Type-Driven Gradual Security with References
Matías Toro, Ronald Garcia, Éric Tanter

To cite this version:
Matías Toro, Ronald Garcia, Éric Tanter. Type-Driven Gradual Security with References. ACM Transactions on Programming Languages and Systems (TOPLAS), ACM, 2018, 40 (4), pp.1-55. 10.1145/3229061. hal-01957581v2

HAL Id: hal-01957581
https://hal.archives-ouvertes.fr/hal-01957581v2
Submitted on 14 Oct 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers. L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Type-Driven Gradual Security with References

MATÍAS TORO, PLEIAD Laboratory, Computer Science Department (DCC), University of Chile
RONALD GARCIA, Software Practices Laboratory, University of British Columbia
ÉRIC TANTER, PLEIAD Laboratory, Computer Science Dept (DCC), University of Chile & Inria Paris

In security-typed programming languages, types statically enforce noninterference between potentially conspiring values, such as the arguments and results of functions. But to adopt static security types, like other advanced type disciplines, programmers face a steep wholesale transition, often forcing them to refactor working code just to satisfy their type checker. To provide a gentler path to security typing that supports safe and stylish but hard-to-verify programming idioms, researchers have designed languages that blend static and dynamic checking of security types. Unfortunately most of the resulting languages only support static, type-based reasoning about noninterference if a program is entirely statically secured. This limitation substantially weakens the benefits that dynamic enforcement brings to static security typing. Additionally, current proposals are focused on languages with explicit casts, and therefore do not fulfill the vision of gradual typing, according to which the boundaries between static and dynamic checking only arise from the (im)precision of type annotations, and are transparently mediated by implicit checks.

In this paper we present GSLRef, a gradual security-typed higher-order language with references. As a gradual language, GSLRef supports the range of static-to-dynamic security checking exclusively driven by type annotations, without resorting to explicit casts. Additionally, GSLRef lets programmers use types to reason statically about termination-insensitive noninterference in all programs, even those that enforce security dynamically. We prove that GSLRef satisfies all but one of Siek et al.’s criteria for gradually-typed languages, which ensure that programs can seamlessly transition between simple typing and security typing. A notable exception regards the dynamic gradual guarantee, which some specific programs must violate if they are to satisfy noninterference; it remains an open question whether such a language could fully satisfy the dynamic gradual guarantee. To realize this design, we were led to draw a sharp distinction between syntactic type safety and semantic type soundness, each of which constrains the design of the gradual language.

CCS Concepts:
- Security and privacy → Information flow control;
- Theory of computation → Type structures;
Program semantics;

Additional Key Words and Phrases: Noninterference, language-based security, gradual typing

1 INTRODUCTION

Gradual typing is typically viewed as a means to combine the agility of dynamic languages, like Python and Ruby, with the reliability of static languages, like OCaml and Scala [Siek and Taha 2006]. But static and dynamic are merely relative notions, and several researchers have explored a more relativistic view. For example, Disney and Flanagan [2011] and Fennell and Thiemann [2013] develop languages where only information-flow security properties are enforced using both dynamic and static checking; Bañados Schwerter et al. [2014, 2016] develop a language where only computational effect capabilities are gradualized; Lehmann and Tanter [2017] gradualize only the logical assertions of refinement types; and Jafery and Dunfield [2017] gradualize only refinements of sum types. In each of these cases, the “fully-dynamic” corner of the gradual language is not dynamic by typical standards, but rather simply typed. Nonetheless, each language supports migration toward a richer typing discipline that subsumes simple typing.

This paper revisits gradual information-flow security typing, with a particular focus on the strong information-flow guarantees that security types have historically implied. We describe a
new language, GSLRef, that introduces a type-driven conception of gradual security. Unlike most prior work, GSLRef supports the same static, type-based reasoning about information-flow for gradually-typed programs as SSLRef, its purely static counterpart. To explain this innovation, we review the power of static security types and then show what it means to preserve type-based reasoning power in a gradual language.

**Static security typing.** Consider a program that processes employee data:

```plaintext
let age = 31
let salary = 58000
let toString : Int → String = ...
let print : String → Unit = ...
print (toString (salary))
```

The program is well-typed, but it has a significant error that simple types do not catch: if salaries are confidential and printing is publicly observable, then this program leaks confidential data.

Information-flow security typing lets a programmer statically classify program entities according to a lattice of security labels [Denning 1976] and rely on type-checking to prevent information leaks. One exemplar security lattice, which we use as a running example, is the U.S. Dept of Defense classification scheme: Unclassified ≼ Confidential ≼ Secret ≼ Top Secret, which we simplify to ⊥ ≼ L ≼ H ≼ ⊤, denoting minimum, low, high, and maximum security respectively [Zdancewic 2002]. To inform static type checking, each type constructor is statically annotated with a security label (e.g. Int_L); source program values are also annotated to unambiguously determine their static security (e.g. 58000_H has type Int_H). Security label ordering induces a natural subtyping relation (e.g. Int_L ≼ Int_H and Int_H → L String_L ≼ Int_L → H String_H_L), which denotes security-respecting substitutability. An attacker or observer at level λ_o can discriminate values that have security level at most λ_o. Armed with security types and subtyping, an information-flow security type system statically ensures that high-confidence data may not flow directly or indirectly to low-confidence channels [Volpano et al. 1996].

In the example above, if we annotate the salary as high-security data (of type Int_H), and specify that print takes a low-security argument (of type String_L), then our operational intuition tells us that the program cannot satisfy these directives: it should be rejected. Before the type system can confirm our intuitions, though, we must determine the security levels of every type in the program. In SSLRef, our static language, this means that every type and value must be annotated. While security label inference and polymorphism [Myers and Liskov 2000] can reduce this burden, one cannot experiment with some security levels without first determining all security levels. Once all security types are assigned, the static type system forbids passing a high-security value to a function that expects a low-security argument, so the type checker rejects the program. GSLRef conservatively extends this model to support incremental and localized adoption of security types.

**Security types induce free noninterference theorems.** The employee data example demonstrates a simple security leak, where high-security data flows directly to a low-security channel. But security types must also contend with sophisticated leaks, where low-security variables may change control-flow through high-security code and mutable state can enable implicit security leaks [Denning 1976]. To combat this, information-flow security languages enforce a general property called noninterference, which guarantees that high-security inputs do not affect low-security results [Goguen and Meseguer 1982]. Noninterference clearly subsumes our simple security leak, but it also prevents implicit and control-based leaks, where an attacker attempts to use low-security inputs and outputs to learn about high-security data.

---

1Adapted from [Disney and Flanagan 2011].
In security-typed languages, higher-order security types denote modular guarantees about noninterference [Heintze and Riecke 1998]. In particular, they use Reynold’s theory of parametricity [Reynolds 1983] to ensure that a typing judgment dictates how replacing inputs can affect the resulting output [Abadi et al. 1999]. For example, consider a hypothetical function:

\[
\text{let } \text{mix} : \text{Int} \rightarrow \text{L} \rightarrow \text{Int} \rightarrow \text{L} \rightarrow \text{Int} \rightarrow \text{L} = \text{fun} \text{ pub priv } \Rightarrow \ldots
\]

At first sight, it appears to “mix” its arguments pub and priv to produce some result. However, the security annotations on its type guarantee that the integer result cannot leak information about priv, no matter what value is given to pub. The key to this result is how the relevant typing judgment is interpreted. The body of the mix function, t, must satisfy the typing judgment \(\text{pub} : \text{Int} \rightarrow \text{L}, \text{priv} : \text{Int} \rightarrow \text{H} \Rightarrow t : \text{Int} \rightarrow \text{L}\). To endow this judgment with meaning, a logical relation-based semantic model is defined directly in terms of the language’s dynamic semantics. According to this semantic typing judgment, changing the value of priv has no effect on the final value of t. This guarantee holds even if mix uses mutable state [Zdancewic 2002]. The end result is that an attacker with no direct access to a high-security channel cannot manipulate the value of pub to uncover the value of priv, even by modifying mix’s implementation.

In a static security language, these noninterference guarantees follow from the type structure of the language. No runtime checks are required, and the security labels applied to values and types are simply static annotations. In essence, static security types induce free theorems about the noninterference behaviors of computations, just as parametric polymorphic types induce free theorems about data abstraction [Wadler 1989]. Free noninterference theorems provide enormous benefits to programmers. First, they support modular reasoning about noninterference: a programmer who implements a higher-order function with type \((\text{Int} \rightarrow \text{L} \rightarrow \text{H} \rightarrow \text{L} \rightarrow \text{Int} \rightarrow \text{L} \rightarrow \text{Bool} \rightarrow \text{H})\) knows that the function’s body can safely call its argument with high-security data as the second argument: the provided function cannot leak that data. Second, type-based reasoning is compositional: the syntactic typing rules precisely specify how the security properties of subprograms (e.g., a function-typed expression and a potential argument) compose to determine security properties of a larger program (e.g. via function application). Finally, this reasoning is static: one need not reason directly about operational behavior or data flow to understand security. That reasoning was done once-and-for-all in the type-driven noninterference proof. Instead, type structure guides reasoning. These properties are especially useful for partial programs like software libraries. Below we show that GSL-Ref preserves these advantages while introducing new flexibility by dynamically enforcing some type guarantees.

Relaxing security typing. Like any static type discipline, security typing has its downsides. As discussed above, security typing cannot be checked until all types are given a security level, through ascription, polymorphism, or inference. One cannot incrementally add security levels and observe the consequences. In addition, verifying noninterference is in general undecidable, so static security checking is necessarily conservative, and as a result programmers must sometimes refactor perfectly safe and clear code simply to appease the type checker.

To address these shortcomings, researchers have explored ways to combine static and dynamic security checking. These approaches can be classified roughly as hybrid or gradual. Hybrid approaches, e.g. [Buiras et al. 2015; Chandra and Franz 2007; Shroff et al. 2007; Zheng and Myers 2007], blend various static analysis and runtime monitoring techniques to make analyses more precise, to incorporate dynamically-defined policies, and to target safe executions rather than just safe programs. Gradual approaches [Disney and Flanagan 2011; Fennell and Thiemann 2013, 2016],

\[^2\] Like type annotations, security labels appear in dynamic semantics solely to prove type safety: they are erased in a practical runtime.
inspired by gradual typing, focus on type systems for static analysis and add the extra goal of enabling seamless incremental evolution from programs with no information-flow control whatsoever to programs with security-type based static enforcement, while fulfilling the goals of hybrid approaches.

To clearly understand the contribution of the present work, it is important to clarify that the prior work in this space, hybrid and gradual alike, take a check-driven approach to analysis: the core of the security model is based on associating a security level to each value in a program and managing security levels using two distinct operations: security upgrades and checks. A security upgrade elevates a value’s security label, e.g. \((\text{Int}\ H)5_L \rightarrow 5_H\). A security check signals an error if the checked label is not at least as high as the value’s tag, e.g. \((\text{Int}\ H?)5_L \rightarrow 5_L\), but \((\text{Int}\ L?)5_H \rightarrow \text{error}\). upgrades and checks have different dynamic behavior, but with help from static typing, gradual security languages combine them into type-based upcasts and downcasts, e.g. \((\text{Int}\ L)t\), which checks \(t\) if \(L\) is lower than \(t\)’s static security and upgrades \(t\) otherwise. This approach easily detects direct flows of high-security values to low-security channels, but preventing implicit flows through control transfer requires extra care, including prophylactic upgrades to program values [Chandra and Franz 2007] and policies to restrict upgrades [Fennell and Thiemann 2013]. As we will see, our development similarly requires careful treatment of assignments.

**Check-driven approaches break free theorems.** Dynamic security casts give flexibility to programmers, but fundamentally cripple the ability to reason statically using security types. In particular, if security downcasts are added to the language, although noninterference is still preserved, static type judgments no longer imply free theorems about security of programs, as was discussed above. As a result, programmers must reason about the dynamic semantics—dynamic labels, dynamic upgrades, and dynamic checks—to uncover which values do not interfere with one another. In particular, a function’s type no longer denotes noninterference properties about its arguments and results. For example, consider the function:

```plaintext
let mix : \text{Int} \rightarrow \text{Int} \rightarrow \text{Int} =
  \text{fun pub priv => if pub < (\text{Int}L)priv then 1_L else 2_L}
```

This program is statically accepted by languages that only check for compatibility of base types [Disney and Flanagan 2011; Fennell and Thiemann 2013]. The type of \(\text{mix}\), while fully static, does not guarantee that \(\text{mix}\) never reveals information about its second argument. Rather, the type merely guarantees that the second argument’s security level is at most \(H\) and the result is at most \(L\). But upper-bounds on security labels do not suffice to make definitive assertions about the noninterference behavior of this function.\(^3\) Indeed, the program \(\text{mix} 1_L \ 5_L\) successfully reduces to \(1_L\). In order to avoid such behavior, the programmer must explicitly upgrade the dynamic security level of the value passed as second argument at each call site. Alternatively, one can upgrade \(\text{mix}\) to its own type, thereby forcing the second argument to be upgraded before executing the function body (and hence preventing any information leak about that argument). This highlights the fact that types alone do not denote noninterference properties: the two versions of the \(\text{mix}\) function behave differently although they have the same type.

This phenomenon, that adding dynamic checking to a static system may weaken type-based reasoning principles, is not unique to security typing. Prior work on cast calculi with parametric polymorphism observes that adding runtime type tests to System F preserves type safety—i.e. that programs do not crash—but sacrifices type soundness—i.e. that polymorphic types denote strong data abstraction guarantees via parametricity [Ahmed et al. 2011, § 5.1].

\(^3\)Recent work by Fennell and Thiemann [2016] on LGJS addresses this particular problem, as described in Sec. 7.
**Contribution:** type-driven gradual security typing. Modular, compositional, and type-based reasoning are hallmark benefits of type systems. Thus, to facilitate the seamless transition toward static security typing, the typing judgment of a gradual type system should imply the same semantic invariants that its fully-static counterpart does. To that end, this paper presents GSLRef, a type-driven gradual security language that extends a static security type discipline with gradual security labels and corresponding notions of gradual type precision and consistent subtyping. To secure GSLRef programs, one just adds static security labels: dynamic checks arise automatically and implicitly, as needed to enforce the noninterference guarantees denoted by static types.

Unlike most prior work, GSLRef’s static security types denote the same noninterference guarantees as its fully static counterpart language SSLRef. As such, GSLRef’s security types enable modular and compositional type-based reasoning about noninterference, just like the fully static SSLRef, whereas security types in most prior gradual languages do not. GSLRef’s type system supports reasoning about termination-insensitive noninterference because it is sound with respect to a security logical relation defined directly in terms of type structure. This result is standard for a purely-static security language [Heintze and Riecke 1998], but novel for a gradual security language with imprecise types supported by dynamic checks. In fact the dynamics are guided by the needs of the noninterference proof.

To summarize, this work makes the following contributions:

- We present GSLRef, a gradual security language that supports seamless transition between simply-typed and security-typed programming. Security typing annotations alone drive the balance between static and dynamic information flow checking. (Sec. 4)
- We prove that GSLRef’s type discipline enforces termination-insensitive noninterference: GSLRef’s types reflect strong information-flow invariants that hold even in code that contains gradually-typed subexpressions. (Sec. 5)
- We prove the static gradual criteria of Siek et al. [2015]. Interestingly, in order to ensure noninterference in presence of references (and hence implicit flows through the heap), GSLRef sacrifices the dynamic gradual guarantee.
- We contribute more generally to the foundations of gradual typing for advanced type disciplines. We find that GSLRef’s security invariants require separate consideration of syntactic type safety and semantic type soundness, each of which constrains the design of the gradual language.
- This work also represents a particularly challenging application of the Abstracting Gradual Typing (AGT) methodology [Garcia et al. 2016]. AGT is a framework that uses abstract interpretation [Cousot and Cousot 1977] at the type level to systematically construct gradually-typed languages from pre-existing statically typed ones. We report on our experience with a number of important considerations that complement the original presentation of AGT. In addition, we highlight the limitation of AGT when applied to semantically-rich type disciplines. (Sec. 6)

Before diving into the development of GSLRef, Sec. 2 informally introduces the type-driven approach to gradual security typing through examples. Then, Sec. 3 presents SSLRef, the fully-static security type language from which GSLRef is derived. Supplementary definitions can be found in the Appendix. Complete definitions, as well as the proofs of all the results stated in the paper, can be found in the companion technical report [Toro et al. 2018]. An interactive executable model of GSLRef is available online at https://pleiad.cl/gradual-security/.
2 TYPE-DRIVEN GRADUAL SECURITY TYPING IN ACTION

Static security type systems impose a burdensome all-or-nothing adoption model: all security types must be determined before the type system can check security. Even then, some secure programs have no statically-checkable type assignment, or may require substantial refactoring to satisfy the type checker. Gradual security typing addresses these shortcomings by enabling a programmer to incrementally add security information to the program, progressively introducing dynamic and static checks and guarantees.

Let us consider how gradual security typing can progressively introduce security guarantees and help detect and fix bugs in our first example from Sec. 1. Recall the problem with the program: salary is a high-security value, but print is a low-security channel. We can statically reflect these intentions:

1 let age = 31;
2 let salary = 58000;
3 let intToString : Int → String = ...
4 let print : String → Unit = ...
5 print (intToString (salary))

In practice the programmer just marks the value of salary and the input type of print: all omitted security annotations desugar to the unknown security label ?. Under our gradual security semantics, this program type checks, but triggers a runtime check failure at line 5. If the highlighted annotations were omitted or ?, then the program would check and run exactly as a simply-typed one, because it would not impose, and thus not enforce, any security invariants.

How do we repair this program? Simply adding more annotations cannot fix it. Case in point, adding a reasonable security annotation to line 3 escalates the runtime failure to a static type error.

3 let intToString : Int → String = ...

