Omega \vdash$ notation on precision relations when it is not relevant for the argument.

Case ($\rightarrow +$). We know that $t_{1}^{U_1} = (\varepsilon_1(n_1) + \varepsilon_2(n_2))$ then by $\subseteq_{\text{app}}$ $t_{1}^{U_1'} = (\varepsilon_2(n_1) + \varepsilon_2(n_2))$ for some $\varepsilon_2, \varepsilon_2$ such that $\varepsilon_1 \subseteq \varepsilon_2$ and $\varepsilon_2 \subseteq \varepsilon_2$ . If $t_{1}^{U_1} \rightarrow n_3$ where $n_3 = (n_3 \sqsupseteq n_2)$, then $t_{1}^{U_1'} \rightarrow n_3'$ where $n_3' = (n_3 \sqsupseteq n_2)$ . But $n_3 = n_3'$ and therefore $t_{1}^{U_1} \sqsubseteq t_{2}^{U_2}$ and the result holds.

Case ($\rightarrow \text{app}$). We know that $t_{1}^{U_1} = \varepsilon_1(x_{U_1}^{U_1} \circ_{U_1} t_{U_2}^{U_1} \circ_{U_1} t_{U_1}^{U_1})$ then $\text{app} \subseteq_{\text{app}}$ $t_{U_1}^{U_1}$ must have the form $t_{U_1}^{U_1} = \varepsilon_2(x_{U_1}^{U_1}, t_{U_1}^{U_1}) \circ_{U_1} t_{U_1}^{U_1}$ for some $\varepsilon_2, \varepsilon_3, \varepsilon_4$ and $\varepsilon_2 \subseteq \varepsilon_4$. Let us pose $\varepsilon_2 \subseteq \varepsilon_2 \circ_{\text{app}} \text{app}(\varepsilon_4)$. Then $t_{1}^{U_1} \rightarrow \text{app}(\varepsilon_4) t_{1}^{U_1} :: U_2$ with $t_1^{U_1} = [(\varepsilon_1 n_1 :: U_1)] U_1 t_{U_2}^{U_1}$.

Also, let us pose $\varepsilon_2 \subseteq \varepsilon_2 \circ_{\text{app}} \text{app}(\varepsilon_4)$. Then $t_{1}^{U_1} \rightarrow \text{app}(\varepsilon_4) t_{1}^{U_1} :: U_4$ with $t_1^{U_1} = [(\varepsilon_2 n_2 :: U_2)] U_2 t_{U_2}^{U_1}$.

As $\Omega \vdash t_{1}^{U_1} \sqsubseteq t_{2}^{U_2}$, then $u_1 \subseteq u_2$, $\varepsilon_2 \subseteq \varepsilon_2$ and $\text{app}(\varepsilon_4) \subseteq \text{app}(\varepsilon_4)$ as well, then by Prop $29$ $\varepsilon_1 \subseteq \varepsilon_2$. Then $\varepsilon_1 U_{11} :: \varepsilon_3 U_{21} :: U_{21}$ by $\subseteq$. We also know by $\subseteq_{\text{app}}$ that $\Omega \sqcup \{x_{U_1}^{U_1} \subseteq x_{U_2}^{U_1}\} \vdash t_{U_2}^{U_1} \sqsubseteq t_{U_2}$.

But Substitution preserves precision (Prop $28$) $t_1^{U_1} \subseteq t_2^{U_2}$, therefore $\text{app}(\varepsilon_4) t_1^{U_1} :: U_2 \subseteq \text{app}(\varepsilon_4) t_2^{U_2} :: U_4$ by $\subseteq$. Then $t_{1}^{U_1} \subseteq t_{2}^{U_2}$.

Case ($\rightarrow \text{if-true}$). $t_{1}^{U_1} = \text{if } \varepsilon_1 \text{true then } \varepsilon_2 t_{U_2}^{U_1} \text{ else } \varepsilon_3 t_{U_3}^{U_1}$ then by $\subseteq_{\text{if}}$ $t_{1}^{U_1}$ has the form $t_{1}^{U_1} = \text{if } \varepsilon_2 \text{true then } \varepsilon_2 t_{U_2}^{U_2} \text{ else } \varepsilon_3 t_{U_3}^{U_2}$ for some $\varepsilon_2, \varepsilon_2, t_{U_2}^{U_2}, \varepsilon_2$ and $t_{U_2}^{U_2}$. Then $t_{1}^{U_1} \rightarrow \varepsilon_2 t_{U_2}^{U_1} :: (U_{12} \cap U_{13})$, and $t_{1}^{U_1} \rightarrow \varepsilon_2 t_{U_2}^{U_2} :: (U_{22} \cap U_{23})$.

Using the fact that $t_{1}^{U_1} \subseteq t_{2}^{U_2}$ we know that $\varepsilon_2 \subseteq \varepsilon_2$, $t_{U_2}^{U_2} \subseteq t_{U_2}^{U_2}$ and by Prop $28$ $U_{12} \subseteq U_{22}$ and $U_{13} \subseteq U_{23}$ Therefore by Prop $30$ $(U_{12} \cap U_{13}) \subseteq (U_{22} \cap U_{23})$. Then using $\subseteq_{\text{if}}$, $t_{1}^{U_1} \subseteq t_{2}^{U_2}$.

Case ($\rightarrow \text{if-false}$). Same as case $\rightarrow \text{if-true}$, using the fact that $\varepsilon_1 \subseteq \varepsilon_3$ and $t_{U_1}^{U_1} \subseteq t_{U_2}^{U_2}$.

Proposition 32 (Dynamic guarantee). Suppose $t_{1}^{U_1} \subseteq t_{1}^{U_2}$. If $t_{1}^{U_1} \rightarrow t_{2}^{U_2}$ then $t_{1}^{U_1} \rightarrow t_{2}^{U_2}$ where $t_{2}^{U_1} \subseteq t_{2}^{U_2}$.
Proof. We prove the following property instead: Suppose \( \Omega \vdash t_1^{U_1} \subseteq t_2^{U_2} \). If \( t_1^{U_1} \rightarrow t_2^{U_2} \) then \( t_1^{U_1} \rightarrow t_2^{U_2} \) where \( \Omega' \vdash t_1^{U_1} \subseteq t_2^{U_2} \), for some \( \Omega' \supseteq \Omega \).

By induction on the structure of a derivation of \( t_1^{U_1} \subseteq t_2^{U_2} \). For simplicity we omit the \( \Omega' \vdash \) notation on precision relations when it is not relevant for the argument.

Case \((R\rightarrow)\). \( \Omega \vdash t_1^{U_1} \subseteq t_2^{U_2} \), \( t_1^{U_1} \rightarrow t_2^{U_2} \). By dynamic guarantee of \( \rightarrow \) (Prop 31), \( t_1^{U_1} \rightarrow t_2^{U_2} \) where \( \Omega' \vdash t_1^{U_1} \subseteq t_2^{U_2} \), for some \( \Omega' \supseteq \Omega \). And the result holds immediately.