If the security annotations are as intended, however, then the runtime error must be due to some behavioral bug in the program (e.g. the programmer might have intended to print the employee’s age instead).

Reasoning with imprecision. The gradual type checker statically enforces the invariants it can, deferring checks to runtime when the static type information is insufficient. Rather than introducing dynamic casts, as in the check-driven approach, our type-driven approach to gradual security typing builds on foundations laid by prior research on gradual typing. Siek and Taha [2006] observe similar difficulties as in the check-driven approach when trying to use subtyping to combine dynamic and simple type checking. This inspired gradual typing, which extends static types with an unknown type to form gradual types, relating them to one another using consistency and precision relations [Siek et al. 2015]. Since these notions are conceptually orthogonal to subtyping, they blend well with pre-existing subtyping disciplines [Siek and Taha 2007]. Our type-driven approach adapts these concepts to gradual security and its natural notion of subtyping.

In this model, the unknown label ? represents imprecise security information. Precision ⊑ is a partial order from more-precise labels to less-precise labels: static security labels are perfectly precise, e.g. H ⊑ H, while ? denotes utter imprecision, e.g. H ⊑ ?. Precision extends covariantly to security types, e.g. Int₁ → Int₃ ⊑ Int₁ → Int₁, in contrast to subtyping.

The ordering on security labels ≼ consequently extends to consistent ordering ≺ on gradual labels. Consistent ordering preserves every order relation among precise labels (e.g. ⊥ ≺ T and T ≺ ⊤), but mathematically, it is not an ordering relation (e.g. both ? ≺ T and T ≺ ?). Rather, it reflects consistent reasoning in the face of imprecise information: since we do not know what label ? represents, either static order is plausible. Consistent ordering induces an analogous notion of
consistent subtyping, e.g. \( \text{Int} \preceq \text{Int} \) and \( \text{Int} \preceq \text{Int} \), which is not transitive, e.g. \( \text{Int} \not\preceq \text{Int} \), so it is not a subtyping relation, but embodies imprecise reasoning about static subtyping [Siek and Taha 2007]. An attacker or observer at level \( \ell_0 \) can now also observe values that have unknown security levels, as long as the dynamic security information about the value is observable at \( \ell_0 \). This is formally explained in Section 5.

**Flexibility.** As we have seen, GSLRef lets programmers write statically secure programs by first writing the simply-typed version and progressively adding labels. But gradual typing also provides flexibility, so that safe programs that veer from the static type discipline can strategically revert to dynamic checking. GSLRef’s type-driven approach provides this flexibility. Consider an example adapted from Fennell and Thiemann [2013].

```plaintext
let infoH : RefReportH = ... let sendToFacebook : RefReportL →UnitL = ... let sendToManager : RefReportH →UnitL = ... let addPrivileged : Boolean? → (RefReport? →UnitL) →RefReport? →UnitL = fun isPrivileged worker report => if isPrivileged then report := !report + !infoH else (); worker report let sendHi : RefReportH →UnitL = addPrivileged true sendToManager let sendLow : RefReportL →UnitL = addPrivileged false sendToFacebook
```

The program starts with the creation of a public reference to a private report, infoH. It then defines two routines for submitting reports: sendToFacebook publishes data publicly, and sendToManager publishes data privately. The addPrivileged function decides dynamically whether to add high-security information to the sent report, and is used to implement the sendHi and sendLow functions. This code is secure, but SSLRef, our static security system, cannot type check addPrivileged because of its dynamic choice.

Interestingly, GSLRef can type check this program, thanks to a few well-placed ? labels (line 4), and it dynamically ensures that the program does not leak data. Case in point, the following gradually-typeable function is poised to leak private data:

```plaintext
let sendFail : RefReportL →UnitL = addPrivileged true sendToFacebook
```

but if called, GSLRef’s dynamic security monitor signals an error when sendToFacebook dereferences the report, thereby preventing the leak.

**Type-based reasoning in GSLRef.** Like prior work, GSLRef supports smooth migration to static security and flexible programming idioms. Its most significant innovation is that GSLRef retains the type-based reasoning power of static security typing.

Consider again the example mix function of Sec. 1. In GSLRef, the function body cannot violate the noninterference property implied by its type, just as in its fully static counterpart language SSLRef. In particular, the following definition is rejected statically as expected:

```plaintext
let mix : IntL →IntH →IntL = fun pub priv => if pub < priv then 1L else 2L
```

In fact, no function body can satisfy this type signature and use its second argument to determine the result. To do so, we must change the type signature, and with it the implied security invariants:

```plaintext
let mix : IntL →IntL →IntL = fun pub priv => if pub < priv then 1L else 2L
```

4Security labels above function arrows track mutation effects (Sec. 3).
The second argument now has statically unknown security. This definition is accepted statically because the function might respect the static security invariants of its clients. Consider two such clients, which only differ in the security level of the second argument:

\[
\begin{align*}
\text{mix } & \text{ 1}_L \ 5_H \\
\text{Client 1} & \\
\text{mix } & \text{ 1}_L \ 5_L \\
\text{Client 2} &
\end{align*}
\]

Both type check because the security level of the second argument is consistent with the expected, unknown level. Client 2 returns \(1_L\) without incident, because its second argument is public, so applying \(\text{mix}\) does not leak private information. Client 1, however, signals a runtime security error: the function’s intended result would implicitly leak information from a private input, but the impending leak is trapped and reported. Treating static security levels as precise requirements rather than upper-bounds, and supporting imprecision, provides the same flexibility as the check-driven approach, as demonstrated in the reporting example above. The key difference is that dynamicity manifests as imprecision in a function’s static type, so precise types can preserve their static security interpretation. The interaction between types of different precision is transparently guarded by implicit runtime checks.

If we changed the type signature of \(\text{mix}\) to \(\text{Int} \rightarrow L \text{ Int}_H \rightarrow L \text{ Int}_L\), making the return type imprecise, then the definition would type check as well. Nonetheless, \(\text{GSLRef}'s\) dynamic enforcement ensures that the returned value could never leak to a public channel, be it a variable or a heap location, because the result is dynamically secured.

The type-driven model lets programmers use type ascriptions to impose static security guarantees on code that is built from imprecisely typed components. Gradual typing automatically introduces dynamic checks to soundly enforce these invariants. Consider a function called \(\text{smix}\) that has a fully static signature but is implemented using the imprecisely-typed \(\text{mix}\) function:

\[
\begin{align*}
\text{let } \text{mix} : & \text{Int} \rightarrow L \text{ Int}_H \rightarrow L \text{ Int}_L = \text{fun pub priv => if pub < priv then } 1_L \text{ else } 2_L \\
\text{let } \text{smix} : & \text{Int} \rightarrow L \text{ Int}_H \rightarrow L \text{ Int}_L = \text{fun pub priv => mix pub priv}
\end{align*}
\]

Type-based reasoning about noninterference dictates that \(\text{smix}\) cannot reveal any information about its second argument (regardless of the actual security label of the second argument). For instance, consider the clients:

\[
\begin{align*}
\text{smix } & \text{ 1}_L \ 5_H \\
\text{Client 1} & \\
\text{smix } & \text{ 1}_L \ 5_L \\
\text{Client 2} &
\end{align*}
\]

In \(\text{GSLRef}\), both clients type check, but both fail at runtime! Client 2 fails because \(\text{smix}'s\) type dictates a strong noninterference property, independent of the client’s dynamic security levels. To see why, observe that \(\text{smix}\) accepts as second argument any integer value that has a security level no higher than \(H\). When \(5_L\) is substituted in the body of \(\text{smix}\), its runtime security information is upgraded to \(H\). This new security level in turn strengthens the confidentiality of the value returned by \(\text{mix}\), which contradicts the static return type of \(\text{mix}\) (L), hence resulting in a runtime error. This behavior preserves local type-based reasoning about the behavior of components, regardless of how they are composed.

To summarize, in \(\text{GSLRef}\) different gradual security types denote different security guarantees. Most importantly, the flexibility introduced by imprecise security types cannot be abused to violate the type-based noninterference guarantees imposed by static security types.

\textbf{References and implicit flows.} In the presence of mutable references, information-flow security faces the classic problem of implicit flows through the heap [Denning 1976]. Consider the following program, adapted from Austin and Flanagan [2009]:
This program attempts to downgrade the security of it’s input. A static security type system easily rejects it because the first branch of the first conditional (line 4) assigns a low-security reference under a high-security boolean condition. Indeed, in GSLRef this program is statically rejected as well.

This program is tricky for dynamic information flow monitors, however, and has inspired many approaches, e.g. [Austin and Flanagan 2009, 2010, 2012; Hedin and Sabelfeld 2012a]. Since gradual security typing includes both static and dynamic security checking, GSLRef must also address the challenge of dynamically detecting implicit flows. Consider the same program as above but with some imprecise annotations:

```
1 fun x: Bool ⇒
2 let y: RefL Bool = ref trueL
3 let z: RefL Bool = ref trueL
4 if x then y := falseL else unit
5 if !y then z := falseL else unit
6 !z
```

This gradually-typed variant type checks because the reference bound to y now has an unknown security level. But if x is bound to trueH at runtime, then the program fails with an error at the assignment on line 4, because it cannot replace the contents of a reference in a manner that violates the security context H imposed by the conditional expression x. This restriction, and its motivation, is analogous to the “no-sensitive-upgrade” approach of Austin and Planagan [2009].

Now suppose we make y’s type have unknown static security but force its initial contents to have high security, i.e.:

```
2 let y: Ref? Bool = ref trueH
```

Then at runtime the assignment on line 4 succeeds because the assignment on line 2 already refined y’s dynamic security to H, which satisfies the security context. Now if x is falseH then this program fails at the assignment on line 5, because z’s security level violates the dynamic security context introduced by branching on the contents of y.

To sum up, GSLRef ensures termination-insensitive noninterference, gradually, even in the presence of references.

### 3 Static Security Typing with References

This section introduces SSLRef, a higher-order static security-typed language with references, which serves as the static extreme of our gradual language. The language is a straightforward adaptation of prior information-flow security typing disciplines [Fennell and Thiemann 2013; Heintze and Riecke 1998; Zdancewic 2002]. The most significant novelties include a syntax-directed type system and a dynamic semantics that tracks security levels but performs no security checks: the type system alone guarantees noninterference.

**Syntax.** Fig. 1 presents the syntax of SSLRef, at heart a simply-typed higher-order language with references: it includes booleans, functions, unit, mutable references, and type ascription. Each value and type constructor is annotated with a security label $\ell \in \text{LABEL}$ with partial order $\preceq$, where $\top$ and $\bot$ denote the greatest and least labels respectively. Function abstractions, and their corresponding
types, are annotated with an additional security label called the latent security effect: we explain its static semantics below. Two forms arise only at runtime (highlighted in gray): mutable locations \( o \) and a protection term \( \text{prot}_\ell(t) \), which restricts the security effects of its subterm \( t \).

**Statics.** Fig. 1 also presents the type system of \( \text{SSL}_\text{Ref} \), which is technically a type-and-effect system [Gifford and Lucassen 1986]. The judgment \( \Gamma; \Sigma; \ell_c + t : S \) says that the term \( t \) has type \( S \) under type environment \( \Gamma \), store type \( \Sigma \), and security effect \( \ell_c \in \text{Label} \). A type environment \( \Gamma \) is a finite map from variables to types. A store type \( \Sigma \) is a finite map from locations to types. The security effect, sometimes called the program counter label [Denning 1976], is a security label that denotes the least security level of those references that a given term may allocate or mutate [Heintze and Riecke 1998]. The security effect prevents high-security computations—e.g., the branch of an if expression that is chosen based on a high-security Boolean—from leaking information by assigning to low-security references. An \( \text{SSL}_\text{Ref} \) source program \( t \) is well-typed if \( \vdash t : S \).

- Rule (Sx) and rule (So) type variable and location references as usual. Simple values are also typed as usual, but their types inherit their labels from the values themselves (Sb/Su).
- Rule (Sλ) annotates the type of a function with the latent security effect of its body, as is standard for type-and-effect systems. The greatest (i.e., best) security effect can be inferred from the function body, but for simplicity this type system consults an explicit annotation \( \ell' \).
• Rule (Sprot) imposes a lower bound \( \ell \) on the security effect of the subterm \( t \). This restriction is captured by stamping the label \( \ell \) onto the type [Heintze and Riecke 1998]—e.g. \( \text{Bool}_\ell \prec \ell' = \text{Bool}_{\ell \vee \ell'} \), where \( \ell \vee \ell' \) represents the least upper-bound, or join, of security levels \( \ell \) and \( \ell' \).

• Rule (S⊕) types Boolean operations, yielding a result with the join of the operand security levels.

• Rule (Sapp) is mostly standard, but also enforces security restrictions. First, to prevent mutation-based security leaks, the operator’s latent effect \( \ell' \) must upper-bound its security level as well as the latent security effect of the entire expression. Both restrictions are captured with a single label comparison in the premise. Second, to prevent value-based security leaks, the security level of the entire expression must upper-bound the level \( \ell \) of the operator—this is done by stamping label \( \ell \) onto the type. Rule (Sapp) also appeals to the subtyping relation induced by ordering the security labels. Subtyping is driven by security labels: it is invariant on reference types, covariant on security labels, and contravariant on latent effects [Pottier and Simonet 2003]:

\[
\begin{align*}
\ell &\ll \ell' \\
\text{Bool}_\ell &\prec \text{Bool}_{\ell'} \\
\ell &\ll \ell' \\
\text{Unit}_\ell &\prec \text{Unit}_{\ell'} \\
\ell &\ll \ell' \\
\text{Ref}_\ell S &\prec \text{Ref}_{\ell'} S
\end{align*}
\]

\[
\begin{align*}
S_1' &\ll S_1 \\
S_2 &\ll S_2' \\
\ell_1 &\ll \ell_1' \\
\ell_2 &\ll \ell_2 \\
S_1'_{\ell_1} &\ll S_1'_{\ell_1'} \\
S_2 &\ll S_2'_{\ell_2}
\end{align*}
\]

• Rule (Sif) incorporates the standard structure for a subtype discipline: the type of the expression involves the subtyping join \( \ll \) of its branches. To protect against explicit information flows, the expression type is stamped to incorporate the security level \( \ell \) of the predicate. Additionally, to prevent effect-based leaks, each branch is type checked with a security effect that incorporates the security level of the predicate.\(^5\)

• Rules (Sref) and (Sasgn), which perform write effects, are constrained by the security effect of the typing judgment to prevent leaks through the store. Rule (Sref) honors the effect discipline by requiring the current security effect to lower-bound the security level of the stored value. The resulting reference has least security \( \bot \) because it is newly minted and cannot leak information: the type of the stored content is known and its security level prevents further prying.

Rule (Sasgn) ensures that the security level of the location and current security effect lower-bound the assigned value. The result of assignment has \( \bot \) security because unit cannot leak information. Rule (Sderef) stamps the security level of the reference onto the resulting type.

• Finally, Rule (S::) is typical for ascription, requiring the ascribed type to be a supertype of the subterm’s type.

**Dynamics.** With fully static security typing, programs execute on a standard runtime with no additional security-enforcing machinery. Type safety—well-typed terms do not get stuck—is guaranteed by the underlying run-of-the-mill simple type discipline. However, to establish the soundness of security typing—high-security computations have no effect on low-security observations—one must characterize computations and their resulting values with respect to their security levels. To this end, the SSL\(_{\text{ref}}\) dynamic semantics explicitly tracks security labels as programs evaluate, but never checks them. The noninterference proof demonstrates that no such

---

\(^5\)Note that SSL\(_{\text{ref}}\) does not have an explicit effect ascription form \( t :: \ell_c \) [Bañados Schwerter et al. 2014], but this can be encoded using the expression \((\lambda x : \text{Unit}. \bot)_{\bot} \) unit\(_\bot\).
Notion of Reduction

$$t \mid \mu \xrightarrow{\ell} t \mid \mu$$

<table>
<thead>
<tr>
<th>Rule</th>
<th>Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>b_1\ell_1 \oplus b_2\ell_2</td>
<td>\mu \xrightarrow{\ell} (b_1 [\oplus] b_2)(\ell_1 \lor \ell_2)</td>
</tr>
<tr>
<td>if true_\ell then t_1 else t_2</td>
<td>\mu \xrightarrow{\ell} \text{prot}_\ell(t_1)</td>
</tr>
<tr>
<td>if false_\ell then t_1 else t_2</td>
<td>\mu \xrightarrow{\ell} \text{prot}_\ell(t_2)</td>
</tr>
<tr>
<td>\text{prot}_\ell(v)</td>
<td>\mu \xrightarrow{\ell} v \lor \ell</td>
</tr>
<tr>
<td>ref^{S} v</td>
<td>\mu \xrightarrow{\ell} o_\perp</td>
</tr>
<tr>
<td>!o_\ell</td>
<td>\mu \xrightarrow{\ell} v \lor \ell</td>
</tr>
</tbody>
</table>

Fig. 2. SSL_{\text{Ref}}: Label Tracking Dynamic Semantics

checks are required: static typing suffices. Tracking labels provides weak security guarantees that are exploited in the proof of the stronger noninterference result.

Fig. 2 presents the rules of the label-tracking dynamic semantics. The judgment $t_1 | \mu \xrightarrow{\ell_c} t_2 | \mu_2$ says that a term $t_1$ and store $\mu_1$ step to $t_2$ and $\mu_2$ respectively, in security effect $\ell_c$. Reduction of terms is specified using term frames $f$:

$$f ::= \square \oplus t | v \oplus o | \square t | v \square | \square :: S | if \square then t else t | !\square | \square :: t | v::\square | \text{ref}^{S} \square$$

The core semantics is typical, so we focus on tracking security. The runtime security effect $\ell_c$, which reflects its static counterpart, affects the security level of reads from and writes to the store, as well as the security level of values returned from high-security contexts to low-security ones.

Protection terms $\text{prot}_\ell(t)$ control the current program counter label. Apart from prot, all expressions propagate the current program counter to subterms. Rule (Rprot) upgrades $\ell_c$ for the dynamic extent of $t$. The resulting value is stamped with the protected label $\ell$, in case the contents leak information to a context that lacks the confidentiality of $\ell$. Values are stamped much like types: $r_{\ell \lor \ell'} = r_{(\ell \lor \ell')}$.

Protection terms do not exist in source programs: they are introduced by control operations, i.e. function calls and conditionals. The intuition is that calling a function or destroying a Boolean of security level $\ell$ may leak information about the identity of the function or Boolean respectively. As such, the context of the resulting computation should communicate (via mutation) only with reference cells that have high-enough security, and the result of the computation is classified as well.$^6$ Function calls ignore the operator’s latent effect $\ell'$, which promises the type system

---

$^6$Zdancewic [2002] observes that e.g. if $x$ then $e_l$ else $e_l$ leaks no information about Boolean $x : \text{Bool}_1$ so could be deemed low-security, but security type systems must be conservative for the sake of tractability.
that the ensuing computation will not violate the stated confidentiality. However the operator’s security label determines the confidentiality of the ensuing computation.

When stored, a value inherits confidentiality from both the current security effect and the location itself. This behavior tracks both the confidentiality of the location and the induced security effect.

Properties. SSL$_{Ref}$ is type safe: we establish this result via a standard progress and preservation argument [Toro et al. 2018]. Since the runtime semantics includes no security checks, progress mirrors the corresponding argument for the underlying simple type discipline. To prove preservation, we must show that after each reduction step the resulting term still has the same security according to the typing rules of Fig. 1, modulo subtyping.

Proposition 3.1 (Type Safety). If $\cdot ; \Sigma ; \ell_c \vdash t : S$ then either

- $t$ is a value $v$
- for any store $\mu$ such that $\Sigma \vdash \mu$ and any $\ell'_c \leq \ell_c$, we have $t \mid \mu \xrightarrow{\ell'_c} t' \mid \mu'$ and $\cdot ; \Sigma ; \ell_c \vdash t' : S'$ for some $S' <: S$, and some $\Sigma' \supseteq \Sigma$ such that $\Sigma' \vdash \mu'$.

The store typing judgment $\Sigma \vdash \mu$ holds if and only if $\text{dom}(\mu) = \text{dom}(\Sigma)$ and $\cdot ; \Sigma ; \ell_c \vdash \mu(o) : \Sigma(o)$ for all $o \in \text{dom}(\mu)$, $\ell_c \in \text{LABEL}$.

The most important property of a security-typed language like SSL$_{Ref}$ is the soundness of security typing, i.e. that well-typed programs have no forbidden information flows. We formally state and prove noninterference using step-indexed logical relations (see the companion technical report [Toro et al. 2018]). We do not include the definitions of the logical relations and noninterference statement here because proving that SSL$_{Ref}$ is secure is not the main focus of this work, and the full treatment of noninterference for the gradual language (Sec. 5) subsumes them.

4 GSL$_{Ref}$: TYPE-DRIVEN GRADUAL SECURITY TYPING

This section presents the static and dynamic semantics of GSL$_{Ref}$, and addresses its type safety and gradual guarantees. We show that GSL$_{Ref}$ enforces noninterference in Sec. 5.

The reader might (understandably!) wonder how some of the definitions presented in this section were conceived. This section largely appeals to intuition to justify these definitions, but in practice they were obtained by following the Abstracting Gradual Typing methodology [Garcia et al. 2016], which exploits principles of abstract interpretation [Cousot and Cousot 1977] to systematically derive a gradual language from a static one. In fact, this work can be seen as a particularly challenging case study for AGT—which has led us to identify the limits of the AGT approach when applied to disciplines where type safety (i.e. “well-typed terms do not get stuck”) does not imply type soundness (i.e. “well-typed terms do not leak”). The gradual language obtained by a straightforward application of AGT is type safe, but does not ensure noninterference because of subtle interactions between security typing imprecision and heap-based flows. We discuss the key elements, pitfalls, and discoveries of this systematic derivation process in Sec. 6.

To aid the reader, Fig. 3 indicates where important terms, operations and relations are presented, along with their notation.

4.1 Static semantics

Fig. 4 presents the syntax and static semantics of GSL$_{Ref}$.$^7$ A gradual security label $g \in \text{GLABEL}$ is either a static label $\ell$ or the unknown label $\text{?}$, which represents any label whatsoever. Each value and gradual type constructor is now annotated with a gradual security label.

$^7$In GSL$_{Ref}$, the $o$ and $\text{prot}_g(t)$ forms and typing rules merely serve to induce corresponding GSL$_{Ref}^\ell$ forms (Sec 4.2).
The typing judgment $\Gamma; \Sigma; g_c \vdash t : U$ says that the term $t$ has gradual type $U$ under type environment $\Gamma$, store environment $\Sigma$, and gradual security effect $g_c$. The typing rules are analogous to the static typing rules presented in Fig. 1 except that security labels, types, type functions and predicates are all replaced by their gradual counterparts. For instance, static label ordering $\leq$ is replaced with consistent label ordering $\hat{\leq}$:

$$\hat{\leq}$$

Intuitively, if consistent label ordering between two gradual labels holds, then it means that the static relation holds for some static labels represented by the gradual labels. It is always plausible in the presence of $\_\_\_\_\_$, since the unknown label represents any label. Similarly, subtyping is lifted to consistent subtyping $\trianglelefteq$, whose definition is analogous to static subtyping, but using consistent label ordering:

$$\trianglelefteq$$

$$\trianglelefteq$$
The label join and meet operators are replaced with consistent join and consistent meet respectively:

\[
\begin{align*}
\top \triangledown \Vdash = \top & \quad g \triangledown \Vdash g = \top & \quad \ell_1 \triangledown \ell_2 = \ell_1 \land \ell_2 \\
\bot \triangledown \Vdash = \bot & \quad g \triangledown \Vdash g = \bot & \quad \ell_1 \triangledown \ell_2 = \ell_1 \land \ell_2
\end{align*}
\]

These operators recover precise label information when the unknown label interacts with the relevant boundary element (\(\top\) for \(\triangledown\), and \(\bot\) for \(\triangledown\)) otherwise the result is always unknown. Intuitively, this is because any label \(\ell\) joined (resp. met) with \(\top\) (resp. \(\bot\)), yields \(\top\) (resp. \(\bot\), so imprecise arguments do not perturb the results. But when the relevant boundary is not involved, then varying \(\ell\) can vary the results, a possibility that is captured by using the unknown label as result.
The join operators for subtyping and label ordering are replaced with consistent join \( \sim \) and consistent label join \( \oversim{\vee} \) respectively:

\[
\begin{align*}
\text{Bool}_g \oversim{\vee} \text{Bool}_{g'} &= \text{Bool}_{(g \sim g')} \\
\text{Unit}_g \oversim{\vee} \text{Unit}_{g'} &= \text{Unit}_{(g \sim g')} \\
\text{Ref}_g U \oversim{\vee} \text{Ref}_{g'} U' &= \text{Ref}_{(g \sim g')} U \cap U'
\end{align*}
\]

\[
(U_1 \overset{g_1}{\rightarrow} U_{12}) \oversim{\vee} (U_2 \overset{g_2}{\rightarrow} U_{22}) = (U_1 \overset{g_1 \sim g_2}{\rightarrow} U_{12} \overset{g_1 \sim g_2}{\rightarrow} U_{22})
\]

\[U \oversim{\vee} U \text{ undefined otherwise}\]

The consistent subtyping meet operator is defined dually (definition in Appendix A.4).

Consistent subtyping join appeals to a gradual meet operator \( \cap \) on the referent types. This gradual meet arises because static subtyping is invariant for the contents of references, so static subtype join is only defined for references with equal referent types. The gradual meet operator can be understood as the gradual counterpart of a static type equality partial function \( \text{equate} \) (i.e. \( \text{equate}(S, S) = S \), undefined otherwise) [Garcia et al. 2016]. Intuitively, if the \( \cap \) of two gradual entities is defined, then it means that they are possibly equal. For instance, \( H \cap L \) is undefined, but \( H \cap ? = H \). Formally:

\[
\begin{align*}
g \cap g &= g \\
g \cap ? &= ? \cap g = g \\
\text{Bool}_g \cap \text{Bool}_{g'} &= \text{Bool}_{g \cap g'} \\
\text{Unit}_g \cap \text{Unit}_{g'} &= \text{Unit}_{g \cap g'} \\
\text{Ref}_g U \cap \text{Ref}_{g'} U' &= \text{Ref}_{g \cap g'} U \cap U'
\end{align*}
\]

\[
U_1 \overset{g_1}{\rightarrow} U_{12} \cap U'_1 \overset{g'_1}{\rightarrow} U'_{12} = (U_1 \cap U'_1) \overset{g_1 \cap g'_1}{\rightarrow} (U_2 \cap U'_2)
\]

Finally, The SSL\(_{\text{Ref}}\) rules (Sapp) and (Sasgn) from Fig. 1 have compound premises that combine both label join and label ordering, e.g. \( \ell \oversim{\vee} \ell' \oversim{\cap} \ell'' \). One subtlety we discovered while applying the AGT methodology is that these premises lose precision when lifted compositionally: simply replacing join with consistent join and label ordering with consistent label ordering yields different results when lifted in aggregate; we discuss this further in Sec. 6. Therefore rules (Uapp) and (Uasgn) use the consistent bounding predicate, which is defined algorithmically as: \( g_1 \oversim{\vee} g_2 \oversim{\cap} g_3 \iff g_1 \sim g_3 \). Technically, we could have used this definition to split each premise, but treating the predicate atomically matters when we consider the dynamic semantics.

### 4.2 Dynamic semantics

To present the dynamic semantics of GSL\(_{\text{Ref}}\), we first define a reduction relation for an internal language GSL\(_{\text{Ref}}^\epsilon\) that directly mirrors GSL\(_{\text{Ref}}\), except that all terms are augmented with some evidence information that justifies why the term is well-typed according to the gradual type system. During reduction steps, units of evidence are combined to form new evidence that supports type preservation between a term and its contractum. If the combination succeeds, reduction goes on; if the combination fails, a runtime error is raised. We first explain what evidence is, then how GSL\(_{\text{Ref}}\) programs are elaborated with evidence information into GSL\(_{\text{Ref}}^\epsilon\), and finally how evidence is combined, yielding the GSL\(_{\text{Ref}}^\epsilon\) reduction rules.
Evidence for consistent judgments. Evidence captures why a consistent judgment holds. To explain this concept, we begin with consistent judgments about security labels, then consider the more complex consistent judgments about types.

We use the metavariable \( \varepsilon \) to range over evidence, and write \( \varepsilon \vdash g_1 \sim \leq g_2 \) to say that evidence \( \varepsilon \) supports the plausibility that \( g_1 \sim \leq g_2 \) holds.

For instance, consider the consistent ordering judgment \( ? \varepsilon \leq L \). Even though the unknown label generally denotes any security label, consistent ordering insists that this \( ? \varepsilon \) can only denote labels that are bounded from above by \( L \). Furthermore, this consistent ordering judgment yields no additional information about the right-hand side, which is already precise. We capture this learned information by representing evidence as a pair of static label intervals, noted \( \langle i_1, i_2 \rangle \), where \( i = [\ell, \ell'] \). If \( \langle i_1, i_2 \rangle \vdash g_1 \sim \leq g_2 \) then \( i_1 \) and \( i_2 \) represent inferred range restrictions for \( g_1 \) and \( g_2 \), respectively. Therefore,

\[
\langle [\bot, L], [L, L] \rangle \vdash ? \sim \leq L
\]

By analogous reasoning, the consistent judgment \( H \varepsilon \leq ? \) is initially justified by the evidence \( \langle [H, H], [H, \top] \rangle \), gaining precision about the right-hand side. Interval precision is defined as containment over intervals, i.e. \( [\ell_1, \ell_2] \subseteq [\ell'_1, \ell'_2] \) if and only if \( \ell'_1 \leq \ell_1 \) and \( \ell_2 \leq \ell'_2 \). Precision between interval pairs \( \langle i_1, i_2 \rangle \subseteq \langle i'_1, i'_2 \rangle \) is defined pointwise.

We represent evidence as pairs of intervals, rather than pairs of labels, essentially because pairs of labels are not precise enough to support gradual security. The formal rationale is involved, so we defer it to Sec. 6. For some intuition, though, consider the program \( \text{true} :: \text{Bool} \sim \text{H} :: \text{Bool} \sim ? :: \text{Bool} \sim L \). Evaluating it ultimately involves combining evidence for three consecutive judgments:

\[
\varepsilon_1 \vdash ? \sim \leq H, \quad \varepsilon_2 \vdash H \sim \varepsilon, \quad \text{and} \quad \varepsilon_3 \vdash ? \sim \leq L \quad \text{The program should fail at runtime because an H security value should not be coercable to L, so these three evidences should not compose. Unfortunately, pairs of labels are not precise enough to ensure this: they forget the intermediate step through H. In contrast, pairs of label intervals retain enough precision to warrant the expected runtime failure.}

To justify consistent judgments about types like consistent subtyping, we lift label evidence to type evidence \( \varepsilon \) by naturally lifting intervals to types: type constructors are now marked with label intervals instead of labels. For instance:

\[
\langle \text{Bool}[\bot, L], \text{Bool}[L, L] \rangle \vdash \text{Bool} \sim \text{L} \]

The syntax of evidence is as follows:

- \( E \in \text{GEType} \), \( i \in \text{Interval} \), \( \varepsilon \in \text{Evidence} \)
- \( i ::= \langle \ell, \ell' \rangle \) (intervals)
- \( E ::= \text{Bool}, E \rightarrow E \mid \text{Ref}, E \mid \text{Unit} \) (type evidences)
- \( \varepsilon ::= \langle E, E \rangle \mid \langle i, i \rangle \) (evidences)

Note that we use the same metavariable \( \varepsilon \) to represent both label evidence and type evidence, since which kind of evidence is meant is always clear from the context.

Terms with evidence. Each well-typed term of GSLRef is recursively elaborated into a GSLRef term by decorating it with evidence for the consistent judgments used to establish its well-typedness.

\(^8\)in a way that we make precise below.
The syntax of GSL$^L_{\text{Ref}}$ terms follows:

\[
\begin{align*}
  t &::= \ v \mid \mathit{et} \ @_e \ et \mid \mathit{et} \oplus \ et \mid \mathit{if} \ et \ \text{then} \ et \ \text{else} \ et \mid \mathit{ref}_U^et \ | \ !et \mid \mathit{et} \ ::=_v \ et \mid \mathit{prot}_{g^e} \mathit{eg}(et) \mid et \\
  r &::= \ b \mid (\lambda^y x : U.t) \mid \mathit{unit} \mid o \\
  u &::= \ r_g \mid x \\
  v &::= \ u \mid \mathit{eu}
\end{align*}
\]

During reduction, the actual type of a subterm may evolve to a consistent subtype of the statically-determined type. For this reason, each term is augmented with evidence for their immediate subterms. This extra evidence supports the consistent label ordering judgments at that of their subterms. For instance, in the term $\mathit{ref}_1^{et} \oplus \mathit{ref}_2^{et}$, $\mathit{ref}_1$ justifies $t_1$ being a consistent subtype of $\mathit{Bool}_{g_1}$, the type deduced during type checking. In particular, $t_1$ could be such a consistent subtype because it is a value that was ascribed $\mathit{type} \mathit{Bool}_{g_1}$ using an explicit ascription. In fact, GSL$^L_{\text{Ref}}$ ascriptions are represented simply as evidence-augmented terms $et$ in GSL$^L_{\text{Ref}}$: the evidence $\epsilon$ holds all the computationally-relevant information about consistent subtyping. For instance, the GSL$^L_{\text{Ref}}$ term $(10_L :: \mathit{Int}_t) :: \mathit{Int}_H$ is translated to $\mathit{ref}_2(\mathit{ref}(10_L))$, where $\mathit{ref}_1 :: \mathit{Int}_L \leq \mathit{Int}_\epsilon$ and $\mathit{ref}_2 :: \mathit{Int}_L \leq \mathit{Int}_H$.

Note that in addition, some terms carry extra evidences that are needed during reduction to justify type preservation. A conditional if $\mathit{ref}_1 t_1$ then $\mathit{ref}_2 t_2$ else $\mathit{ref}_3 t_3$ carries evidences $\epsilon_2$ and $\epsilon_3$ that justify that the type of each branch $t_2$ and $t_3$ is a consistent subtype of the type of the conditional expression. For instance, if $U_2$ and $U_3$ are the types of $t_2$ and $t_3$ respectively, then $\mathit{ref}_2 t_2 :: U_2 \vdash U_2 \vdash U_3$, where $U_1 :: U_2 \vdash U_3$ is the consistent lifting of the ternary static judgment $T_1 :: T_2 \vdash T_3$. Similarly, a protection term $\mathit{prot}_{\mathit{ref}_1^{et} \mathit{ref}_2^{et} \mathit{ref}_3^{et}}(\epsilon_3 t)$ carries a security effect $g_2$ (and its evidence $\epsilon_2$), which represents the security effect of the subterm $t$; specifically, $g_2$ is the join of $g_1$ and the current security effect.

Values are either raw values $v$ or evidence-augmented raw values $\mathit{eu}$. The latter correspond to ascribed values $v :: U$ in GSL$^L_{\text{Ref}}$: the evidence $\epsilon$ confirms that the $u$’s type is a consistent subtype of the ascribed type $U$.

Several terms—applications, references, assignment, and protection—have evidence in addition to that of their subterms. This extra evidence supports the consistent label ordering judgments of their corresponding typing rule, which relate to the current latent effect label. For instance, in the term $\mathit{ref}_U^{et}$, the evidence $\epsilon'$ supports the consistent label ordering judgment $g_1 \leq \mathit{label}(U)$. For uniformity, we overload the metavariable $\epsilon$ to denote both label and type evidence, since the difference is always clear from the context. Evidence attached to subterms is type evidence, and evidence attached to the security effect or to an expression symbol ($@$, $\mathit{ref}$, $::$, or $\mathit{prot}$) is label evidence.