Case \((Rf)\). \( t_1^{U_1} = f_1[t_1^{U_1}'], t_2^{U_2} = f_2[t_2^{U_2}'] \). We know that \( \Omega \vdash f_1[t_1^{U_1}'] \subseteq f_2[t_2^{U_2}'] \). By using Prop 23, \( U_1' \subseteq U_2' \). By Prop 27, we also know that \( \Omega \vdash t_1^{U_1} \subseteq t_1^{U_1'} \). By induction hypothesis, \( t_1^{U_1'} \rightarrow t_2^{U_2} \), hence \( t_1^{U_1} \rightarrow t_2^{U_2} \), \( \Omega' \vdash t_1^{U_1} \subseteq t_2^{U_2} \) for some \( \Omega' \supseteq \Omega \). Then by Prop 26 then \( \Omega' \vdash f_1[t_1^{U_1}'] \subseteq f_2[t_2^{U_2}'] \) and the result holds.

Case \((Rg)\). \( t_1^{U_1} = g_1[et_1], t_2^{U_2} = g_2[et_2] \), where \( \Omega \vdash g_1[et_1] \subseteq g_2[et_2] \). Also \( et_1 \rightarrow c \epsilon t_1' \) and \( et_2 \rightarrow c \epsilon t_2' \).

Then there exists \( U_1, \epsilon_{11}, \epsilon_{12} \) and \( v_1 \) such that \( et_1 = \epsilon_{11}(\epsilon_{12}v_1 : U_1) \). Also there exists \( U_2, \epsilon_{21}, \epsilon_{22} \) and \( v_2 \) such that \( et_2 = \epsilon_{21}(\epsilon_{22}v_2 : U_2) \). By Prop 25 \( \epsilon_{11} \subseteq \epsilon_{21} \) and by \( (\subseteq_c) \epsilon_{12} \subseteq \epsilon_{22}, v_1 \subseteq v_2 \) and \( U_1 \subseteq U_2 \). Then as \( et_1 \rightarrow_c (\epsilon_{12} \circ^c \epsilon_{11})v_1 \) and \( et_2 \rightarrow_c (\epsilon_{22} \circ^c \epsilon_{21})v_2 \) then, by Prop 29 we know that \( \epsilon_{12} \circ^c \epsilon_{11} \subseteq \epsilon_{22} \circ^c \epsilon_{21} \).

Then using this information, and the fact that \( v_1 \subseteq v_2 \), by Prop 24 it follows that \( \Omega \vdash g_1[et_1'] \subseteq g_2[et_2'] \).

5 Compiling GTFL\(^{\oplus}\) to Threesomes

This section presents the translational semantics of GTFL\(^{\oplus}\). Section 5.1 presents the intermediate language. Section 5.2 presents the cast insertion rules, and Section 5.3 presents the full formalization of the correctness of the translational semantics.

5.1 Intermediate language: GTFL\(^{\oplus}\)\(_{\oplus}\)

Figure 11 presents the syntax of GTFL\(^{\oplus}\)\(_{\oplus}\). Figure 12 presents the full type system of GTFL\(^{\oplus}\)\(_{\oplus}\).

Figure 13 presents the full dynamic semantics of GTFL\(^{\oplus}\)\(_{\oplus}\). Applications of a non-casted function are standard. The reduction rule for additions and conditionals use the \( \text{rval} \) metafunction, which strips away the surrounding cast, if any, to access the underlying value. The reduction of the application of a casted function is standard, splitting the function cast into a cast on the argument and a cast on the result. Two threesomes that coincide on their source/target types are combined by meeting their middle types. If the meet is undefined then the term steps to \text{error}. Otherwise both casts are merged to a new cast where the middle type is now the meet between the middle types. Note that new casts are introduced using the following cast metafunction, which avoids producing useless threesomes:
\[
T \in \text{Type}, \quad x \in \text{Var}, \quad t \in \text{Term}, \quad \Gamma \in \text{Var}^{\text{fin}} \rightarrow \text{Type}
\]

\[
T ::= \text{Bool} \mid \text{Int} \mid T \rightarrow T \quad \text{(types)}
\]

\[
u ::= n \mid b \mid (\lambda x : U.t) \quad \text{(simple values)}
\]

\[
v ::= u \mid (U \Downarrow U)u \quad \text{(values)}
\]

\[
t ::= v \mid x \mid tt \mid t + t \mid \text{if } t \text{ then } t \text{ else } t \mid t : T \mid (U \Downarrow U)t \quad \text{(terms)}
\]

**Fig. 11.** Syntax of the intermediate language

\[
\frac{x : U \in \Gamma}{\Gamma \vdash x : U} \quad \frac{\Gamma \vdash b : \text{Bool}}{\Gamma \vdash \text{dom}(U_1)} \quad \frac{\Gamma \vdash n : \text{Int}}{\Gamma \vdash \text{cod}(U_1)}
\]

\[
\frac{\Gamma, x : U_1 \vdash t : U_2}{\Gamma \vdash (\lambda x : U_1.t) : U_1 \rightarrow U_2}
\]

\[
\frac{\Gamma \vdash U_2 \sim U_1 \sim U_2}{\Gamma \vdash \langle U_2 \Downarrow U_1 \rangle t : U_2}
\]

\[
\frac{\Gamma \vdash \text{Int}}{\Gamma \vdash \text{Int}} \quad \frac{\Gamma \vdash t_1 : \text{Int} \quad \Gamma \vdash t_2 : \text{Int}}{\Gamma \vdash t_1 + t_2 : \text{Int}}
\]

\[
\frac{\Gamma \vdash \text{Int} \quad \Gamma \vdash t_3 : U_2}{\Gamma \vdash \text{if } t_1 \text{ then } t_2 \text{ else } t_3 : U_2}
\]

**Fig. 12.** GTFL\(^{\oplus}\)\(\Rightarrow\) Type system for the intermediate language

\[
\langle \langle U_2 \Downarrow U_1 \rangle \rangle t = \begin{cases} t & \text{if } U_1 = U_2 = U_3 \\ \langle U_2 \Downarrow U_1 \rangle t & \text{otherwise} \end{cases}
\]

### 5.2 Cast Insertion

We now briefly describe the cast insertion translation from a GTFL\(^{\oplus}\) term \(\bar{t}\) to a GTFL\(^{\oplus}\)\(\Rightarrow\) term \(t\). The cast insertion rules are presented in Figure 14. Cast insertion rules use twosomes to ease readability; a twosome \(\langle U_2 \Downarrow U_1 \rangle t\) is equal to \(\langle \langle U_2 \Downarrow U_1 \rangle \rangle t\); the initial middle type is the meet of both ends [4]. Note that useless casts are not introduced by translation due to the use of the cast metafunction.