**Introducing evidence.** Fig. 5 presents rules for elaborating GSL$^L_{\text{Ref}}$ source terms to evidence-augmented GSL$^L_{\text{Ref}}$ terms. This elaboration is akin to a cast insertion translation [Siek and Taha 2006], but simpler because it inserts evidence uniformly [Garcia et al. 2016]. Basically, each consistent label and type judgment in Fig. 4 is replaced by an evidence-computing partial function called an initial evidence operator ($\mathcal{I}$). An initial evidence operator computes the most precise evidence that can be deduced from a given judgment. For instance, given a consistent label ordering judgment $g_1 \leq g_2$, the initial evidence for it is computed as follows:

\[
\mathcal{I}[g_1 \leq g_2] = \text{intr}(\mathit{bounds}(g_1), \mathit{bounds}(g_2))
\]
The bounds function produces the label interval that corresponds to a given gradual label, i.e. $\text{bounds}(?) = [\bot, \top]$ and $\text{bounds}(\ell) = [\ell, \ell]$. The interior operator intr computes the smallest sub-intervals of its arguments that include all plausible orderings. Given two intervals $\ell_1$ and $\ell_2$, $\text{intr}(\ell_1, \ell_2)$ yields the greatest pair of sub-intervals $(\ell'_1, \ell'_2) \subseteq (\ell_1, \ell_2)$ such that each label $\ell_1$ in the interval $\ell'_1$ is less than some label $\ell_1$ in $\ell'_2$, and each label in $\ell'_2$ is greater than some label in $\ell'_1$. Formally:

$$\text{intr}([\ell_{11}, \ell_{12}, [\ell_{21}, \ell_{22}]) = \langle [\ell_{11}, \ell_{12} \land \ell_{22}], [\ell_{11} \lor \ell_{21}, \ell_{22}] \rangle$$

In Garcia et al. [2016], the interior and initial evidence operators coincide under the name "interior" because both operate on pairs of gradual types. By distinguishing between intervals and labels, the present development induces a corresponding distinction between these notions.
This operation only changes the upper-bound of the lower interval and the lower-bound of the upper interval. The resulting intervals are well-defined because we only use this operator in \( \mathcal{J} \) after consistent label ordering is already known to hold.

Similarly, the initial evidence of a consistent judgment \( \Gamma \vdash g_1 \lor g_2 \leq g_3 \) is computed as

\[
\mathcal{J}[g_1 \lor g_2 \leq g_3] = \text{intr}(\text{bounds}(g_1) \lor \text{bounds}(g_2), \text{bounds}(g_3))
\]

This definition uses join of intervals, defined as \([\ell_1, \ell_2] \lor [\ell'_1, \ell'_2] = [\ell_1 \lor \ell'_1, \ell_2 \lor \ell'_2] \). For instance, the initial evidence for consistent judgment \( \succeq \) is:

\[
\mathcal{J}[\succeq] = \text{intr}(\text{bounds}(\succeq), \text{bounds}(\succeq))
\]

\[
= \text{intr}([H, \top], [L, \top])
\]

\[
= ([H, \top], [H, \top])
\]

A generalized definition of \( \mathcal{J} \), considering any consistent bounding judgment can be found in Fig. 28. The definition of \( \mathcal{J} \) extends naturally to compute the initial evidence for consistent subtyping judgments (the complete definition can be found in Fig. 29). For instance, in the (Tip) rule, \( \mathcal{J}[U_2 <: U_2 \lor U_2] \) computes the initial evidence for the consistent lifting of the fact that the type of the first branch is a subtype of the type of the entire conditional expression.

Rule \((T :)\) recursively translates the subterm \( t \), and the consistent subtyping judgment \( U_1 <: U_2 \) from \((S :)\) is replaced with \( \mathcal{J}[U_1 \leq U_2] \), which computes evidence \( e \) for consistent subtyping. This evidence is eventually placed next to the translated term \( t' \). The ascription itself is erased because it does not affect the results of the computation.

Rule \((T \text{app})\) works similarly. Since \( t_1 \) is not constrained by a consistent subtyping judgment, the rule generates evidence for reflexive consistent subtyping: that the type is a consistent subtype of itself. \( \mathcal{J}[U_{11} \xrightarrow{g'} U_{12}] \). This seemingly vacuous evidence evolves nontrivially as a program reduces. Evidence for the judgment \( g_c \lor g \leq g' \) is computed as \( \mathcal{J}[g_c \lor g \leq g'] \), and placed next to the @ symbol, since it does not logically belong to any subterm.

The rest of the translation rules are analogous: each term is translated recursively, judgments are replaced by functions that determine the corresponding initial evidence, and the evidence for reflexive consistent subtyping \( \mathcal{J}[\approx] \) is associated to otherwise unconstrained types.

As an example, consider the GSL-Ref program \( x := \text{true} \), with current security effect \( L \) and environment \( \Gamma \vdash x : \text{Ref}_\text{T} : \text{Bool}_\text{H} \). It elaborates to GSL as follows:

\[
\begin{align*}
\Gamma;.; L \vdash x & \leadsto x : \text{Ref}_\text{T} : \text{Bool}_\text{H} & \Gamma;.; L \vdash \text{true} & \leadsto \text{true} : \text{Bool}_\text{T} \\
\epsilon_1 = \mathcal{J}[\text{Ref}_\text{T} : \text{Bool}_\text{H}] & = \langle \text{Ref}_\text{L,T} : \text{Ref}_\text{L,T} : \text{Bool}_\text{H,T} \rangle & \epsilon_2 = \mathcal{J}[\text{Bool}_\text{T} \leq \text{Bool}_\text{H}] & = \langle \text{Bool}_\text{L,H}, \text{Bool}_\text{H,H} \rangle \\
\epsilon_3 = \mathcal{J}[L \lor ? \leq H] & = \langle \text{Unit}_\text{H,H} \rangle \\
\text{(Tassign)} & & \\
\Gamma;.; L \vdash x := \text{true} & \leadsto \epsilon_1 x := \epsilon_2 \text{true} : \text{Unit}_\text{H}
\end{align*}
\]

**Evolving evidence.** During reduction, evidence for consistent judgments must be combined to justify each reduction step. This combination is realized by two operators: **consistent transitivity for label ordering** and **consistent join monotonicity**.

The consistent transitivity operator \( \circ \) attempts to combine evidence for \( g_1 \sim g_2 \) and \( g_2 \sim g_3 \) to produce evidence for \( g_1 \sim g_3 \). Since \( \sim \) is not in general transitive, \( \circ \) is partial, giving rise to runtime errors. For instance, both \( H \sim ? \) and \( ? \sim L \) hold, but can they be combined to deduce that \( H \sim L \)? Of course not, otherwise high-confidence data could flow to low-confidence positions. To
understand this failure of consistent transitivity, consider the initial evidence for these judgments, \( \langle \mathbb{H}, \mathbb{H}, \mathbb{H}, \top \rangle \) and \( \langle \bot, \bot, \bot, \bot \rangle \). They cannot be combined because “they do not meet in the middle”, i.e. the middle intervals \( \mathbb{H}, \top \) and \( \bot, \bot \) share no labels in common, which would justify transitivity. This intuition is formalized as follows:

\[
\langle t_1, t_2 \rangle \circ \kappa \langle t_{22}, t_3 \rangle = \Delta^{\kappa}(t_1, t_{21} \cap t_{22}, t_3)
\]

where \( [\ell_1, \ell_2] \cap [\ell'_1, \ell'_2] = [\ell_1 \lor \ell'_1, \ell_2 \land \ell'_2] \) if \( \ell_1 \lor \ell'_1 \preceq \ell_2 \land \ell'_2 \)

and \( \Delta^{\kappa}([\ell_1, \ell_2], [\ell'_1, \ell'_2], [\ell''_1, \ell''_2]) =

\[
\langle [\ell_1, \ell_2 \land \ell'_2 \land \ell''_2], [\ell_1 \lor \ell'_1 \lor \ell''_1, \ell'_2 \land \ell''_2] \rangle
\]

if \( \ell_1 \preceq \ell'_2, \ell'_1 \preceq \ell''_2, \ell_1 \preceq \ell''_2 \)

The meet operator \( \cap \) denotes the intersection of two intervals. Given three intervals \( t_1, t_2, t_3 \), the \( \Delta^{\kappa} \) operator calculates, if possible, a pair of intervals \( \langle t'_1, t'_2 \rangle \subseteq \langle t_1, t_3 \rangle \) such that transitivity of label ordering through elements of \( t_2 \) is always plausible. Both operators are undefined if their side conditions do not hold.

The consistent join monotonicity operator \( \tilde{\gamma} \) reflects another facet of reasoning about consistent ordering relationships. Recall from Fig. 2 that during reduction, labels are sometimes joined, either for stamping values or for augmenting the security effect. Similarly, in GSL\(_{\text{Ref}}^e\) evidence must be combined to support new consistent judgments that involve these joined labels. Consistent join monotonicity combines evidence for \( g_1 \preceq g_2 \) and \( g_3 \preceq g_4 \) to produce evidence for \( g_1 \lor g_3 \preceq g_2 \lor g_4 \), the consistent lifting of the static judgment \( \ell_1 \lor \ell_3 \preceq \ell_2 \lor \ell_4 \).

\[
\langle t_1, t_2 \rangle \tilde{\gamma} \langle t'_1, t'_2 \rangle = \langle t_1 \lor t'_1, t_2 \lor t'_2 \rangle
\]

In contrast to consistent transitivity, this operator is total.

Lifting these label operators to types is direct, albeit verbose, and can be found in Appendix A.6. These type operators inherit properties from the label operators, e.g. consistent transitivity of subtyping \( \circ \kappa \) is partial just like consistent transitivity of label ordering.

**Reduction rules.** Fig. 6 presents reduction semantics for GSL\(_{\text{Ref}}^e\). Reduction operates on configurations \( C \), which consist of a term and a store, and a security effect. Specifically, \( t_1 \mid \mu_1 \xrightarrow{e} t_2 \mid \mu_2 \) denotes the reduction of term \( t_1 \) in store \( \mu_1 \) to term \( t_2 \) in store \( \mu_2 \) under security effect \( g_e \); the label evidence \( e \) confirms that the runtime security effect is a sublabel of the label that was used statically to type check the original term (and is preserved by reduction).

The semantics is defined using two notions of reduction, \( \xrightarrow{-} \) and \( \xrightarrow{-}_{<} \). The rules directly mirror the rules of SSL\(_{\text{Ref}}^e\) (Fig. 2), except that they also manage evidence at subexpression borders and combine evidence as needed to justify the preserved typing of the contractum. If evidence fails to combine, the program ends with an \textit{error}.

A word about notation: to select evidences for sub-components of types, we use evidence inversion functions [Garcia et al. 2016]. For instance, given a function type evidence \( e \), \( \text{idom}(e) \) (resp. \( \text{icod}(e) \)) retrieves the type evidence of the domain (resp. co-domain). Similarly, \( \text{ilat} \) retrieves latent effect evidence from the evidence for a function type, and \( \text{iref} \) performs likewise for reference types. Finally, given type evidence \( e \), \( \text{ilbl}(e) \) yields the corresponding label evidence.

We now describe each reduction rule in turn.

- Rule (r1) reduces a binary operation by joining the evidence of both operands to confirm that type preservation holds.
- Rule (r2) reduces a protected value by stamping the security effect of the prot on the value and joining both evidences accordingly. We stamp \( g_1 \) on the value to prevent it from leaking

...
\( (r1) \quad \epsilon_1(b_1) \otimes \epsilon_2(b_2) \mid \mu \xrightarrow{\epsilon gc} (\epsilon_1 \lor \epsilon_2)(b_1 \otimes b_2) \mid \mu \xrightarrow{\epsilon gc} C \times (C \cup \{\text{error}\}) \)

\( (r2) \quad \text{prot}_{\epsilon_1 \epsilon_2}(\epsilon_3 u) \mid \mu \xrightarrow{\epsilon gc} (\epsilon_3 \lor \epsilon_1)(u \lor g_1) \mid \mu \)

\( (r3) \quad \epsilon_1(\lambda^x : U.t) \otimes \epsilon_2 u \mid \mu \xrightarrow{\epsilon gc} \begin{cases} \text{prot}_{\text{ilbl}(\epsilon_1)}g(\epsilon_1'g'(icod(\epsilon_1)([\epsilon_2' u / x]t))) \mid \mu & \text{error if } \epsilon_1' \text{ or } \epsilon_2' \text{ are not defined} \\ \text{where:} & \\ \epsilon_1' = (v \lor \text{ilbl}(\epsilon_1)) \circ \epsilon_3 \circ \text{ilat}(\epsilon_1) \\ \epsilon_2' = \epsilon_2 \circ \epsilon_3 \circ \text{idom}(\epsilon_1) \\ g_1' = (g \lor g_1) \end{cases} \)

\( (r4) \quad \text{if } \epsilon_1 b_1 \text{ then } t_2 \text{ else } t_3 \mid \mu \xrightarrow{\epsilon gc} \begin{cases} \text{prot}_{\text{ilbl}(\epsilon_1)}g(\epsilon_2 t_2) \mid \mu & \text{if } b = \text{true} \\ \text{prot}_{\text{ilbl}(\epsilon_1)}g(\epsilon_3 t_3) \mid \mu & \text{if } b = \text{false} \\ \text{where:} & \\ \epsilon' = \epsilon \lor \text{ilbl}(\epsilon_1) \\ g' = g \lor g_1 \end{cases} \)

\( (r5) \quad \text{ref}^{U}_{\epsilon_2}(\epsilon_1 u) \mid \mu \xrightarrow{\epsilon gc} \begin{cases} \emptyset \mid \mu[o \mapsto \epsilon'(u \lor g_1)] & \\ \text{error} & \text{if } (\epsilon \circ \text{ilbl}(\epsilon_2)) \text{ is not defined} \\ \text{where:} & \\ o \notin \text{dom}(\mu) \\ \epsilon' = \epsilon \lor \text{ilbl}(\epsilon_2) \end{cases} \)

\( (r6) \quad !\epsilon_1 o_g \mid \mu \xrightarrow{\epsilon gc} \text{prot}_{\text{ilbl}(\epsilon_1)}g'(\text{iref}(\epsilon_1)u) \)

\( (r7) \quad \epsilon_1 o_g := \epsilon_3 \epsilon_2 u \mid \mu \xrightarrow{\epsilon gc} \begin{cases} \text{unit}_\bot \mid \mu[o \mapsto \epsilon'(u \lor (g \lor g_1))] & \text{error if } \epsilon' \text{ is not defined, or } \epsilon \mid \leq \text{ilbl}(\epsilon'') \text{ does not hold} \\ \text{where:} & \\ \mu(o) = u \\ \epsilon' = \epsilon \lor \text{ilbl}(\epsilon_1) \\ g' = g \lor g_1 \end{cases} \)

\( \epsilon_1(\epsilon_2 u) \xrightarrow{\epsilon'} \begin{cases} \text{error} & \text{if } \epsilon' \text{ is not defined, or } \epsilon \mid \leq \text{ilbl}(\epsilon'') \text{ does not hold} \end{cases} \)

Fig. 6. GSL_{Ref} \text{: Dynamic semantics}
information to the current context when \( g_1 \) is more confidential than the current security effect \( g_c \). Note that \( g_2 \)—which represents the join between \( g_1 \) and the current security effect \( g_c \)—is not used in this rule; it is used during reduction of the protected subterm.

- Rule \((r3)\) reduces a function application either to a protected body or to an error. The term reduces to an error if consistent transitivity fails to justify that the type of the actual argument is a consistent subtype of the formal argument type. This prevents an evident invalid information flow from the actual argument to the formal argument. Also, to prevent implicit flows via the store, an error is signaled if consistent transitivity fails to confirm that the latent effect of the function is greater than both the current security effect and that of the function. If the function application is valid, then the body is protected at the security level of the function. Label \( g'_1 \) represents the security effect that is used to reduce the body, where \( \epsilon'_1 \) confirms that \( g'_1 \) is no more confidential than the latent effect \( g' \).

- Similarly, rule \((r4)\) reduces a conditional expression by protecting the chosen branch. The resulting prot term is constructed using the dynamic information of the conditional.

- Rule \((r5)\) reduces a reference term to a fresh location. To prevent invalid implicit flows, the current security effect is stamped on the stored value. The term reduces to an error if consistent transitivity fails to confirm that the current security effect is lower than the statically-determined security level of the reference content \( U \).

- Rule \((r6)\) reduces a dereference term. In the dynamic semantics of SSL\(_{\text{Ref}}\), dereferencing a store location causes the actual security of the location to be stamped on the resulting value. Here, the term reduces instead to a protected expression, which is equivalent but simplifies the proofs.

- Rule \((r7)\) is critical to ensuring noninterference. It can reduce to an error, and thereby preventing either implicit or explicit invalid flows, for three reasons:
  1. the security level of the stored value should be no more confidential than the statically-determined security level of the reference content (explicit flow).
  2. both the current security effect and the actual security level of the reference should be no more confidential than the static security level of the reference content (implicit flow).
  3. the evidence of the current security effect must denote possible labels that are necessarily lower than those denoted by the evidence of the stored value (implicit flow).

The third condition above, highlighted in gray in Fig. 6, is expressed with the lower-bound comparison operator \([\leq]\) between evidences:

\[
\langle [\ell_1, \ell_2], [\ell_3, \ell_4] \rangle \leq \langle [\ell'_1, \ell'_2], [\ell'_3, \ell'_4] \rangle \iff \ell_3 \leq \ell'_3
\]

This check is necessary to ensure noninterference, and as explained in Sec. 6.3, it arises not from the type preservation argument, but from the noninterference argument. In Sec. 4.3 we illustrate each of these three scenarios.

The \( \rightarrow_{\epsilon} \) reduction rule uses consistent transitivity to combine, if possible, strings of evidence that accumulate on a raw value. It fails with a runtime error if the evidence cannot be combined. Sec. 4.3 presents an example of such a reduction.

Finally, contextual term reduction is specified using term frames \( f \) and evidence frames \( h \):

\[
\begin{align*}
f &::= b(\ell)[] \\
h &::= \square \odot \ddot{e}t | \ddot{e}u \oplus \square | \square @_\ddot{e} \ddot{e}t | \ddot{e}u @_\ddot{e} \square | \ddot{e} \square | \ddot{e} \ddot{e}t \text{ if } \ddot{e}t \text{ else } \ddot{e}t | ! \square | \square :=_\ddot{e} \ddot{e}t | \ddot{e}u :=_\ddot{e} \square | \text{ref}_U \end{align*}
\]

The reduction rules for frames are presented in Fig. 7. Rule \((Rf)\) reduces under term frames. Rule \((\rightarrow)\) reduces a term to either a term or error, using \( \rightarrow \) from Fig. 6. Similarly Rules \((Rh)\) and \((Rprot)\) reduce the subterm using the evidence-combining reduction \( \rightarrow_{\epsilon} \). Rule \((Rprot)\) allows the protected subterm to step under a higher security level, which may be a sublabel of the one
determined statically. Finally, rules (Rferr) and (Rproterr) propagate errors when the subterm reduces to an error, and rules (Rherr) and (Rprot(err)) propagate errors when evidence fails to combine.

4.3 Examples of Reduction

To illustrate the runtime semantics of GSL<sub>Ref</sub> we first illustrate the three scenarios for which an assignment can fail, as per Rule (r7).

(1) Consider the following program, which attempts to assign a high-confidentiality value into a low-confidentiality reference, and its translation (under security effect ⊥):

\[ \bot \vdash \text{ref}^\text{int}_L \text{:: Ref}_L \Downarrow t : \text{Unit}_L \]

Abbreviating \([\bot, \top] \) as \?, \([\ell, \ell] \) as \ell, \([i, i] \) as \iota, and \_ for irrelevant evidence, we have:

\[ t \Downarrow^* \epsilon_1 \text{a}_L := \_ \epsilon_2 10_L \]

where \( \epsilon_1 = \langle \text{Ref}_L \text{:: Int}_L \rangle \) and \( \bot \vdash \text{ref}^\text{int}_L \text{:: Ref}_L \text{:: Int}_L \subseteq \text{Ref}_L \text{:: Int}_L \), \( \epsilon_2 = \langle \text{Int}_H, \text{Int}_L, \text{Int}_T \rangle \) and \( \bot \vdash \text{int}_H \subseteq \text{Int}_L \). Then as \( \epsilon_2 \circ<: \text{iref}(\epsilon_1) \) is not defined, the term reduces to an error, as expected.

(2) The following program attempts to update a low-confidentiality reference under a high-confidentiality security effect. Considering a security effect \(?\), a location \( \vdash \text{a}_L : \text{Ref}_L \text{:: Int}_L \), the program and its translation are:

\[ \bot \vdash \text{true}_L \text{:: Bool}_L \text{:: Ref}_L \text{:: Int}_L \text{:: Unit}_L \Downarrow t : \text{Unit}_L \]

The conditional reduces to the first branch under a security effect \( H \).

\[ t \Downarrow^* \text{prot}_H \langle \epsilon_1 \rangle H(\langle \epsilon_2 \text{a}_L := \_ \epsilon_3 \_ \text{10}_L \rangle) \]

where \( \epsilon_1 = \langle H, [H, T] \rangle \) and \( \bot \vdash \text{ref}^\text{int}_L \text{:: Ref}_L \text{:: Int}_L \subseteq \text{Ref}_L \text{:: Int}_L \). Also, because the static security effect of the assignment is \?, we have \( \epsilon_3 = \langle [\bot, \bot], \bot \rangle \) and \( \bot \vdash \text{?}\bot \subseteq \bot \).
Then as \(((\varepsilon_1 \bowtie \text{ibl}(\varepsilon_2))) \circ \varepsilon_3 \circ \varepsilon \text{ibl}(\text{iref}(\varepsilon_2))) = \langle H, [H, \top] \rangle \circ \varepsilon \langle [\bot, L], L \rangle \circ \varepsilon \langle L \rangle \) is not defined, the term reduces to an error, successfully preventing an invalid implicit flow.

(3) Consider a program fragment similar to the previous one, with security effect \(\bot\), a variable \(x : \text{Bool}_H\), and a location \(\vdash o_\bot : \text{Ref}_\bot \text{Int}_Y\):

\[\bot \vdash x :: \text{Bool}_H; \text{then } o_\bot := \text{10}_H \text{ else } \text{unit}; \sim t : \text{Unit}\]

Suppose as well that \(\mu(o) = \varepsilon_202\), where \(\text{ibl}(\varepsilon_2) = \langle [\bot, \top], [\bot, \top] \rangle \vdash ? \prec ? \) (i.e. the stored number and heap cell have not acquired any security commitments yet). If \(x\) is \(\text{true}_H\), then the first branch is taken:

\[t \overset{\downarrow}{\longrightarrow} \text{prot}_H \varepsilon_1 (\text{H}(\_\_ o_\bot := \_\_ \text{10}_H))\]

where \(\varepsilon_1 = \langle H, [H, \top] \rangle \vdash \bot \Rightarrow \bot \leq \bot \Rightarrow \gamma \). Since \(\varepsilon_1 \downarrow \leq \gamma \) \(\text{ibl}(\varepsilon_2)\) is not defined, because \(H \not\vdash \bot\), the program reduces to an error. The problem is that if \(x\) were changed to \(\text{false}_H\), the unchanged imprecisely labeled contents of \(o\) could be treated as low-security and thereby used to leak information about \(x\), using for instance a test of \(!o\) that conditionally assigns to some other low-security reference (for more see the example of Sec. 2, and Sec. 6.3).

**Type-based reasoning.** Finally, we revisit the \(\text{mix}\) and \(\text{smix}\) functions from Sec. 2, which illustrate how \(\text{GSL}_\text{Ref}\) preserves type-based reasoning principles in the gradual setting. The desugared \(\text{GSL}_\text{Ref}\) program follows:\(^{10}\)

\[\text{mix} = (\lambda \text{pub} :: L.(\lambda \text{priv} :: ?.(? \text{if pub} < \text{priv} \text{then 1}_L \text{ else 2}_L :: L)L)L\]

\[\text{smix} = \text{mix} :: L \rightarrow H \rightarrow L\]

\[\text{smix} 1_L 5_L\]

This program elaborates to the following \(\text{GSL}_\text{Ref}^\epsilon\) program:

\[\text{mix} = (\lambda \text{pub} :: L.(\lambda \text{priv} :: ?.(? \text{if pub} < ? \text{priv} \text{then} (L)1_L \text{ else} (L)2_L :: L)L)L\]

\[\text{smix} = (\lambda L :: \text{L} \rightarrow [H, \top] \rightarrow L, L \rightarrow H \rightarrow L)L\text{mix}\]

\[\langle H \rightarrow L \rangle (L \rightarrow H \rightarrow L)\text{smix} \circ (L)1_L \circ (L)H)\langle [L, H] \rangle 5_L\]

A trace of the program is given in Fig. 8. As before, we abbreviate \([\bot, \top]\) as \(?\), \([\ell, \ell]\) as \(\ell\), and \((i, i)\) as \((i)\). We omit the security effect of the reduction, which is always \(\langle \bot \rangle \bot\), as well as the heap, since the program is pure. The program fails as expected because low-security evidence is attached to the conditional term by a static ascription, which fails to combine with the high-security evidence of the value produced by the conditional. In other words, reduction fails to prove that \(H \leq L\).

### 4.4 \(\text{GSL}_\text{Ref}:\) Safety and Graduality

\(\text{GSL}_\text{Ref}\) satisfies a standard type safety property, whose proofs are in the companion technical report [Toro et al. 2018]. More precisely, type safety is formulated for the evidence-augmented language \(\text{GSL}_\text{Ref}^\epsilon\), and hence appeals to a corresponding typing judgment. As expected, this typing judgment, denoted \(\Gamma; \Sigma; \varepsilon g_\ell \vdash t : U\), is based on the \(\text{GSL}_\text{Ref}\) typing judgment.\(^{11}\) The only difference is that the security effect \(g_\ell\) is enriched with evidence \(\varepsilon\). This evidence accounts for how the runtime security effect can evolve to (consistently) lower levels than the security effect originally determined by the type system.

---

10For brevity, we only show the labels of base types, and omit latent effect annotations on pure functions.

11The full definition of the \(\text{GSL}_\text{Ref}^\epsilon\) type system can be found in Appendix A.4; the (straightforward) theorem that elaboration preserves typing is in the companion technical report [Toro et al. 2018].
Proposition 4.1 (Type Safety). If $\vdash \Sigma; \epsilon \ell_c \vdash t : U$, and consider $\mu$, such that $\Sigma \vdash \mu$, then either:

- $t$ is a value $\nu$
- $t \mid \mu \quad \epsilon_{\ell_c} \rightarrow \text{error}$
- $t \mid \mu \quad \epsilon_{\ell_c} \rightarrow t' \mid \mu'$ and $\vdash \Sigma'; \epsilon_{\ell_c} \vdash t' : U$ for some $\Sigma' \supseteq \Sigma$ such that $\Sigma \vdash \mu'$

Additionally, by design, the type system of GSL_{Ref} is crisply and smoothly connected to that of SSL_{Ref}. First, the two typing judgments are crisply connected in that the GSL_{Ref} judgment conservatively extends the SSL_{Ref} one.

Proposition 4.2 (Static Conservative Extension). Let $\vdash_S$ denote SSL_{Ref}'s type system. Then for any static language term $t \in \text{TERM}$, $\vdash \Sigma; \ell_c \vdash_S t : S$ if and only if $\vdash \Sigma; \ell_c \vdash t : S$.

Second, the two typing judgments are smoothly connected in that each well-typed GSL_{Ref} program (thus each SSL_{Ref} one) preserves well-typing as its security information is made less precise, a property known as the static gradual guarantee [Siek et al. 2015]. Precision orders the static information content of gradual type or labels from most to least. Type and label precision are defined as follows:
Type and label precision are naturally lifted to term precision.

**Proposition 4.4 (Static Gradual Guarantee).** Suppose \( g_{c1} \sqsubseteq g_{c2} \) and \( t_1 \sqsubseteq t_2 \). If \( \cdot ; \cdot ; g_{c1} \vdash t_1 : U_1 \) then \( \cdot ; \cdot ; g_{c2} \vdash t_2 : U_2 \) where \( U_1 \sqsubseteq U_2 \).

This guarantee is best understood in reverse: if a simply-typed program (where all security labels are ?) has a security-typed counterpart (where all security labels are precise), then GSL\(_{\text{Ref}}\) statically accepts every intermediate security typing of that program: type checking is continuous with respect to security precision, so security information can be added in any order and at any rate [Siek et al. 2015].

[Siek et al. 2015] also present a dynamic gradual guarantee, which relates the execution behavior of programs that only differ in their precision. Specifically, if a program takes a step, then the same program with less precise (or fewer) type annotations also takes a step, i.e. reducing precision does not introduce new runtime errors. The formal statement of the guarantee can be found in the companion technical report [Toro et al. 2018]. Unfortunately, we have uncovered a tension between the dynamic gradual guarantee and noninterference. To ensure noninterference, the dynamic semantics of GSL\(_{\text{Ref}}\) includes a specific runtime check (highlighted in gray in Fig. 6) which breaks the dynamic gradual guarantee. Dually, without this check, GSL\(_{\text{Ref}}\) satisfies the dynamic gradual guarantee, but does not enforce noninterference for all programs. We discuss this subtlety in more detail in Sec. 6.3.

Nevertheless, an interesting conservative extension result holds for the dynamic semantics. Specifically, static GSL\(_{\text{Ref}}\) terms never produce errors at runtime.

**Proposition 4.5 (Static Terms Do Not Fail).** Let StaticTerm be the static subset of GSL\(_{\text{Ref}}\) terms, i.e. with fully-static annotations, and StaticStore the set of stores whose codomains are subsets of StaticTerm. Then consider \( t \in \text{StaticTerm} \), \( \mu \in \text{StaticStore} \), and \( \epsilon \ell_c \) such that \( \epsilon = g \| [\ell_c \prec \ell_c'] \).

If \( \cdot ; \cdot ; \epsilon \ell_c \vdash t : U \), then either \( t \) is a value, or \( t \mid \mu_s \xrightarrow{\ell_c} t_s' \mid \mu'_s \), with \( t' \in \text{StaticTerm} \) and \( \mu' \in \text{StaticStore} \).

### 4.5 Prototype Implementation

We have implemented GSL\(_{\text{Ref}}\) in an interactive prototype available online at: [https://pleiad.cl/gradual-security/](https://pleiad.cl/gradual-security/).

The implementation, realized in Scala, supports all of GSL\(_{\text{Ref}}\) plus let-bindings. Given a source program, it either shows the result of the elaboration to GSL\(_{\text{Ref}}\), or reports a static type error. If the source program is well-typed, the evidence-augmented term can be explored interactively, either collapsing or expanding premises of its well-typedness, including evidences. The user can then reduce the term step by step, similarly to PLT Redex’s trace facility. At each step, the full typing derivation of the term can again be explored. The reduction shows how evidences are combined by consistent subtyping transitivity, eventually ending up in a value or a runtime security error.

All examples presented in this paper are available as pre-loaded source examples.
5 GSLRef: NONINTERFERENCE

This section establishes the type soundness of GSLRef, i.e. that gradual security types ensure noninterference. Noninterference formalizes the intuition that low-security observers of a computation cannot detect changes in high-security inputs. Therefore noninterference inherently reflects a relationship between different runs of the same program with different inputs. We establish noninterference for GSLRef using logical relations [Heintze and Riecke 1998; Zdancewic 2002]. More precisely, because general references introduce nontermination, we apply step-indexed relations [Ahmed 2004]. As standard, we focus on termination-insensitive noninterference: interference between two executions is only acknowledged when both terminate in values that are observably different. In line with prior work on gradual security [Disney and Flanagan 2011; Fennell and Thiemann 2013], we consider runtime check errors to be akin to non-termination, because in principle the semantics could deal with errors by diverging and directly reporting the error through a secure channel.

Observing values. The security type of a value dictates both an observation protocol and the clearance required to observe it. Consider a value \( v : U_1 \rightarrow g U_2 \), and an observer with security level \( \ell_o \). Can \( \ell_o \) observe the value? If so, what observations can it make? First, \( \ell_o \) cannot make any observations if its security level does not subsume that of the function \( (g \triangleright \ell_o) \). If clearance is granted \( (g \triangleright \ell_o) \), then \( \ell_o \) may make observations in accordance with the structure of \( v \)'s type: it may construct another value \( v' : U_1 \) and apply it to the function; the observations that \( \ell_o \) can make of the result are then dictated by the type \( U_2 \triangleright g \).

The predicate \( \text{obsVal}_{\ell_o} \), defined formally below, intuitively captures what it means for a value \( v \) of type \( U \) to be observable at \( \ell_o \): \( \ell_o \) must be consistently greater than the security label of \( U \). To account for the gradual security setting, we need to extend this intuitive notion in two ways. First, observation must deal with the potential for values to carry type ascriptions, such as \( v = \text{true}_H : \text{Bool}_H \). An observer at security level \( L \) must not observe the underlying high-security value. The key intuition is that the observation should ultimately be equivalent to applying the source language context if \( \square :: \text{Bool}_H \) then \( \text{true}_L \) else \( \text{false}_L \) to the value, thereby asserting credentials and then using them. Doing so would trigger a runtime check error, which amounts to a non-observation. In GSLRef, \( v \) would be represented as an evidence value \( \epsilon \text{true}_H \), where \( \epsilon \) confirms that \( \text{Bool}_H \triangleright \text{Bool}_H \). We capture the observability of the underlying value by defining the notion of observable evidence at a given observation level. Then, an evidence value \( \nu = \epsilon u \) is observable if its label evidence \( \text{illbl}(\epsilon) \) is observable.

Definition 5.1 (Observable evidence). Suppose observation level \( \ell_o \) and an evidence judgment \( \epsilon \vdash v \triangleright g \triangleright g' \) for some \( g \) and \( g' \). For the evidence \( \epsilon \) to be observable at \( \ell_o \), it must be possible to confirm \( g \triangleright \ell_o \) using consistent transitivity of label ordering through \( g' \). Formally:

\[
\text{obsEv}_{\ell_o}^{g'}(\epsilon) \iff \epsilon \circ \triangleright [g' \triangleleft \ell_o]
\]

Second, observation must account for dynamic security effect clearance: observation leaks a value from its context, so the observer must have the proper credentials. Recall that execution happens under a dynamic security effect \( g \) that, at runtime, can be consistently lower than the security effect originally determined by the type system. Therefore the dynamic security effect is accompanied by evidence \( \epsilon \) that confirms that \( g \triangleright g' \), where \( g' \) is the static security effect. Observation is allowed if such evidence is observable, i.e. \( g \triangleright \ell_o \).