The key idea of the transformation is to insert casts in places where consistency is used to justify the typing derivation. For instance, if a term \(\bar{t}\) of type \(\text{Int} \oplus \text{Bool}\) is used where an \(\text{Int}\) is required, the translation inserts a cast \(\langle \text{Int} \Downarrow \text{Int} \oplus \text{Bool} \rangle t\), where \(t\) is the recursive translation of \(\bar{t}\). This cast plays...
u ::= true | false | n | λx.t
v ::= u | ⟨U ⊑U⟩u

\begin{align*}
\text{f ::= } & \Box + t \mid v + \Box \mid \Box t \mid v \Box \mid ⟨U \subseteq U⟩ \Box \mid \text{if } \Box \text{ then } t \text{ else } t \text{ (frames)} \\
\text{Notions of Reduction} & \\
\frac{n_3 = \text{rval}(v_1) \left[+\right] \text{rval}(v_2)}{v_1 + v_2 \mapsto n_3} & (\lambda x. t) \mapsto [v/x]t \\
\text{if } v \text{ then } t_1 \text{ else } t_2 \mapsto & \\
\begin{cases} 
  t_2 & \text{if } \text{rval}(v) = \text{true} \\
  t_3 & \text{if } \text{rval}(v) = \text{false} 
\end{cases} & \\
\langle U_{21} \mapsto U_{22} \subseteq U_{11} \mapsto U_{12} \rangle v \mapsto & \\
\langle U_{22} \mapsto U_{21} \subseteq U_{11} \downarrow \downarrow U_{12} \rangle (u \langle U_{11} \downarrow \downarrow U_{21} \rangle v) \\
\langle U_{3} \mapsto U_{2} \downarrow \downarrow U_{1} \rangle v \mapsto & \\
\begin{cases} 
  \langle U_{3} \mapsto U_{2} \downarrow \downarrow U_{1} \rangle v & \\
  \text{error} & \text{if } U_{32} \cap U_{21} \text{ is undefined} 
\end{cases} \\
\text{Reduction} & \\
\frac{t_1 \mapsto t_2}{t_1 \mapsto t_2} & \frac{t_1 \mapsto t_2}{f[t_1] \mapsto f[t_2]} & \frac{f[\text{error}] \mapsto \text{error}}{}
\end{align*}

\begin{figure}
\centering
\begin{tabular}{l}
\textbf{Fig. 13. GTFL} \textit{⊕} \textit{⇒}: Dynamic Semantics of GTFL \textit{⊕} \textit{⇒} \\
\end{tabular}
\end{figure}

the role of the implicit projection from the gradual union type. Dually, when a term of type Int is used where a gradual union is expected, the translation adds a cast that performs the implicit injection to the gradual union, e.g. ⟨Int ⊕ Bool ⇐ Int⟩10. Note that a value with a cast that loses precision is like a tagged value in tagged union type systems; the difference again is that the “tag” is inserted implicitly.

Rule (C::) may insert a cast from the type of the body to the ascribed type. Rule (Capp) may insert two casts. By declaring that the resulting type of the application is \( \tilde{\text{cod}}(U_1) \) and that the argument is consistent with \( \tilde{\text{dom}}(U_1) \), we are implicitly assuming that \( U_1 \) is consistent with some function type, which justifies the cast on \( t_1 \). The second cast on \( t_2 \) comes from the consistent judgment \( U_2 \sim \tilde{\text{dom}}(U_1) \). Rule (C+) is similar.
(Cx)  \[ \frac{x : U \in \Gamma}{\Gamma \vdash x \Rightarrow x : U} \]  (Cb)  \[ \frac{}{\Gamma \vdash b \Rightarrow b : \text{Bool}} \]  (Cn)  \[ \frac{}{\Gamma \vdash n \Rightarrow n : \text{Int}} \]  

(Cλ)  \[ \frac{\Gamma, x : U_1 \vdash t \Rightarrow t' : U_2}{\Gamma \vdash (\lambda x : U_1.t) \Rightarrow (\lambda x : U_1.t') : U_1 \to U_2} \]  

(C::)  \[ \frac{\Gamma \vdash \tilde{t} \Rightarrow t' : U \quad U \sim U_1}{\Gamma \vdash (\tilde{t} :: U_1) \Rightarrow (U_1 \leq U)t' : U_1} \]  

(Capp)  \[ \frac{\Gamma \vdash \tilde{t}_1 \Rightarrow t'_1 : U_1 \quad \Gamma \vdash \tilde{t}_2 \Rightarrow t'_2 : U_2 \quad U_2 \sim \text{dom}(U_1)}{\Gamma \vdash \tilde{t}_1 \tilde{t}_2 \Rightarrow (\text{dom}(U_1) \to \text{cod}(U_1) \leq U_1)t'_1 \quad (\text{dom}(U_1) \leq U_2)t'_2 : \text{cod}(U_1)} \]  

(C+)  \[ \frac{\Gamma \vdash \tilde{t}_1 \Rightarrow t'_1 : U_1 \quad \Gamma \vdash \tilde{t}_2 \Rightarrow t'_2 : U_2 \quad U_1 \sim \text{Int} \quad U_2 \sim \text{Int}}{\Gamma \vdash \tilde{t}_1 + \tilde{t}_2 \Rightarrow (\text{Int} \leq U_1)t'_1 + (\text{Int} \leq U_2)t'_2 : \text{Int}} \]  

(Cif)  \[ \Gamma \vdash \tilde{t}_1 \Rightarrow t'_1 : U_1 \quad \Gamma \vdash \tilde{t}_2 \Rightarrow t'_2 : U_2 \quad \Gamma \vdash \tilde{t}_3 \Rightarrow t'_3 : U_3 \]  

\[ \begin{align*} & \Gamma \vdash \text{if } \tilde{t}_1 \text{ then } \tilde{t}_2 \text{ else } \tilde{t}_3 \Rightarrow \text{if } (\text{Bool} \leq U_1)t'_1 \text{ then } (U_2 \cap U_3 \leq U_2)t'_2 \text{ else } (U_2 \cap U_3 \leq U_3)t'_3 : U_2 \cap U_3 \end{align*} \]

Fig. 14. Cast insertion rules
(b_1, b_2) \in U_0[\text{Bool}] \iff b_1 \in \text{TERM}_{\text{Bool}} \land b_2 : \text{Bool} \land b_1 = b_2

(n_1, n_2) \in U_0[\text{Int}] \iff n_1 \in \text{TERM}_{\text{Int}} \land n_2 : \text{Int} \land n_1 = n_2

(\bar{u}_1, u_2) \in U_k[U_1 \rightarrow U_2] \iff \bar{u}_1 \in \text{TERM}_{U_1 \rightarrow U_2} \land u_2 : U_1 \rightarrow U_2 \land
\forall U'' = U''_1 \rightarrow U''_2. \bar{e}_1 \vdash U_1 \rightarrow U_2 \Rightarrow U''_1 \rightarrow U''_2, \text{ and}
\exists e \vdash U'_1 \sim U''_1, \text{ we have: } \forall j \leq k. (\bar{e}_1, v_2) \in V_j[U'_1],
(\bar{e}_1, u_1) \oplus U''_1 \bar{e}_1, (U'' \triangleleft U_1 \rightarrow U_2)u_2 \langle U''_1 \triangleleft U''_2 \rangle v_2) \in T_j[U''_1]

(\bar{e}_1 :: U, u_2) \in V_k[U] \iff \bar{e}_1 :: U \in \text{TERM}_U \land \epsilon = U \land (\bar{u}_1, u_2) \in U_k[U]

(\bar{e}_1 :: U, (U \triangleleft U')u_2) \in V_k[U] \iff \bar{e}_1 :: U \in \text{TERM}_U \land (\bar{u}_1, u_2) \in U_{k-1}[U']

(\bar{u}_1, u_2) \in V_k[U] \iff (\bar{u}_1, u_2) \in U_k[U]

(\bar{t}_1, t_2) \in T_k[U] \iff \bar{t}_1 \in \text{TERM}_U \land t_2 : U \land \forall j < k
(\bar{t}_1 \rightarrow^j \bar{e}_1 \Rightarrow (t_2 \rightarrow^* v_2 \land (\bar{e}_1, v_2) \in V_{k-j}[U])) \land
(\bar{t}_2 \rightarrow^j \bar{e}_1 \Rightarrow (t_1 \rightarrow^* \bar{e}_1 \land (\bar{e}_1, v_2) \in V_{k-j}[U])) \land
(\bar{t}_1 \rightarrow^j \text{error} \Rightarrow t_2 \rightarrow^* \text{error}) \land
(\bar{t}_2 \rightarrow^j \text{error} \Rightarrow t_1 \rightarrow^* \text{error})

5.3 Correctness of the Translational Semantics

This section presents all the definitions and properties used to prove the correctness of translational semantics.

One of the novelty of this work is to establish that the translational semantics of the gradual language enjoys both type safety and the gradual guarantees, without relying on the usual proof techniques. The typical approach is to prove type safety of a gradual language by first establishing type safety of the target cast calculus and second proving that the cast insertion translation preserves typing. Proving the gradual guarantees is a separate effort [3].

Here, we instead directly establish that the translation semantics is equivalent to the reference semantics derived with AGT. Because the reference semantics describes a type-safe gradual language that satisfies the gradual guarantees, so does the translational semantics.

We establish the equivalence between the semantics using step-indexed: logical relations. We use step-indexed logical relations so the relation is well-founded: the definition without indexes may contain some vicious cycles in presence of gradual unions. Equivalence between two terms is acknowledged when either both evaluate to the same value, or both lead to an error.

Figure 15 presents the logical relations between simple values, values and computations, which are defined mutually recursively. The logical relations are defined for pairs composed of an intrinsic term \( \bar{t} \), which denotes the typing derivation for a GTFL\( ^{10} \) term \( \bar{t} \), and a GTFL\( ^{10} \) term \( t \). For simplicity, we write \( t : U \) for \( t \vdash U \).

A pair of simple values \((\bar{u}_1, u_2)\) are related for \( k \) steps at type \( U \), notation \((\bar{u}_1, u_2) \in U_k[U]\), if they both have the same type \( U \) and, if \( U \) is either \text{Bool}\( \), \text{Int}\( \), or \text{Bool}\( \rightarrow \text{Int}\(\)
or `Int`, then the values are also equal. If the simple values are functions, then they are related if their application to related arguments, for \( j \leq k \) steps, yields `related computations`, as explained below. Note that the relation between simple values need not consider the case of gradual types, as no literal values have gradual types.

A pair of values \((\tilde{v}_1, v_2)\) are related for \(k\) steps at type \(U\), notation \((\tilde{v}_1, v_2) \in \mathcal{V}_k[U]\), if both have the same type and their underlying simple values are related.

One important point to notice is that we may only relate an ascribed value \(\varepsilon \tilde{u}_1 :: U\) to a simple value \(u_2\) if we do not learn anything new from the ascription, \(i.e.\) both the type of \(\tilde{u}_1\) and the evidence \(\varepsilon\) are \(U\). This corresponds to the case where the reference semantics carries useless evidence—recall that the cast insertion translation does not insert useless casts. Additionally, an ascribed value \(\varepsilon \tilde{u}_1 :: U\) is related to a casted value if the evidence and ascription correspond to the threesome. More precisely, the evidence \(\varepsilon\) must be exactly the middle type of the threesome, and the source and target types of the threesome must correspond to the type of \(\tilde{u}_1\) and the ascribed type \(U\), respectively. Finally, in order to reason about the underlying simple values, the ascription and cast must be eliminated by combining them with an evidence and a cast respectively. Because of this extra step, the underlying simple values must be related for \(k - 1\) steps instead.

A pair of terms \((\tilde{t}_1, t_2)\) are related computations for \(k\) steps at type \(U\), notation \((\tilde{t}_1, t_2) \in \mathcal{T}_k[U]\), if both terms have the same type \(U\), then either both terms reduce to related values at type \(U\), or both terms reduce to an error. Formally, for any \(j < k\), if the evaluation of the intrinsic term \(\tilde{t}_1\) terminates in a value \(v_1\) at least in \(j\) steps, then the compiled term \(t_2\) also reduces to a value \(v_2\), and the resulting values are related values for \(k - j\) steps at type \(U\). Analogously, if the evaluation of the compiled term \(t_2\) reduces to a value \(v_2\) at least in \(j\) steps, then the intrinsic term \(\tilde{t}_1\) also reduces to a related value \(v_1\). Finally, if either term reduces to an error in at least \(j\) steps, then the other also reduces to an error. Note that this last condition is only required because we do not assume type safety of GTFL\(^\oplus\).

Armed with these logical relations we can state the notion of semantic equivalence between a GTFL\(^\oplus\) intrinsic term and a GTFL\(^\oplus\) term.

**Definition 20 (Semantic equivalence).** Let \(\tilde{t} \in \text{TERM}\_U\), \(\Gamma = \text{FV}(\tilde{t})\) and a GTFL\(^\oplus\) term \(t\) such that \(\Gamma \vdash t : U\). We say that \(\tilde{t}\) and \(t\) are semantically equivalent, notation \(\tilde{t} \approx t : U\), if and only if for any \(k \geq 0\), \((\sigma_1, \sigma_2) \in \mathcal{G}_k[\Gamma]\), we have \((\sigma_1(\tilde{t}), \sigma_2(t)) \in \mathcal{T}_k[U]\).

The definition of semantic equivalence appeals to the notion of related substitutions. Two substitutions \(\sigma_1\) and \(\sigma_2\) are related for \(k\) steps at type environment \(\Gamma\), notation \((\sigma_1, \sigma_2) \in \mathcal{G}_k[\Gamma]\), if they map each variable in \(\Gamma\) to related values (full definition in 5.3).

Note that we write \(\tilde{t}\) instead of \(t^U\) when it is clear from the context that it is an intrinsic term. Also note that \(t : U \equiv \vdash t : U\).
Definition 21. Let $\sigma$ be a substitution and $\Gamma$ a type substitution. We say that substitution $\sigma$ satisfy environment $\Gamma$, written $\sigma \models \Gamma$, if and only if $\mathrm{dom}(\sigma) = \mathrm{dom}(\Gamma)$.

Definition 22 (Related substitutions). Let $\sigma_1$ be a substitution function from intrinsic variables to intrinsic values, and let $\sigma_2$ be a substitution function from variables to values from the intermediate language. Then we define related substitution as follows:

$$(\sigma_1, \sigma_2) \in \mathcal{G}_k[I] \iff \sigma_i \models \Gamma \land \forall x \in \Gamma. (\sigma_1(x^\Gamma(x)), \sigma_2(x)) \in \mathcal{V}_k[I(x)]$$

Lemma 7 (Reduction preserves relations). Consider $\Gamma \vdash \tilde{t} : U$, $\tilde{t}^U \in \mathrm{TERM}_U$ and $\Gamma \vdash \tilde{t} \Rightarrow t : U$. Consider $k, j > 0$, if $t^U \rightarrow^j v^U$ and $t \rightarrow^j t'$, then we have $(t^U, t) \in \mathcal{T}_k[U]$ if and only if $(v^U, t') \in \mathcal{T}_{k-j}[U]$.