Adding these two refinements of observability to the original notion of observable value yields the following definition.
Definition 5.2 (Observable value). Given an observation level $\ell_o$, we define that a value $v$, typed as $U$, is observable as:

$$\text{obsVal}^U_{\ell_o}(v) \iff g \sim \ell_o \land \big( (v = e_1 u) \Rightarrow \text{obsEv}^\beta_{\ell_o}(ilbl(e_1)) \big)$$

where $g = \text{labell}(U)$

Security logical relations. We define logical relations between both computations and values in Figs. 9 and 10. The notions of related values and related computations are mutually recursive, as explained below. Note that the logical relations are only defined for pairs of GSL$_\text{Ref}$ terms that have the same type $U$, so simple type safety ensures that the behaviors dictated by $U$ will produce defined behavior (including runtime error). To make the relations well-defined in the presence of nontermination, we index them on the number of steps $k$ that the observer $\ell_o$ may take. If no inequivalent observations are made after $k$ steps, the terms are deemed equivalent. Ultimately we require that $\ell_o$ observes equivalence for any arbitrary number of steps, which implies that nonterminating computations also respect the noninterference guarantees. This is the essence of step-indexing [Ahmed 2004].

The definition of related values is presented in Fig. 9. We use notation $\hat{g}_i$ to denote the evidence-augmented security context $\epsilon_i g_i$. The notation $\Sigma; g_c \vdash (\hat{g}_1, v_1, \mu_1) \approx^k_{\ell_o} (\hat{g}_2, v_2, \mu_2) : U$ indicates that the triple of security context $\hat{g}_i$, value $v_1$ and store $\mu_1$, is related to the triple of dynamic security context $\hat{g}_2$, value $v_2$ and store $\mu_2$ at type $U$ for $k$ steps under store typing $\Sigma$ and static security context $g_c$ when observed at the security level $\ell_o$. For two such triples to be related, four conditions must be satisfied:

1. The security effects must be related under security effect $g_c$, meaning they denote execution contexts that are either both above $\ell_o$ (high-security), or both below (low-security). Formally, two security effects are related if their underlying evidences are either both observable or both not observable:

$$g_c \vdash \epsilon_1 g_1 \approx \ell_o \epsilon_2 g_2 \iff (\text{obsEv}^\beta_{\ell_o}(\epsilon_1) \land \text{obsEv}^\beta_{\ell_o}(\epsilon_2)) \lor (\lnot \text{obsEv}^\beta_{\ell_o}(\epsilon_1) \land \lnot \text{obsEv}^\beta_{\ell_o}(\epsilon_2))$$

where $\epsilon_1 \vdash g_1 \sim g_c$.

2. The stores must be related for $k$ steps under store typing $\Sigma$, notation $\Sigma; \vdash \mu_1 \approx^k_{\ell_o} \mu_2$. This means that, for locations that are common to both stores, the stored values are related at $j < k$ steps. Formally:

$$\Sigma; \vdash \mu_1 \approx^k_{\ell_o} \mu_2 \iff \forall j < k, \exists \Sigma; \vdash g_c \vdash (\hat{g}_j, \mu_1 \approx_{\ell_o} \hat{g}_j, \mu_2) : (\Sigma(U))$$

In particular, stored values must be related at all related security effects $\hat{g}_1, \hat{g}_2$. This generality is necessary because all reference operations involve stamping the current security effect (and its evidence) onto the stored value, and doing so must preserve relatedness. For instance, two runs of a program can update a store location with different values under a high-security effect because both will be stamped high-security, and thus indistinguishable by a low-security observer $\ell_o$.

3. The values must both have the same type $U$ under an empty type environment and valid store type.

4. The values must be either both observable or both not observable. If the values are not observable, they are deemed equivalent. If they are observable, then they must be related at their specific type, as specified by the auxiliary relation $\text{obsRe}_{\ell_o}^{\epsilon_2 g_2, U}$, defined by case analysis on $U$. If $U$ is either $\text{Bool}_g$, $\text{Unit}_g$ or $\text{Ref}_g U'$, two values are related simply if their raw values

\footnote{For simplicity and without loss of generality, like Austin and Flanagan [2009], we assume that a new reference in two related executions is allocated at the same address.}
The judgment $\Gamma \vdash \mathsf{obsVal}_{\ell_o}^U (v_1) \land \neg \mathsf{obsVal}_{\ell_o}^U (v_2) \land (\mathsf{obsVal}_{\ell_o}^U (v_1) \land \mathsf{obsEv}_{\ell_o}^{\mathsf{Ref}_g} (\epsilon_1)) \Rightarrow \mathsf{obsRel}_{\ell_o}^{\Sigma} (\hat{g}_1, v_1, \mu_1, \hat{g}_2, v_2, \mu_2)$

\[
\mathsf{obsRel}_{\ell_o}^{\Sigma} (\hat{g}_1, v_1, \mu_1, \hat{g}_2, v_2, \mu_2) \iff \mathsf{rval}(v_1) = \mathsf{rval}(v_2) \quad \text{if } U \in \{\mathsf{Bool}_g, \mathsf{Unit}_g, \mathsf{Ref}_g U'\}
\]

\[
\mathsf{obsRel}_{\ell_o}^{\Sigma} (\hat{g}_1, v_1, \mu_1, \hat{g}_2, v_2, \mu_2) \iff \forall j \leq k, \forall U' = U_1 \mathord{\xrightarrow{\epsilon_1}} \hat{g}_1 U_2, \forall U_2', \forall g'_c, \forall \hat{g}'_1, \text{ where } \epsilon_1 \vdash g'_c \not\lessdot g'_c, \text{ s.t. } \hat{g}_1 \leq \ell_o \hat{g}'_1,
\]

\[
\epsilon_1 \vdash U_1 \mathord{\xrightarrow{\epsilon_{11}}} \hat{g}_1 U_2 \subseteq U', \epsilon_{12} \vdash U_2' \subseteq U', \text{ and } \epsilon_{31} \vdash \mathsf{dom}(\mu_1) \subseteq \mathsf{dom}(\mu'_1),
\]

\[
\forall v_1', \mu'_1, \Sigma', \Sigma' \subseteq \Sigma, \Sigma'; \hat{g}_1 \vdash (\hat{g}_1, v_1', \mu'_1) \mathord{\approx_{\ell_o}} (\hat{g}_2, \mu_2', v_2) : U_1' \mathord{\xrightarrow{\mu'_1}} \mathsf{dom}(\mu_1) \subseteq \mathsf{dom}(\mu'_1),
\]

\[
\Sigma'; \hat{g}_1 \vdash (\hat{g}_1 (\epsilon_{11} v_1 @ \epsilon_{31} \epsilon_{12} v_1), \mu'_1) \mathord{\approx_{\ell_o}} (\hat{g}_2 (\epsilon_{11} v_2 @ \epsilon_{31} \epsilon_{12} v_2), \mu'_2) : C(U_2' \mathord{\negarrow} \hat{g}_1)
\]

Fig. 9. Related values

The definition of related computations is presented in Fig. 10. First, two triples of security effect, term, and store are related computations for k steps at type $U$ if the security effects and the stores are related, as defined previously. Second, the terms must have type $U$ under any observationally higher security effect $\hat{g}'$. We say $\hat{g}' = \epsilon' g'$ is observationally higher than $\hat{g} = \epsilon g$, notation $\hat{g} \leq_{\ell_o} \hat{g}'$ if $\neg \mathsf{obsEv}^{\mathsf{Ref}_g}_{\ell_o} (\epsilon) \Rightarrow \neg \mathsf{obsEv}^{\mathsf{Ref}_g}_{\ell_o} (\epsilon')$, where $\epsilon \vdash g \not\lessdot g_c$ and $\epsilon' \vdash g' \not\lessdot g'_c$. For instance, in the static language it is the case that for any $\ell$, $H \leq_{\ell_o} H \land \ell$, because by monotonicity of the join $H \lor \ell_o \Rightarrow H \lor \ell$, additionally, for any $j < k$, if both terms can be reduced for at least $j$ steps under security effect $\hat{g}'$, then the resulting stores should be related for the remaining $k - j$ steps. Finally, if the resulting terms are irreducible, they must be related values for the remaining $k - j$ steps at type $U$, as defined previously. The logical relation relates computations that do not terminate as long as the stores are also related after $k$ steps.

Noninterference. Armed with these logical relations, we can state a semantics-driven notion of noninterference, and prove that well-typed terms of the internal language are sound with respect to it. The judgment $\Gamma; \hat{g} \models t : U$ says that term $t$ is semantically well-typed, meaning that it respects the security protocol $U$ for all observers, substitutions, stores, and steps [Ahmed 2004].

---

13This requirement is motivated by the proof, in order to obtain a stronger induction hypothesis [Toro et al. 2018].
Definition 5.3 (Semantic Security Typing).

\[ \Gamma; \Sigma; \hat{g} \vdash t : U \iff \forall \ell_o \in \text{LABEL}, k \geq 0, \rho_1, \rho_2 \in \text{SUBST} \text{ and } \mu_1, \mu_2 \in \text{STORE}, \forall g_c, \hat{g} = \varepsilon g, \]
\[ \varepsilon \vdash g \preceq g_c, \text{ such that } \Sigma \vdash \mu_1 \text{ and } \Gamma; \Sigma; g_c \vdash (\hat{g}, \rho_1, \mu_1) \approx^k_{\ell_o} (\hat{g}, \rho_2, \mu_2), \]
\[ \text{we have } \Sigma; g_c \vdash (\hat{g}, \rho_1(t), \mu_1) \approx^k_{\ell_o} (\hat{g}, \rho_2(t), \mu_2) : \mathcal{C}(U) \]

The definition above appeals to a notion of related substitutions. Indeed, the term \( t \) may have free variables, indicating “input parameters”. The term is semantically well-typed if applying related substitutions (and stores) yields related computations at type \( U \), for any number of steps \( k \), and for any observer \( \ell_o \). Two substitutions are related if they map each variable in the term to related closed values:

Definition 5.4 (Related substitutions). Tuples \((g_1, \rho, \mu_1)\) and \((g_2, \rho, \mu_2)\) are related on \( k \) steps under \( \Gamma, \Sigma \) and \( g_c \), notation \( \Gamma; \Sigma; g_c \vdash (g_1, \rho_1, \mu_1) \approx^k_{\ell_o} (g_2, \rho_2, \mu_2) \), if \( \rho_1 \models \Gamma \), \( \Sigma + \mu_1 \approx^k_{\ell_o} \mu_2 \) and

\[ \forall x \in \text{dom}(\Gamma), \Sigma; g_c \vdash (g_1, \rho_1(x), \mu_1) \approx^k_{\ell_o} (g_2, \rho_2(x), \mu_2) : \Gamma(x) \]

Note that because a low-security observer equates all high-security values, the actual substitutions and stores can be wildly different, up to the strictures that the logical relation imposes on their types.

Finally, Security Type Soundness says that the syntactic type system enforces noninterference.

Proposition 5.5 (Security Type Soundness). \( \Gamma; \Sigma; \hat{g} \vdash t : U \implies \Gamma; \Sigma; \hat{g} \models t : U \)

6 DERIVING GSL\textsubscript{Ref} WITH AGT (ALMOST)

So far the presentation of GSL\textsubscript{Ref} has focused on describing the language as it is and its properties, without explaining how it came to be designed that way. Several definitions in both the static and dynamic semantics may seem to come out of nowhere, and hard to accept without further justification.

This work originated in part from our desire to apply the Abstracting Gradual Typing (AGT) methodology [Garcia et al. 2016] in a challenging setting. Indeed, AGT has been shown to be effective in different contexts: records and subtyping [Garcia et al. 2016], static semantics of gradual effects [Bañados Schwerter et al. 2014, 2016], gradual unions [Toro and Tanter 2017], as well as refinement types [Lehmann and Tanter 2017] and set-theoretic types [Castagna and Lanvin 2017]. But AGT has never been applied to a type discipline that denotes a relational property over multiple executions.

Therefore, we have systematically derived GSL\textsubscript{Ref} from SSL\textsubscript{Ref} using AGT. This methodology, which starts from considering gradual types as abstractions of static types, drove the entire design of GSL\textsubscript{Ref}. The abstract interpretation framework of AGT provides definitions—semantically-defined notions—which may be hard to implement directly. From these definitions, we devise equivalent algorithmic characterizations—easily implementable, but hard to convincingly justify informally. AGT also explains how to derive the dynamic semantics of a gradual language based on the type safety argument of the static language. In Sec. 4 we try to convey guiding intuitions, but in this section we show how the definitions are not driven by intuition, but rather formally justified by AGT. Each algorithmic characterization from Sec. 4 is equivalent to its semantic definition, obtained using AGT and presented hereafter. These equivalences are proven in the companion technical report [Toro et al. 2018].

Before diving into the subtleties of applying AGT to security typing, we quickly describe the main elements of the AGT approach as spelled out by Garcia et al. [2016]: its inputs, steps, and outputs.
AGT in a nutshell. The AGT methodology proposes to derive the static and dynamic semantics of a gradual language in the following manner:

1) Deriving the statics.
   (a) Start from a language with a fully-static typing discipline, including the particulars of its type safety proof.
   (b) Define the syntax of gradual types, and give them meaning via a concretization function, which maps gradual types to sets of static types; then define the corresponding most precise abstraction function, forming a Galois connection.
   (c) Lift type predicates and functions used in the type system of the static language through the Galois connection to obtain the gradual type system.

2) Deriving the dynamics.
   (a) Define the structure of evidence for consistent judgments, which represents justification for why such a judgment holds; this representation depends on a Galois connection—usually the same as the one used for deriving the static semantics.
   (b) Reduce gradual programs by reducing gradual typing derivations decorated with evidence, mirroring reasoning steps of the static language’s type safety proof, hence exploiting the correspondence between proof normalization and term reduction [Howard 1980].

Therefore, the “inputs” to AGT are only the static language, and the Galois connection(s) that give meaning to gradual types and evidences. As “output”, one obtains the static and dynamic semantics of the gradual language, together with the guarantee that it is type safe, is a conservative extension of the static discipline, and satisfies the gradual guarantees.

Note that, as alluded to above, in order to achieve an implementation one must also provide algorithmic characterizations of the operators obtained through the abstract interpretation framework. Often these algorithms can be calculated by induction on types, but sometimes it requires trial-and-error. In any case, the AI-based definition provides the baseline against which to formally validate such characterizations.

Applying AGT to security typing. As mentioned above, applying AGT ensures by construction that the derived gradual language is type safe and satisfies the gradual guarantees. In prior work, we applied AGT to a pure language with security typing, and found the resulting language to satisfy noninterference [Garcia and Tanter 2015]. However, in this work, where the languages support mutable references, applying AGT to SSL_{Ref} yielded a gradual language that violates noninterference! By applying AGT, we surely obtained a gradual language that was type safe and satisfied the gradual guarantees, but unfortunately, the crucial semantic property of security types was broken. In brief, we had to apply two refinements. The first was proposed in the AGT methodology, though not needed in prior work. The second is novel, but conflicts with the dynamic gradual guarantee.

This section reports on these wrinkles and refinements so that future efforts to apply AGT to rich type disciplines can build on our experience. In particular:

- Sec. 6.1 sets up the basics to derive the static semantics of GSL_{Ref} with AGT, which was a successful endeavor. In the process, we identified one subtlety (about compositional lifting) that is worth highlighting.
- Sec. 6.2 explains the AGT approach to deriving the dynamic semantics of the gradual language. Here, we discover that evidence must use a more precise abstraction than the one used in the static semantics. While this possibility is briefly mentioned in [Garcia et al. 2016], it was not necessary in other applications of AGT.
Sec. 6.3 discusses a crucial point related to enforcing noninterference in the presence of references, and hence potential implicit flows. This observation led us to add an extra check to GSLRef’s dynamic semantics. The check ensures noninterference, but breaks the dynamic gradual guarantee.

6.1 Deriving the Statics
Following the AGT approach, we give meaning to gradual security labels directly in terms of the original static security labels. The driving intuition is that the unknown label ? represents any label whatsoever, while a gradual label ℓ represents a single static security label. We formalize this with a concretization function.

Definition 6.1 (Label Concretization). \( \gamma : \text{GLABEL} \rightarrow \mathcal{P}(\text{LABEL}) \)
\[
\begin{align*}
\gamma(\ell) &= \{ \ell \} \\
\gamma(?) &= \text{LABEL}
\end{align*}
\]

Concretization immediately induces the notion of precision, which orders the static information content of gradual labels from most to least:

Definition 6.2 (Label Precision). \( g_1 \subseteq g_2 \) if and only if \( \gamma(g_1) \subseteq \gamma(g_2) \).

In order to exploit AGT to gradualize SSLRef, we also require an abstraction function to precisely summarize a set of static labels as a single gradual label (round hats \( \widehat{\ } \) denote sets of \( x \)):

Definition 6.3 (Label Abstraction). \( \alpha : \mathcal{P}(\text{LABEL}) \rightarrow \text{GLABEL} \):
\[
\begin{align*}
\alpha(\{ \ell \}) &= \ell \\
\alpha(\emptyset) &= \text{undefined} \\
\alpha(? &= \text{otherwise}
\end{align*}
\]

The \( \gamma \) and \( \alpha \) functions are tightly connected by two properties that together form a Galois connection [Cousot and Cousot 1977].

Proposition 6.4 (\( \alpha \) is Sound and Optimal). If \( \widehat{\ell} \neq \emptyset \) then,
\[
(i) \quad \widehat{\ell} \subseteq \gamma(\alpha(\widehat{\ell})).
(ii) If \( \widehat{\ell} \subseteq \gamma(g) \) then \( \alpha(\widehat{\ell}) \subseteq g \).
\]

Soundness \( i \) means that \( \alpha \) always produces a gradual label whose concretization over-approximates the original set. Optimality \( ii \) means that \( \alpha \) always yields the best \( i.e. \) least) sound approximation that gradual labels can represent.

The meaning of gradual security types is derived from the meaning of gradual security labels. Therefore, we naturally define a Galois connection for gradual security types (see Appendix A.4.1).