Proof. The $\Rightarrow$ direction relies on the determinism of the reduction relation and the definition of related computations. The $\Leftarrow$ direction follows direct from the definition of $(t^U, t) \in \mathcal{T}_k[U]$ and transitivity of $\rightarrow$.

Lemma 8. If $(\tilde{t}_1, t_2) \in \mathcal{T}_k[U]$ then if $\varepsilon \vdash U \sim U'$, then $(\varepsilon \tilde{t}_1 :: U', (U' \triangleleft U)t_2) \in \mathcal{T}_{k+1}[U']$

Proof. If either term reduce to an error then the lemma trivially holds. If either one of the term reduce to a value, then it holds by definition of related values and Lemma 7.

Lemma 9. Consider $k > 0$. If $(\tilde{t}_1, t_2) \in \mathcal{T}_k[U]$ then $(\tilde{t}_1, t_2) \in \mathcal{T}_{k-1}[U]$.

Proof. Trivial by definition of related computations, as $(\tilde{t}_1, t_2) \in \mathcal{T}_k[U]$ is a stronger property than $(\tilde{t}_1, t_2) \in \mathcal{T}_{k-1}[U]$.

Finally, semantic equivalence between the reference and the translational semantics says that given a well-typed term $\tilde{t}$ from the gradual source language, its corresponding intrinsic term $\tilde{t}$ is semantically equivalent to the cast calculus term $t$ obtained after the cast insertion translation.

Proposition 33 (Equivalence of reference and translational semantics). If $\Gamma \vdash \tilde{t} : U$, represented as the intrinsic term $\tilde{t} \in \mathrm{TERM}_U$, and $\Gamma \vdash \tilde{t} \Rightarrow t : U$, then $\tilde{t} \approx t : U$.

We open the proposition to prove this instead:

If $\Gamma \vdash \tilde{t} : U$, $\tilde{t}^U \in \mathrm{TERM}_U$, $\Gamma \vdash \tilde{t} \Rightarrow t : U$, then $\forall k \geq 0, (\sigma_1, \sigma_2) \in \mathcal{G}_k[I], (\sigma_1(t^U), \sigma_2(t)) \in \mathcal{T}_k[I]$.

Proof. By induction on the type derivation of $\tilde{t}$.
Case \((Ub)\). Then \(\bar{t} = b\) and therefore:

\[
\begin{align*}
(Ub) \quad & \Gamma \vdash b : \mathsf{Bool} \\
\end{align*}
\]

where \(U = \mathsf{Bool}\). Then the corresponding intrinsic term is:

\[
\begin{align*}
(Ub) \quad & b \in \text{TERM}_{\mathsf{Bool}}
\end{align*}
\]

and the type derivation of the compiled term is:

\[
\begin{align*}
(ITb) \quad & \Gamma \vdash b : \mathsf{Bool}
\end{align*}
\]

But \(\sigma_1(b) = b\), \(\sigma_2(b) = b\), and \(b = b\) and the result holds immediately.

Case \((Un)\). Then \(\bar{t} = n\) and therefore:

\[
\begin{align*}
(Un) \quad & \Gamma \vdash n : \mathsf{Int}
\end{align*}
\]

where \(U = \mathsf{Int}\). Then the corresponding intrinsic term is:

\[
\begin{align*}
(Un) \quad & n \in \text{TERM}_{\mathsf{Int}}
\end{align*}
\]

and the type derivation of the compiled term is:

\[
\begin{align*}
(ITn) \quad & \Gamma \vdash n : \mathsf{Int}
\end{align*}
\]

But \(\sigma_1(n) = n\), \(\sigma_2(n) = n\), and \(n = n\) and the result holds immediately.

Case \((Ux)\). Then \(\bar{t} = x\) and therefore:

\[
\begin{align*}
(Ux) \quad & x : U \in \Gamma
\end{align*}
\]

Then the corresponding intrinsic term is:

\[
\begin{align*}
(Ux) \quad & x^U \in \text{TERM}_U
\end{align*}
\]

and the type derivation of the compiled term is:

\[
\begin{align*}
(ITx) \quad & x : U \in \Gamma
\end{align*}
\]

As \((\sigma_1, \sigma_2) \in \mathcal{G}_k[\Gamma]\) and \(x \in \text{dom}(\Gamma)\), then \((x^U, x) \in \mathcal{V}_k[\mathcal{U}]\) and the result holds immediately.

Case \((U\lambda)\). Then \(\bar{t} = (\lambda x : U_1.\bar{t}_2)\) and therefore:

\[
\begin{align*}
(U\lambda) \quad & \Gamma, x : U_1 \vdash \bar{t}_2 : U_2 \\
\end{align*}
\]

where \(U = U_1 \rightarrow U_2\). Then the corresponding intrinsic term is:

\[
\begin{align*}
(U\lambda) \quad & \bar{t}_2^{U_2} \in \text{TERM}_{U_2}
\end{align*}
\]

\[
\begin{align*}
(U\lambda) \quad & \bar{t}_2^{U_2} \in \text{TERM}_{U_1 \rightarrow U_2}
\end{align*}
\]
prove that:

\[ \Gamma, x : U_1 \vdash \bar{t}_2 : U_2 \]

\[ \Gamma \vdash (\lambda x : U_1. t_2) : U_1 \rightarrow U_2 \]

where \( \Gamma, x : U_1 \vdash \bar{t}_2 \Rightarrow t'_2 : U_2 \). Consider \( j \leq k, U' = U'' \Rightarrow U''_1, \varepsilon \vdash \Gamma \rightarrow U_2 \sim U'' \Rightarrow U''_1, \varepsilon_2 \vdash U_1' \sim U''_1, \bar{v}_1' \), and \( \bar{v}_2' \), such that \( (v'_1, v'_2) \in V_j[U''_1] \). We have to prove that:

\[(\varepsilon)(\lambda x^{U_1}. \sigma_1(t'_2)) \bar{U} \varepsilon_2 \bar{v}_1', (U'=U_2) (\lambda x : U_1. \sigma_2(t_2)) \bar{U} \varepsilon U''_1 \bar{v}_2') \in \mathcal{T}[U''_2] \]

Then we proceed depending on the structure of \( (v'_1, v'_2) \), but ultimately we converge to analogous cases where the argument are just related simple values.

1. If \( (v'_1, v'_2) = (\bar{u}'_1, \bar{u}'_2) \in \mathcal{V}_k[U''_1] \), then \( (\bar{u}'_1, \bar{u}'_2) \in \mathcal{U}_k[U''_1] \). Therefore

\[ \langle U' \varepsilon_2 \bar{U} U_2 \rangle = \langle U_1 \rightarrow U_2 \rangle (\lambda x : U_1. \sigma_2(t_2)) \bar{U} \varepsilon U''_1 \bar{v}_2' \]

(a) If \( \varepsilon_2 \circ \varepsilon = idom(\varepsilon_1) \) is not defined, then

\[ \varepsilon_2(\lambda x^{U_1}. \sigma_1(t'_2)) \bar{U} \varepsilon_2 \bar{u}_1' \rightarrow \text{error} \]

But by definition of consistent transitivity \( \varepsilon_2 \cap idom(\varepsilon_1) = \emptyset \) and therefore

\[ \langle U' \varepsilon_2 \bar{U} U_1 \rightarrow U_2 \rangle (\lambda x : U_1. \sigma_2(t_2)) \bar{U} \varepsilon U''_1 \bar{v}_2' \rightarrow \text{error} \]

and the result holds.

(b) If \( \varepsilon' = \varepsilon_2 \circ \varepsilon = idom(\varepsilon_1) \) is defined, then

\[ \varepsilon_1(\lambda x^{U_1}. \sigma_1(t'_2)) \bar{U} \varepsilon_2 \bar{u}_1' \]

\[ \rightarrow \text{icod}(\varepsilon_1)([\varepsilon' \bar{u}_1' :: U_1/x^{U_1}] \sigma_1(t'_2)) :: U''_2 \]

\[ = \text{icod}(\varepsilon_1)(\sigma_1[x^{U_1} \mapsto \varepsilon' \bar{u}_1'] :: U_1(t'_2)) :: U''_2 \]

and, let us suppose than \( \neg (U' = U'' = \varepsilon') \) (the other case is similar modulo one step of evaluation)

\[ \langle U' \varepsilon_2 \bar{U} U_1 \rightarrow U_2 \rangle (\lambda x : U_1. \sigma_2(t_2)) \bar{U} \varepsilon U''_1 \bar{v}_2' \]

\[ \rightarrow \text{icod}(\varepsilon_1)(U_2)(\sigma_1[x^{U_1} \mapsto \varepsilon' \bar{u}_1'] :: U_1 \rightarrow U''_1 \bar{v}_2') \]

\[ = \langle U'' \varepsilon_2 \bar{U} U_2 \rangle \bar{U} \sigma_2(x \mapsto \sigma_2(t_2)) \]

As \( (\bar{u}'_1, \bar{u}'_2) \in \mathcal{U}_k[U''_1] \) then by definition of related values,

\[ (v' \bar{u}_1' :: U_1, (U' \varepsilon_2 \bar{U} U_2) \bar{v}_2') \in \mathcal{V}_j[[U]] \]

Then by Lemma \( [9] \), \( (\varepsilon' \bar{u}_1' :: U_1, \sigma_1[x^{U_1} \mapsto \varepsilon' \bar{u}_1'] :: U_1 \rightarrow U''_1 \bar{v}_2') \in \mathcal{V}_j[[U]] \)

Therefore by definition of related substitutions, \( (\sigma_1[x^{U_1} \mapsto \varepsilon' \bar{u}_1'] :: U_1, \sigma_2[x \mapsto \bar{v}_2'] \in \mathcal{V}_j[[U]] \)

and by induction hypothesis on pair \( (t''_2, \Gamma, x : U_1 \vdash \bar{t}_2 : U_2) \)

\[ ((\sigma_1[x^{U_1} \mapsto \varepsilon' \bar{u}_1'] :: U_1)(t''_2)), \sigma_2[x \mapsto \sigma_2(t_2)] \in \mathcal{T}[U_2] \]

and the result holds by Lemma \( [7] \) and backward preservation of the relations (Lemma \( [7] \)).
2. If $\langle v_1', v_2' \rangle = (\varepsilon u_1' :: U_1', u_2') \in \mathcal{V}_j[U_1']$, then $\varepsilon = U_1'$ and $(u_1', u_2') \in \mathcal{U}_j[U_1']$.

Then $\varepsilon_2' = \varepsilon \circ \varepsilon_2$ is defined because $U_1' \sim U_1''$, and therefore:

$\varepsilon_1(\lambda x^{U_1}.\sigma_1(U_2')) \circ U'' \varepsilon_2 u_1' \rightarrow \varepsilon_1(\lambda x^{U_1}.\sigma_1(U_2')) \circ U'' \varepsilon_2' u_1'$. Then we proceed analogous to (1) and the result holds.

3. If $\langle v_1', v_2' \rangle = (\varepsilon u_1' :: U_1', (U_1' \triangleleft U') u_2') \in \mathcal{V}_j[U_1']$, then $(u_1', u_2') \in \mathcal{U}_j[U''']$, for some $U'$ such that $\varepsilon \vdash U' \sim U_1'$.

(a) If $\varepsilon \circ \varepsilon_2$ is not defined then $\varepsilon \cap \varepsilon_2 = \emptyset$,

$\varepsilon_1(\lambda x^{U_1}.\sigma_1(U_2')) \circ U'' \varepsilon_2 u_1' :: U_1' \rightarrow \textbf{error}$ and

$\langle U' \triangleleft U_1 \rightarrow U_2 \rangle (\lambda x : U_1.\sigma_2(t_2)) \langle U_1' \triangleleft U_1' \rangle \langle U_1' \triangleleft U' \rangle u_2' \rightarrow \textbf{error}$, and the result holds.

(b) If $\varepsilon_2' = \varepsilon \circ \varepsilon_2$ is defined then

$\varepsilon_1(\lambda x^{U_1}.\sigma_1(U_2')) \circ U'' \varepsilon_2 u_1' :: U_1' \rightarrow \varepsilon_1(\lambda x^{U_1}.\sigma_1(U_2')) \circ U'' \varepsilon_2' u_1'$

and we proceed analogous to (1) and the result holds.

Case $(U : ::)$. Then $t_1 :: U$ and therefore:

$\begin{align*}
(U : ::) & \quad \Gamma \vdash t_1 : U' \\
\Gamma \vdash t_1 :: U & \quad U \\
\end{align*}$

Then the corresponding non ascribed intrinsic term is:

$\begin{align*}
(\varepsilon_1(\lambda x^{U_1}.\sigma_1(U_2')) \circ U'' \varepsilon_2 u_1') :: U_1' & \quad \varepsilon \vdash U' \sim U \\
\varepsilon_1(\lambda x^{U_1}.\sigma_1(U_2')) \circ U'' \varepsilon_2 u_1' & \quad \varepsilon_1(\lambda x^{U_1}.\sigma_1(U_2')) \circ U'' \varepsilon_2 u_1' \\
\end{align*}$

Let us assume $U' \neq U$ (the other case is analogous). The type derivation of the compiled term is:

$\begin{align*}
(IT<>) & \quad \Gamma \vdash t_1' : U' \\
\Gamma \vdash (U \triangleleft U') t_1' & \quad \varepsilon_1(\lambda x^{U_1}.\sigma_1(U_2')) \circ U'' \varepsilon_2 u_1' \\
\end{align*}$

Then we have to prove that

$(\varepsilon_1(\lambda x^{U_1}.\sigma_1(U_2')) :: U, (U \triangleleft U') \sigma_2(t_1')) \in \mathcal{T}_k[U']$

By induction hypotheses on $\tilde{t}_1$ ($\sigma_1(\lambda x^{U_1}.\sigma_2(t_1')) \in \mathcal{T}_k[U']$). If either term reduces to an error in less than $k$ steps, then the result holds immediately. The interesting case if they reduce to related values in less than $k$ steps. Then suppose $\sigma_1(\lambda x^{U_1}.\sigma_2(t_1')) \rightarrow^j \tilde{v}_1$, $\sigma_2(t_1') \rightarrow^* v_1'$, where $j < k$ ($\tilde{v}_1, v_1'$) $\in \mathcal{V}_{k-j}[U_1]$.