Lifting predicates and functions. Following AGT, we exploit the Galois connections to lift all predicates and functions over labels and types from SSLRef to obtain the definition of their counterparts in GSLRef. In essence, each gradual entity (label, type) represents some set of static entities, so a consistent predicate holds among gradual entities so long as the underlying static predicate could plausibly hold. For instance, consistent ordering on gradual labels is defined as follows:

Definition 6.5 (Consistent label ordering). \( g_1 \prec g_2 \iff \ell_1 \leq \ell_2 \) for some \( (\ell_1, \ell_2) \in \gamma(g_1) \times \gamma(g_2) \).
Consistent ordering conservatively extends static label ordering because each static label, when treated as a gradual label, concretizes to a singleton set that contains only itself; conservative extension is central to the concept of graduality [Siek et al. 2015]. On the other hand, consistent ordering holds universally for the unknown label _, since it concretizes to all possible static labels.

Similarly, the join of two gradual labels is defined by lifting static label join:

**Definition 6.6 (Gradual label join).** \( g_1 \gtrdot g_2 = \alpha(\{ \ell_1 \gtrdot \ell_2 \mid (\ell_1, \ell_2) \in \gamma(g_1) \times \gamma(g_2) \}) \)

The gradual join of two gradual labels is the best abstraction of the set of all plausible static joins. For more insight, recall its equational characterization in Sec. 4: the unknown label disappears when joined with \( \top \), while it otherwise survives all joins. This is an emergent property of lifting: we did not anticipate it.

**Compositional vs. aggregate lifting.** One unanticipated subtlety observed in Sec. 4 involves the compound premises of the (Sapp) and (Sref) rules, such as \( \ell_c \gtrdot \ell \gtrdot \ell' \). One might be tempted to lift this premise compositionally as \( g_c \gtrdot g \gtrdot g' \). But Garcia et al. [2016] explicitly warn against blindly lifting static predicates compositionally: compositional lifting must be proven (for instance, they show that lifting their subtyping premises compositionally yields the same result as lifting them aggregately). Here it matters! Consider the definition induced by AGT:

**Definition 6.7 (Consistent bounding).**

\[ \neg \neg g_1 \gtrdot g_2 \gtrdot g_3 \iff \ell_1 \gtrdot \ell_2 \gtrdot \ell_3 \text{ for some } (\ell_1, \ell_2, \ell_3) \in \gamma(g_1) \times \gamma(g_2) \times \gamma(g_3) \]

This definition is _not_ equivalent to compositional lifting. For instance, the relation \( H \gtrdot ? \gtrdot L \) holds, but we know that no static label \( \ell \) satisfies \( H \gtrdot \ell \gtrdot L \) (because \( H \gtrdot \ell \) must be at least as high as \( H \)). In fact, precise lifting becomes critical when we reason about combining such lattice relations in the dynamic semantics. To the best of our knowledge, this is the first instance of aggregate lifting affecting the application of AGT.

### 6.2 Deriving the Dynamics

Garcia et al. [2016] derive the dynamic semantics of a gradual language by reduction of *gradual typing derivations* (augmented with evidence), thereby exploiting the correspondence between proof normalization and term reduction [Howard 1980]. This approach, which directly exploits the proof of syntactic type safety for the static language (SSL\(_{\text{Ref}} \) in our case), provides the direct runtime semantics of gradual programs, instead of the usual approach by translation to some internal cast calculus [Siek and Taha 2006].

Since writing down reduction rules over (two-dimensional) derivation trees is unwieldy, Garcia et al. [2016] use intrinsically-typed terms [Church 1940] as a convenient flat notation for derivation trees. Intrinsic terms are heavy notationally because they carry all type annotations, yielding to reduction rules that are hard to read. To alleviate this burden, we have chosen to present the dynamic semantics by reducing _evidence-augmented terms_, which are more lightweight notationally, and establish a more direct connection with the traditional translational approach. The counterpart of this choice is that we had to present a translation from source GSL\(_{\text{Ref}} \) terms to evidence-augmented GSL\(_{\text{Ref}} \) terms. Apart from this cosmetic difference, the central approach to reduction is the same: evidence is combined during reduction, producing either new evidence to support the plausibility of the contractum, or a runtime error if _no evidence remains_, thereby _refuting type safety._

---

To be honest, despite the warning of Garcia et al., we first overlooked the issue and applied compositional lifting, assuming it would hold. We then observed that the resulting design loses enough precision to miss some evident inconsistencies, with dramatic consequences for security.
In essence, GSL$^e_{Ref}$ terms are intrinsic terms from which computationally irrelevant static annotations have been erased. Proofs of theorems about GSL$^e_{Ref}$'s dynamic semantics need these annotations, so they use intrinsic terms. The companion technical report formalizes the relationship between intrinsic terms and evidence-augmented terms by giving a translation from intrinsic terms to evidence-augmented terms [Toro et al. 2018]. We show that, intrinsic terms can always be erased to GSL$^e_{Ref}$ terms, and that the process can be reversed for well-typed GSL$^e_{Ref}$ terms. Furthermore, related intrinsic and GSL$^e_{Ref}$ terms either reduce to related terms or yield errors. Therefore the theorems about intrinsic terms transfer to GSL$^e_{Ref}$ terms.

**Reduction and consistent deductions.** All instances of combining evidence in the reduction rules are dictated by SSL$^e_{Ref}$'s type safety proof. To illustrate this deep connection, we now analyze a case of the SSL$^e_{Ref}$ type safety proof and describe how to lift the argument to GSL$^e_{Ref}$. Consider the assignment case of SSL$^e_{Ref}$'s preservation proof, which in essence reduces a type derivation $\mathcal{D}$ to a new one and updates the program counter $\ell_c$ and store $\mu$.

\[
\begin{array}{c}
\mathcal{D} = \vdash \Sigma; \ell_c + \alpha_{\ell} : \mathcal{Ref}_\ell S \\
\quad \quad \quad \vdash \Sigma; \ell_c + v : S_2 \quad S_2 \triangleleft S \quad \ell_c \triangleright v \triangleleft \text{label}(S) \\
\quad \vdash \Sigma; \ell_c + \alpha_{\ell} = v : \text{Unit}_\perp
\end{array}
\]

The relevant reduction rule (Fig. 2) follows:

\[
\alpha_{\ell} = v \mid \mu \xrightarrow{\ell_c} \text{unit}_\perp \mid \mu[o \mapsto v \triangleright \ell_c \triangleright \ell].
\]

The fact that $\mathcal{D}$ reduces to $\vdash \Sigma; \ell_c + \text{unit}_\perp : \text{Unit}_\perp$ is immediate, but we must also prove that the stored value $v \triangleright \ell_c \triangleright \ell$ respects the store type, i.e. $S_2 \triangleright \ell_c \triangleright \ell \triangleleft S$. Since $\vdash \Sigma; \ell_c + v : S_2$ and $S_2 \triangleleft S$, it suffices to show that $\ell_c \triangleright v \triangleright \ell \triangleleft \text{label}(S)$. We do so as follows. Since $\triangleright$ is monotone with respect to $\triangleleft$ in both arguments, we can combine $\ell_c \triangleright v \triangleright \ell$ (assumed in the statement of preservation) and $\ell \triangleleft \ell$ (deduced by $\triangleleft$ reflexivity) to deduce $\ell_c \triangleright v \triangleleft \ell_c \triangleright \ell$. Finally, since $\triangleleft$ is transitive, we combine the above with the $\ell_c \triangleright v \triangleleft \text{label}(S)$ to deduce $\ell_c \triangleright v \triangleleft \text{label}(S)$. To recap, this "reduction" applies reasoning steps with a computational flavor: it composes $\triangleleft$ relations to deduce new ones, using both *join monotonicity* and *order transitivity*.

In the gradual setting, transitivity of ordering of gradual labels does not always hold: e.g. $H \triangleleft L$ and $H \triangleleft L$ but $H \not\triangleleft L$. As such, transitivity of consistent ordering is plausible but not definite, so we have to check. How? Here is the key intuition: recall that a consistent judgment like $H \triangleleft L$ means that $\ell_1 \triangleleft \ell_2$ holds for some pair of labels $(\ell_1, \ell_2)$ drawn from the concretizations $\gamma(H) = \{H\}$ and $\gamma(L) = \text{LABEL}$ respectively. We do not know which pair, so we must consider all plausible ones, i.e. $\{(H, H), (H, \top)\}$: the rest are surely wrong so we discard them. Similarly, the plausible pairs for $\ell \triangleleft \top$ are $\{\ell \triangleleft \top\}$. Now, given these two sets of plausible orderings, is transitivity plausible? Yes, because two plausible deductions arise: 1) $H \triangleleft H$ and $H \triangleleft \top$ implies $H \triangleleft \top$; and 2) $H \triangleleft \top$ and $\top \triangleleft \top$ implies $H \triangleleft \top$. When collected, the deduced pairings collapse to the singular expected result: $\{(H, \top)\}$. If we replay the same reasoning for $H \triangleright L$, however, we deduce $\emptyset$, which means that transitivity is not plausible: it has been refuted. An analogous process applies for join monotonicity, as well as transitivity of consistent subtyping, yielding sets of pairs of candidate subtypings.

In both of the above deductions, we reason imprecisely yet still deduce definite results: a single possibility in one, and none in the other. But in general, imprecision begets imprecision. The main source of complication is that static safety arguments deduce ordering relationships by interleaving transitivity and monotonicity arguments, so corresponding consistent deductions must mirror them. Furthermore, it would be especially burdensome to explicitly track sets of pairs of labels at runtime, let alone the sets of pairs of types that arise when reasoning about consistent
subtyping. This is where AGT suggests to use an abstraction of the possible static candidates, evidence. Evidence of a consistent judgment is a pair of abstractions of sets of static entities that justify a consistent judgment. Which abstraction to use turns out to be a crucial decision in order to preserve noninterference, as discussed next.

**Problems with evidence as gradual labels.** The “natural” abstraction of sets of labels are gradual labels, as used in the static semantics. In fact, Garcia et al. [2016] use the same abstraction to represent both runtime evidence and static gradual types; we initially followed suit. However, the first major subtlety we uncovered while deriving GSL Ref’s dynamic semantics is that using gradual labels (and consequently, gradual types) for evidence yields a design that achieves both type safety and the gradual criteria, but violates noninterference!

This problem manifested in two parts of the noninterference proof. First, the noninterference proof relies on the associativity of consistent transitivity. However, consistent transitivity of label ordering is not associative if gradual labels are used to represent evidence. Recall the program true : Bool ⊢ Bool : Bool, introduced in Sec. 4.2, which we expect to fail at runtime, and which ultimately involves combining three consistent label ordering judgments: \( e_1 \vdash ? \preceq H, e_2 \vdash H \preceq ?, \) and \( e_3 \vdash ? \preceq L. \) If we use a pair of gradual labels to represent evidence, eventually we have to calculate \( (e_1 \circ \preceq e_2) \circ \preceq e_3. \) But \( e_1 = (?, H), e_2 = (H, ?), \) and \( e_3 = (?, L), \) then \( e_1 \circ \preceq e_2 = (?, ?) \) and \( (?, ?) \circ \preceq e_3 = (?, L), \) so no runtime error is produced. Note that \( e_1 \circ \preceq (e_2 \circ \preceq e_3) \) fails as expected, because \( e_2 \circ \preceq e_3 \) is not defined, but this is not the composition order that arises at runtime.

Second, the proof of noninterference relies on the observational completeness of the consistent join operator:

**Lemma 6.8.** Suppose \( e_1 \vdash g_1 \rightsquigarrow \preceq g_1 \) and \( e_2 \vdash g_2 \rightsquigarrow \preceq g_2 \) such that \( e_1 \preceq \lor e_2 \vdash g_1 \lor g_2 \preceq \lor g_1 \lor g_2. \) Then \( (\neg \text{obsEv}_{\ell_1}^g(e_1) \lor \neg \text{obsEv}_{\ell_2}^g(e_2)) \iff \neg \text{obsEv}_{\ell_1}^g \lor \text{EV}_{\ell_2}^g(e_1) \lor e_2). \)

The analogous static lemma, i.e. \( (\neg \text{obsEv}_{\ell_1}^g(e_1) \lor \neg \text{obsEv}_{\ell_2}^g(e_2)) \iff \neg \text{obsEv}_{\ell_1}^g \lor \text{EV}_{\ell_2}^g(e_1) \lor e_2), \) holds trivially by the very definition of the join, but this property fails to hold in the presence of the unknown label. Suppose \( e_1 \vdash H \preceq ? \) and \( e_2 \vdash ? \preceq ?. \) If we use a pair of gradual labels to represent evidence, then \( e_1 \circ \preceq (H, ?), e_2 \circ \preceq (?, ?), \) and \( e_1 \lor e_2 \circ \preceq (?, ?) \) losing information about \( H. \) But \( \neg \text{obsEv}_{\ell_1}^g((H, ?)) \) and \( \text{obsEv}_{\ell_2}^g((?, ?)) \), therefore invalidating the lemma.

**Representing evidence as intervals.** These observations forced us to seek a more precise abstraction whose composition (through consistent transitivity) is associative and preserves the observational completeness of consistent join. Since it suffices to know whether the upper- and lower-bounds of the plausible static labels overlap to deduce the plausibility of consistent ordering, intervals seem to be a fitting abstraction. Indeed, this abstraction is sufficiently precise to guarantee the desired properties.

---

15 Note that associativity of cast composition is also critical for space-efficient semantics of gradual typing, e.g. Sick and Wadler [2010]. We conjecture that associativity may be a fundamentally desirable property, and intend to pursue this question.

16 One could design a gradual security language that uses label intervals instead of gradual labels right from the start, including in the static semantics. While this would unify the abstractions used in the statics and dynamics, it would yield a gradual type system that rejects more secure programs than GSL Ref does. For instance, the program (if false \( \vdash ? \) then \( 1 \vdash 2 \) else \( 2 \vdash 1 \)) \vdash L, is accepted and runs without errors in GSL Ref. But if we use intervals in the static semantics, then the security level of the conditional expression which boils down to the join between \( ?, H \) and \( L \), would be \([L, H]\), therefore the program would be rejected statically. Applying a \( ? \) ascription to \( 1 \vdash 2 \) would fix this program.
Definition 6.9 (Interval Concretization). \( \gamma_i : \text{INTERVAL} \to \mathcal{P}(\text{LABEL}) \), where
\[
\text{INTERVAL} = \{ (\ell_1, \ell_2) \in \text{LABEL}^2 \mid \ell_1 \preceq \ell_2 \}
\]
\[
\gamma_i((\ell_1, \ell_2)) = \{ \ell \mid \ell \in \text{LABEL}, \ell_1 \leq \ell \leq \ell_2 \}.
\]

Definition 6.10 (Interval Abstraction). \( \alpha_i : \mathcal{P}(\text{LABEL}) \to \text{INTERVAL} \)
\[
\alpha_i(\emptyset) \text{ is undefined} \quad \alpha_i(\{ T_i \}) = [\wedge T_i, \vee T_i] \text{ otherwise}
\]

With evidence based on intervals, \( (\epsilon_1 \circ^\prec \epsilon_2) \circ^\prec \epsilon_3 \) and \( \epsilon_1 \circ^\prec (\epsilon_2 \circ^\prec \epsilon_3) \) are equivalent. Back to the example, now \( \epsilon_1 = \langle [\bot, H], [H, H] \rangle \), \( \epsilon_2 = \langle [H, H], [H, T] \rangle \) and \( \epsilon_3 = \langle [\bot, L], [L, L] \rangle \), then \( \epsilon_1 \circ^\prec \epsilon_2 = \langle [\bot, H], [H, T] \rangle \). Because \( \langle [\bot, H], [H, T] \rangle \circ^\prec \epsilon_3 \) is undefined, a runtime error is raised, avoiding the breach of noninterference. Also, the observational-monotonicity of the join is preserved. Now \( \epsilon_1' = \langle [H, H], [H, T] \rangle \) and \( \epsilon_2' = \langle [\bot, T], [\bot, T] \rangle \), then \( \epsilon_1' \triangleright \epsilon_2' = \langle [H, T], [H, T] \rangle \) and now \( \neg \text{obsEv}_i(\langle [H, T], [H, T] \rangle) \) as expected.

Lifting consistent lattice relations. We now explain how the definitions of consistent transitivity and join monotonicity are semantically justified. As discussed in Sec. 6.1, premises such as \( \ell_c \triangleright \ell \leq \ell_c' \) must be lifted as aggregates. In fact, such a judgment is likely the consequence of similar deductions from earlier reduction steps. For instance \( \ell \) must be some lattice expression \( F(\overline{T_i}) \) comprising joins (and meets) of source program labels \( T_i \). Therefore, to mirror static type safety reasoning steps at runtime, and catch inconsistencies if they arise, we must generalize each ordering premise in a derivation and consider it as some lattice relation \( F_1(\overline{T_i}) \preceq F_2(\overline{T_j}) \). The notion of evidence must consequently account for the plausibility of consistent lattice relations:
\[
\langle t_1, t_2 \rangle \vdash F_1(\overline{g_i}) \preceq F_2(\overline{g_j})
\]

The definitions of consistent join monotonicity and consistent transitivity then follow directly from AGT by consistent lifting.

Definition 6.11 (Consistent transitivity for label ordering).
\[
\circ^\prec : \text{INTERVAL}^2 \times \text{INTERVAL}^2 \to \text{INTERVAL}^2
\]
\[
\langle t_1, t_{21} \rangle \circ^\prec \langle t_{22}, t_3 \rangle = \alpha_i^2(\{ (\ell_1, \ell_2) \in \gamma_i^2(\langle t_1, t_2 \rangle) \mid \exists \ell \in \gamma_i(t_{21}) \cap \gamma_i(t_{22}), \ell_1 \leq \ell \land \ell \leq \ell_3 \})
\]

Consistent transitivity produces evidence for all plausible instances of consistent ordering that can be deduced using transitivity from the plausible instances of ordering represented by the two inputs. By design, \( \alpha_i^2(\emptyset) \) is undefined, so consistent transitivity is also undefined if no plausible pairings remain to support a deduction.