Let us assume $\tilde{v}_1 = \tilde{u}_1$ then $v_1' = u_1'$ (if they are ascribed values, then the argument is similar modulo one extra step of evaluation, where a runtime error may be produced).

$\varepsilon_1(\lambda x^{U_1}.\sigma_1(U_2')) :: U \rightarrow^3 \varepsilon \tilde{u}_1 :: U$
and
\[
(U \triangleq U') \sigma_2(t'_1) \rightarrow^j (U \triangleq U') u'_1.
\]

We need to prove that
\[
(\varepsilon \bar{u}_1 :: U, (U \triangleq U') u'_1) \in \mathcal{V}_{k-j}[U]
\]
but \((\tilde{v}_1, v'_1) \in \mathcal{V}_{k-j}[U_1]\) and by Lemma 9 \((\tilde{v}_1, v'_1) \in \mathcal{V}_{k-j-1}[U_1]\), and the result holds by backward preservation lemma.

**Case (U app).** Then \(\bar{t} = \bar{t}_1 \bar{t}_2\) and therefore:

\[
\begin{array}{c}
(U_{\text{app}}) \\
\frac{\Gamma \vdash \tilde{t}_1 : U_1 \quad \Gamma \vdash \tilde{t}_2 : U_2 \quad U_2 \sim \text{dom}(U_1)}{\Gamma \vdash \bar{t}_1 \bar{t}_2 : \text{cod}(U_1)}
\end{array}
\]

and \(U = \text{cod}(U_1)\). Then the corresponding intrinsic term is:

\[
(U_{\text{app}}) \\
\frac{t^{U_1} \in \text{TERM}_{U_1} \quad \varepsilon_1 \vdash U_1 \sim U_{11} \rightarrow U_{12} \quad t^{U_2} \in \text{TERM}_{U_2} \quad \varepsilon_2 \vdash U_2 \sim U_{11}}{(\varepsilon_1 t^{U_1}) @ t^{U_1 \rightarrow U_{12}} (\varepsilon_2 t^{U_2}) \in \text{TERM}_{U_{12}}}
\]

where \(U_{11} = \text{dom}(U_1)\) and \(U_{12} = \text{cod}(U_1)\).

We proceed assuming that the compilation always inserts casts (the other cases are similar because then the evidences are equal to the types in the judgment. Therefore the next combinations of those evidences are redundant and never fails). Then suppose \(U_1 \neq U_{11} \rightarrow U_{12}\) and \(U_2 \neq U_{11}\). As \(\varepsilon_1 = U_1 \cap U_{11} \rightarrow U_{12}\), and \(\varepsilon_2 = U_2 \cap U_{11}\), the type derivation of the compiled term is:

\[
(U_{\text{app}}) \\
\frac{\Gamma \vdash \bar{t}_1 : U_1 \quad \Gamma \vdash \bar{t}_2 : U_{11}}{\Gamma \vdash \langle U_{11} \rightarrow U_{12} \triangleq U_1 \bar{t}_1 \rangle (U_{11} \triangleq U_2 \bar{t}_2) : U_{12}}
\]

Then we have to prove that
\[
((\varepsilon_1 \sigma_1(t^{U_1})) @ t^{U_1 \rightarrow U_{12}} (\varepsilon_2 \sigma_2(t^{U_2})), (U_{11} \rightarrow U_{12} \triangleq U_1 \sigma_1(t'_1)) \langle U_{11} \triangleq U_2 \sigma_2(t'_2) \rangle) \in \mathcal{T}_k[U_{12}]
\]

By induction hypotheses on \(\bar{t}_1\) and \(\bar{t}_2\) \((\sigma_1(t^{U_1}), \sigma_2(t'_1)) \in \mathcal{T}_k[U_1]\) and \((\sigma_1(t^{U_2}), \sigma_2(t'_2)) \in \mathcal{T}_k[U_2]\). If either term reduces to an error in less than \(k\) steps, then the result holds immediately. The interesting case if they reduce to related values in less than \(k\) steps. Then suppose \(\sigma_1(t^{U_1}) \rightarrow^j \tilde{v}_1\), \(\sigma_1(t^{U_2}) \rightarrow^j \tilde{v}_2\), \(\sigma_2(t'_1) \rightarrow^* v'_1\), \(\sigma_2(t'_2) \rightarrow^* v'_2\), where \(j < k\) \((\tilde{v}_1, v'_1) \in \mathcal{V}_{k-j}[U_1]\) and \((\tilde{v}_2, v'_2) \in \mathcal{V}_{k-j}[U_2]\). If \(\tilde{v}_1 = \bar{u}_1\) then \(v'_1 = u'_1\), by canonical forms the simple values must be lambdas and the proof follows from Case(U app). If \(\tilde{v}_1 = \varepsilon_1 \bar{u}_1 :: U_1\) and \(\bar{u}_1 \in \text{TERM}_{U_1}\), then suppose \(v'_1 = \langle U_1 \triangleq U'_1 \rangle u'_1\) (the other case is similar but the evidence combination never fails). Also \((\tilde{u}_1, u'_1) \in \mathcal{V}_{k-j-1}[U'_1]\). Suppose \(\varepsilon'_1 \circ \varepsilon_1\) is not defined (which is equivalent to \(\varepsilon'_1 \cap \varepsilon_1 = \emptyset\)), therefore

\[
(\varepsilon_1 \varepsilon'_1 \bar{u}_1 :: U_1) @ t^{U_{11} \rightarrow U_{12}} (\varepsilon_2 v_2) \rightarrow \text{error} \iff \langle U_{11} \rightarrow U_{12} \triangleq U_1 \rangle (U_1 \triangleq U'_1) u'_1 \langle U_{11} \triangleq U_2 \rangle v'_2 \rightarrow \text{error}
\]
and the result follows. Suppose \( \varepsilon''_1 = \varepsilon'_1 \circ \varepsilon_1 \) is defined. Then

\[
\langle U_{11} \rightarrow U_{12} \triangleq U_1 \rangle \langle U_1 \triangleright U_1' \rangle u_1 \langle U_{11} \triangleright U_2 \rangle v_2 \rightarrow
\]

which is exactly the definition of related functions and then the result holds by backward preservation of the relations (Lemma 7) and Lemma 9.

Case (U if). Then \( t = \bar{t}_1 \bar{t}_2 \) and therefore:

\[
\begin{align*}
\text{(U if) } & \quad \Gamma \vdash \bar{t}_1 : U_1 \quad U_1 \sim \text{Bool} \quad \Gamma \vdash \bar{t}_2 : U_2 \quad \Gamma \vdash \bar{t}_3 : U_3 \\
& \quad \Gamma \vdash \text{if } \bar{t}_1 \text{ then } \bar{t}_2 \text{ else } \bar{t}_3 : U_2 \cap U_3
\end{align*}
\]

and \( U = U_2 \cap U_3 \). Then the corresponding intrinsic term is:

\[
\begin{align*}
\text{(U if) } & \quad t^{U_1} \in \text{TERM}_{U_1} \\
& \quad t^{U_2} \in \text{TERM}_{U_2} \\
& \quad \varepsilon_1 \vdash U_1 \sim \text{Bool} \\
& \quad \varepsilon_2 \vdash U_2 \sim U \\
& \quad \varepsilon_3 \vdash U_3 \sim U \\
& \quad \text{if } \varepsilon_1 t^{U_1} \text{ then } \varepsilon_2 t^{U_2} \text{ else } \varepsilon_3 t^{U_3} \in \text{TERM}_U
\end{align*}
\]

We proceed assuming that the compilation always inserts casts (the other cases are similar because then the evidences are equal to the types in the judgment. Therefore the next combinations of those evidences are redundant and never fails). Then suppose \( U_1 \neq U_{11} \rightarrow U_{12} \) and \( U_2 \neq U_{11} \). As \( \varepsilon_1 = U_1 \cap U_{11} \rightarrow U_{12} \), and \( \varepsilon_2 = U_2 \cap U_{11} \), the type derivation of the compiled term is:

\[
\begin{align*}
\text{(Cif) } & \quad \Gamma \vdash \bar{t}_1 : U_1 \\
& \quad U_1 \sim \text{Bool} \\
& \quad \Gamma \vdash \bar{t}_2 : U_2 \\
& \quad \Gamma \vdash \bar{t}_3 : U_3 \\
& \quad \text{if } \langle \text{Bool} \triangleright U_1 \rangle \bar{t}_1' \text{ then } \langle U_2 \cap U_3 \triangleright U_2 \rangle \bar{t}_2' \text{ else } \langle U_2 \cap U_3 \triangleright U_3 \rangle \bar{t}_3' : U_2 \cap U_3
\end{align*}
\]

where \( \Gamma \vdash \bar{t}_1 \Rightarrow \bar{t}_1' : U_1, \Gamma \vdash \bar{t}_2 \Rightarrow \bar{t}_2' : U_2 \), and \( \Gamma \vdash \bar{t}_3 \Rightarrow \bar{t}_3' : U_3 \).

But by definition of substitution, \( \sigma_1(t^{U_1}) = \text{if } \varepsilon_1 \sigma_1(t^{U_1}) \text{ then } \varepsilon_2 \sigma_1(t^{U_2}) \varepsilon_3 \sigma_1(t^{U_3}) \) and \( \sigma_2(t') = \text{if } \langle \text{Bool} \triangleright U_1 \rangle \sigma_2(t_1') \text{ then } \langle U_2 \cap U_3 \triangleright U_2 \rangle \sigma_2(t_2') \text{ else } \langle U_2 \cap U_3 \triangleright U_3 \rangle \sigma_2(t_3') \).

By induction hypotheses on \( \bar{t}_1, \bar{t}_2 \) and \( \bar{t}_3, (\sigma_1(t^{U_1}), \sigma_2(t_1')) \in \mathcal{T}_k[U_1] \) and \( (\sigma_1(t^{U_2}), \sigma_2(t_2')) \in \mathcal{T}_k[U_2] \) and \( (\sigma_1(t^{U_3}), \sigma_2(t_3')) \in \mathcal{T}_k[U_3] \) if either \( \sigma_1(t^{U_1}) \) or \( \sigma_2(t') \) term reduces to an error then the result holds immediately. The interesting case is when they reduce to related values. Then suppose \( \sigma_1(t^{U_1}) \rightarrow^j \bar{v}_1, \sigma_2(t_1') \rightarrow^j v_1' \), where \( (\bar{v}_1, v_1') \in \mathcal{V}_k \cap \mathcal{V}_j[U_1] \) and \( (\bar{v}_2, v_2') \in \mathcal{V}_k \cap \mathcal{V}_j[U_2] \).

1. If \( \bar{v}_1 = \bar{u}_1 \) then \( v_1' = u_1' \), by canonical forms \( u_i \) must be booleans \( \text{bool} \) and \( b \). Suppose that \( b = \text{true} \) (the other case is analogous). Then \( t^{U_1} \rightarrow^j \varepsilon_2 \sigma_1(t^{U_2}) : U_2 \cap U_3 \) and \( t' \rightarrow^j \langle U_2 \cap U_3 \triangleright U_2 \rangle \sigma_2(t_2') \). Then as \( (\sigma_1(t^{U_2}), \sigma_2(t_2')) \in \mathcal{T}_k[U_2] \) and Lemma 7 and Lemma 9 and backward preservation of the relation the result holds.
2. If $\tilde{v}_1 = \varepsilon'_1 \tilde{u}_1 :: U_1$ and $\tilde{u}_1 \in \text{TERM}_{U'_1}$, then suppose $\nu_1' = \langle U_1 \overset{\tilde{v}_1}{\rightleftharpoons} U'_1 \rangle \nu_1'$ (the other case is similar but the evidence combination never fails). Also $(\tilde{u}_1, u_1') \in \mathcal{U}_{k-j}[U'_1]$. Suppose $\varepsilon_1' \circ \varepsilon_1$ is not defined (which is equivalent to $\varepsilon_1' \cap \varepsilon_1 = \emptyset$), therefore

$$\begin{align*}
\text{if } \varepsilon_1 \varepsilon_1' \tilde{u}_1 :: U_1 \text{ then } \varepsilon_2 \sigma_1 (t^{U_2}) \text{ else } \varepsilon_3 \sigma_1 (t^{U_3}) & \rightarrow \text{error} \\
\text{if } \langle \text{Bool} \overset{\tilde{v}_1}{\rightleftharpoons} U_1 \rangle \langle U_1 \overset{\tilde{v}_1}{\rightleftharpoons} U'_1 \rangle u_1' \text{ then } ... \text{ else } ... & \rightarrow \text{error}
\end{align*}$$

and the result follows. Suppose $\varepsilon''_1 = \varepsilon'_1 \circ \varepsilon_1$ is defined. Then

$$\begin{align*}
\text{if } \varepsilon_1 \varepsilon_1' \tilde{u}_1 :: U_1 \text{ then } \varepsilon_2 \sigma_1 (t^{U_2}) \text{ else } \varepsilon_3 \sigma_1 (t^{U_3}) & \rightarrow \text{error} \\
\text{if } \varepsilon''_1 \tilde{u}_1 \text{ then } \varepsilon_2 \sigma_1 (t^{U_2}) \text{ else } \varepsilon_3 \sigma_1 (t^{U_3}) & \Rightarrow \\
\text{if } \langle \text{Bool} \overset{\tilde{v}_1}{\rightleftharpoons} U_1 \rangle \langle U_1 \overset{\tilde{v}_1}{\rightleftharpoons} U'_1 \rangle u_1' \text{ then } ... \text{ else } ... & \rightarrow \text{error}
\end{align*}$$

Then as $(\tilde{u}_1, u_1') \in \mathcal{U}_{k-j}[U'_1]$ we proceed analogous to (1) and the result holds.

**Case (U+).** Similar to the (Uapp) and (Uif) case.

**References**