Definition 6.12 (Consistent join monotonicity). \( \triangleright \) : \text{INTERVAL}^2 \times \text{INTERVAL}^2 \to \text{INTERVAL}^2
\[
\epsilon_1 \triangleright \epsilon_2 = \alpha_i^2(\{ (\ell_1, \ell_2) \mid \exists (\ell_{11}, \ell_{12}) \in \gamma_i^2(\langle \epsilon_1 \rangle), (\ell_{21}, \ell_{22}) \in \gamma_i^2(\langle \epsilon_2 \rangle), \ell_1 = \ell_{11} \triangleright \ell_{21}, \ell_2 = \ell_{12} \triangleright \ell_{22}, \ell_1 \leq \ell_2 \})
\]

Consistent join monotonicity is analogous, but note that due to lattice and interval properties, consistent join monotonicity is really a total function. Also, the \( \ell_1 \leq \ell_2 \) condition is superfluous; we present the definition in this form to preserve the general structure of consistent deduction definitions.

The algorithmic characterizations from Sec. 4.2 are equivalent to the above definitions. More importantly, we can prove that these operators indeed yield valid evidence for the combined consistent judgments.

Proposition 6.13. Suppose \( \epsilon_1 \vdash F_{11}(\overline{g_i}) \preceq F_{12}(\overline{g_j}) \) and \( \epsilon_2 \vdash F_{21}(\overline{g_i}) \preceq F_{22}(\overline{g_j}) \)
Then \( \epsilon_1 \triangleright \epsilon_2 \vdash F_{11}(\overline{g_i}) \triangleright F_{21}(\overline{g_i}) \preceq F_{12}(\overline{g_j}) \triangleright F_{22}(\overline{g_j}) \)
Proposition 6.14. Suppose $\varepsilon_1 \vdash F_1(\overline{g_1}) \lessgtr F_2(\overline{g_1})$ and $\varepsilon_2 \vdash F_2(\overline{g_1}) \lessgtr F_3(\overline{g_1})$.
If $\varepsilon_1 \circ \leq \varepsilon_2$ is defined, then $\varepsilon_1 \circ \leq \varepsilon_2 \vdash F_1(\overline{g_1}) \lessgtr F_3(\overline{g_1})$.

From labels to types. Finally, in addition to reasoning about consistent label ordering, the dynamic semantics must track and check the plausibility of consistent subtyping. Since (consistent) subtyping is induced by (consistent) ordering, the reasoning in question arises by lifting the same constructions to gradual security types, consistent subtyping, and consistent subtyping join and meet.

Just as we extend gradual labels $g$ to gradual security types $U$ (e.g. $\text{Int}_g$) in the source language, so do we extend label intervals $\overline{t}$ point-wise to type intervals $E$ (e.g. $\langle \text{Int}_h, \text{Int}_l \rangle$), which represent sets of pairs of candidates for plausible subtyping. We introduce evidence judgments $\varepsilon \vdash U_1 \lessgtr U_2$ to associate runtime evidence with particular consistent subtyping judgments. The entire development mirrors the one for labels, and does not convey any new insights (see Appendix D.1).

6.3 Policing Dynamic Heap Updates

Although adopting label intervals for evidence of consistent label judgments addressed some aspects of the noninterference proof, this refinement alone is not sufficient.

To illustrate the remaining problem, recall the example of implicit flows from Sec. 2, in particular the second version of the example, which has some missing static annotations.

```
fun x : BoolH =>
let y : Ref Bool = ref true
let z : Ref BoolL = ref trueL
if x then y := falseL else unit
if !y then z := falseL else unit
!z
```

This program is accepted statically and also runs without errors: if $x$ is true$_H$ then the program reduces to true$_L$, and if $x$ is false$_H$ it reduces to false$_L$: a clear breach of noninterference!

To understand the problem, consider what happens for the different values of $x$. When $x$ is true$_H$ the assignment in line 4 under security effect $H$ is valid, because $H \lessgtr ?$. In that moment we know that the security level of the content of $y$, must be higher than $H$. But when $x$ is false$_H$, in line 5 we assume that the security level of the content of $y$ is lower than $L$. In other words, under supposedly-related executions we get contradictory evidence for $y$. Notice that in the assignment at line 4, the judgment $H \lessgtr ?$ holds, but so does its negation $H \lessgtr \overline{?}$. To preserve noninterference, we must ensure that its negation never holds.

To recover noninterference, we add an extra check to the assignment reduction rule ($r7$) from Fig. 6:

\[
\varepsilon_1 \circ g : \vdash \varepsilon_2 u | \mu \xrightarrow{E_{\leq}} \begin{cases}
\text{unit} \perp & \mu[o \mapsto \varepsilon'(u \overline{\overline{\overline{\overline{\overline{g}}}}})]
\text{error} & \text{if } \varepsilon' \text{ is not defined, or } \varepsilon \lessgtr \overline{ilbl} \varepsilon'' \text{ does not hold}
\end{cases}
\]

where $\mu(o) = \varepsilon''u'$. The highlighted check ensures that if the security effect is not observable, then the content of the heap to be replaced must also be not observable.\(^{17}\) This concept is formalized in the following lemma, which is used in the noninterference proof:

\(^{17}\) This check is analogous to the no-sensitive-upgrade check introduced by Austin and Flanagan [2009], taken to the gradual context, and hence involving unknown labels, evidences and consistent judgments.
Lemma 6.15. Consider \( \varepsilon_1 \vdash g'_1 \sim g_1 \) and \( \varepsilon_2 \vdash g'_2 \sim g_2 \). Then \((\neg \text{obsEv}^0_{\varepsilon_1}(\varepsilon_1) \land \varepsilon_1 [\leq] \varepsilon_2) \Rightarrow \neg \text{obsEv}^0_{\varepsilon_2}(\varepsilon_2)\).

With the additional check, if \( x \) is true\(_H\), the program fails at runtime, preserving noninterference.

The necessity of the check shows up in the noninterference proof for the if case. When two computations have related non-observable conditionals, the booleans can be different. This may lead to two related computations that reduce different branches under a high-security context. At that point, we must enforce that those different executions only write high-security values to the heap. In other words, as long as both executions reduce under high-security contexts, their executions can desynchronize only on private information. Formally, the following lemma should hold:

Lemma 6.16. Consider \( \varepsilon; \Sigma; g_c \vdash t : U \), \( g'_c \) and \( \mu \) such that, \( \varepsilon \vdash g_c \sim g'_c \), \( \neg \text{obsEv}^0_{\varepsilon_2}(\varepsilon) \) and \( \Sigma \vdash \mu \), and \( \forall k > 0, \text{such that } t \mid \mu \xrightarrow{sgc} k t' \mid \mu' \).

1. \( \forall o \in \text{dom}(\mu') \setminus \text{dom}(\mu), \neg \text{obsVal}^U_{\varepsilon_2}(\mu'(o)) \).
2. \( \forall o \in \text{dom}(\mu') \cap \text{dom}(\mu) \) where \( \mu'(o) \neq \mu(o) \),
   a) \( \neg \text{obsVal}^U_{\varepsilon_2}(\mu(o)) \), and
   b) \( \neg \text{obsVal}^U_{\varepsilon_2}(\mu'(o)) \).

Without the additional check in rule (r7), we cannot prove (2.a): before updating a reference, the current content should be non observable. And as we can see in the example above, without the check, the reference before the assignment would be observable, hence breaking the Lemma.

In its current formulation [Garcia et al. 2016], AGT derives the dynamic semantics of the gradual language from the type safety argument of the static language. Here, we are facing a typing discipline in which type safety does not imply type soundness (i.e. noninterference), and hence, the methodology falls short of naturally preserving that property. This suggests that extending AGT to ensure type soundness of the derived gradual language might require adapting the conceptual framework to take the purely static type soundness proof as a source of design insight.

Noninterference vs. Dynamic gradual guarantee. Although the extra check above allows GSL\(_{\text{Ref}}\) to ensure noninterference, it sacrifices the dynamic gradual guarantee. Recall that this guarantee says that removing a static security annotation cannot introduce new runtime errors.

Consider the following example:

```
1 fun x: Bool\(_H\) =>
2  let y: Ref Bool\(_H\) = ref true\(_H\)
3  if x then y := false\(_H\) else unit
```

The program is accepted statically and runs without error as it does not break noninterference. If we remove the type annotations on line 2:

```
1 fun x: Bool\(_H\) =>
2  let y: Ref Bool\(_H\) = ref true\(_H\)
3  if x then y := false\(_H\) else unit
```

then the program is conservatively rejected at runtime, because of the additional check for assignments. This behavior violates the dynamic gradual guarantee.\(^{18}\)

To sum up, if decreasing the precision of a type annotation results in performing an assignment to a reference whose content now has an unknown security label, and that assignment occurs under a non-public security effect, a runtime error can be raised, whereas the more precise program did

\(^{18}\)Removing the additional check on assignments recovers the dynamic gradual guarantee, but it breaks noninterference: there is no free lunch in presence of mutable references.
not fail. More precisely, even in such situations, a runtime error will only be raised if the dynamic security information about the stored value up to the point of the actual assignment is lower than the current security effect. For instance, in our example above, if we modify the security level of the boolean in line 2 to $H$ (leaving the type of $y$ as it is), then the program performs a valid assignment on a reference whose content has a statically-unknown security level, but dynamically $H$; therefore no runtime error is raised. Unfortunately, beyond pure and read-only programs, it seems impossible to provide any useful syntactic characterization of the programs for which the dynamic gradual guarantee holds, because both the current security effect and the accumulated evidence about a given value are essentially dynamic information.

7 RELATED WORK

Static and dynamic information-flow control techniques have been extensively studied in the literature. The area is too vast to exhaustively review here: we refer to [Hedin and Sabelfeld 2012b; Russo and Sabelfeld 2010; Sabelfeld and Myers 2003] for broad overviews of the area. This section first focuses on security type systems, as well as some specific approaches to dynamic information flow control, given the static-to-dynamic spectrum that gradual security typing covers. We also discuss existing proposals that combine static and dynamic checking. Finally we relate our work to other efforts to gradualize advanced type disciplines.

Static information flow control. Volpano et al. [1996] present one of the first type systems for information flow analysis, developed for a first-order imperative language with conditionals and loops. They present and formalize the first soundness result for a security-typed language, namely that altering the initial values of locations cannot affect resulting values of locations with a lesser security level.

Subsequently, Heintze and Riecke [1998] present a security-typed higher-order language called the Secure Lambda Calculus (SLam). SLam is a functional language extended with sums, products, and recursion, that supports both confidentiality and its dual notion, integrity [Biba 1977]. They introduce the prot expression, which we also use, to increase the ambient security level for the dynamic extent of evaluating a term. The noninterference proof for SLam is also based on logical relations. The authors extend SLam with concurrency and references. They prove that the resulting language is type safe, but they do not prove noninterference, deemed too problematic in a concurrent setting. SSL$_{Ref}$ is also a higher-order language with references, but it does not support sums, products, recursion and concurrency. We prove noninterference for both GSL$_{Ref}$ and SSL$_{Ref}$. Extending GSL$_{Ref}$ to richer types and concurrency is a challenge worth addressing in future work.

To consolidate different related efforts, Abadi et al. [1999] develop the Dependency Core Calculus (DCC), an extension of the lambda calculus that tracks dependencies such as security, partial evaluation, program slicing and call-tracking. In particular, they show that different languages such as SLam can be translated to DCC. They present a semantic model of DCC that helps to provide a simple proof of noninterference. It would be interesting to study the application of AGT to DCC, to provide a general account of gradual dependency tracking.

JFlow [Myers 1999; Myers and Liskov 1997], which later evolved into Jif [Myers and Liskov 2000], is a practical extension of the Java language that protects both confidentiality and integrity of sensitive data. Jif supports statically-checked information flow annotations, a decentralized label model with principals, automatic label inference, and security label polymorphism, all integrated with object-oriented features like class inheritance, as well as exceptions, among other features. Jif supports runtime label tests that can be used to encode explicit security casts, although such casts break type-based reasoning about noninterference. Scaling up GSL$_{Ref}$ to cover the feature set of Jif would open the door to a practical implementation of gradual security typing.
Zdancewic [2002] proposes $\lambda^{SEC}$, a simple security language similar to SLam, and proves noninterference using logical relations. He then extends the language with references, yielding $\lambda^{SEC}_{REF}$, which was the starting point for our design of SSL\textsubscript{Ref}. Unlike SSL\textsubscript{Ref}, the operational semantics of $\lambda^{SEC}_{REF}$ includes additional checks to control whether it is safe to assign to references; the type system then makes these checks redundant. In SSL\textsubscript{Ref}, we omit these checks, and the runtime only tracks security levels. The runtime checks needed in the gradual setting arise as evidence combination. Also, Zdancewic does not prove noninterference for $\lambda^{SEC}_{REF}$ directly, but instead by a CPS translation to a lower-level imperative language with explicit continuations, for which noninterference is established [Zdancewic and Myers 2001]. This setting permits studying information flow with concurrency and as such could be a judicious starting point to study the interaction of gradual security typing and concurrency.

Much work on static information flow analysis focuses on declassification, which is the limited, intentional, and controlled release of confidential information. Declassification is outside the scope of this work, though a very interesting perspective for future work; we refer to [Sabelfeld and Sands 2009] for an introductory survey.

An important distinction in information flow analysis is whether an analysis is flow-sensitive, i.e. whether memory cells are allowed to store values of different security levels at different times. Hunt and Sands [2006] explore families of sound flow-sensitive type systems, indexed by the choice of the security lattice. In particular, they show that every program typeable in a flow-sensitive static type system can be translated to an equivalent program typeable in a flow-insensitive type system. SSL\textsubscript{Ref} is a flow-insensitive purely static analysis; GSL\textsubscript{Ref} inherits flow-insensitivity for its static semantics. However, at runtime the security level of references is allowed to vary (through evidence composition) within the bounds imposed by the static type of the reference. This means that a reference that is created with an unknown security label can store values of any security level at different times. This leads us to sharing challenges faced by dynamic information-flow control techniques, discussed hereafter.

**Dynamic information flow control.** Russo and Sabelfeld [2010] show that static mechanisms can be more precise than dynamic ones about certain kinds of information flows. Indeed, noninterference can be characterized as a 2-safety property, meaning that it can only be refuted by observing two different executions of the same program with different inputs. This makes it particularly challenging for dynamic information flow control, which traditionally makes decisions based on a single execution. Most work on dynamic information flow analysis therefore monitors a 1-safety property that conservatively approximates noninterference, but has the advantage of being observable in a single execution. Such approximations necessarily introduce false alarms, especially when mutable references are involved.

To avoid implicit leaks through the heap in a purely dynamic information-flow analysis, Austin and Flanagan [2009] introduce a no-sensitive-upgrade check to prevent implicit security leaks through partially-leaked data, i.e. data produced from updates to public heap data that depend on private information. We adapt this approach to GSL\textsubscript{Ref}, imposing an extra check when assigning to references. Subsequently, Austin and Flanagan [2010] propose a more permissive analysis, where partially-leaked data is allowed, but carefully tracked to ensure that it is upgraded before being used in conditional tests. This allows programmers to iteratively add security upgrades to partially-leak data only when needed, through multiple executions of a program.

Later, Austin and Flanagan [2012] introduce a completely different approach: faceted execution, which simulates multiple executions of a program for different security levels in a single run. A faceted execution yields a faceted value, which in a traditional two-point lattice is a pair of a public
and a private value. This novel approach enables a characterization of noninterference as a 1-safety property, without introducing false alarms. It does however raise questions regarding how to efficiently implement such faceted executions, especially in the presence of complex security lattices. Faceted execution was recently extended to support dynamic information flow with exceptions, declassification and clearance [Austin et al. 2017]. It would be interesting to explore whether basing GSLRef on faceted execution might yield a gradual security language that fully respects the dynamic gradual guarantee, by avoiding the extra runtime check in assignments.

Stefan et al. [2017] present a dynamic information-flow control system called LIO. Contrary to most approaches to dynamic information flow, LIO does not modify the underlying language runtime semantics, being implemented as a Haskell library. LIO supports both mutable references and exceptions. Exceptions are used to recover from security monitor failures, preserving both confidentiality and integrity. The possibility of securely recovering from runtime security exceptions is an interesting perspective to study in the context of gradual security typing. More generally, recovering from runtime type errors raises a number of questions about the metatheory of gradual typing, because doing so can directly affect the dynamic gradual guarantee as well as type-based reasoning (e.g. it becomes possible to encode explicit type tests).

**Hybrid information flow control.** To resolve the tension between flexibility and soundness of flow-sensitive analyses, Russo and Sabelfeld [2010] propose a general hybrid approach, in which a static effect analysis is used to dynamically upgrade the security level of variables of untaken branches of conditionals, thereby preventing implicit leaks through the heap. This hybrid approach is developed on top of a (first-order) imperative language. Moore and Chong [2011] later show how to implement this hybrid approach more efficiently using additional static analyses.

A variety of hybrid information-flow control systems have been investigated, whose designs combine static and dynamic techniques that buttress one another to balance permissiveness and efficiency. Note that although gradual typing also combines static and dynamic techniques, hybrid approaches differ essentially from gradual ones. The key specificity of gradual typing is to smoothly support the continuum between static and dynamic checking based on the (programmer-controlled) precision of type annotations [Siek and Taha 2006; Siek et al. 2015]. This central notion of type precision is absent from hybrid approaches, in which the balance between static and dynamic checking is often driven by other concerns—such as the (un)decidability of a static predicate [Knowles and Flanagan 2010], or the need to pre-compute information for enhancing runtime checking.

Chandra and Franz [2007] implement hybrid security information flow control for the Java Virtual Machine. The operational semantics permits policies to change during execution. To prevent invalid implicit flows through the heap, they perform a static analysis of effects similar to Russo and Sabelfeld [2010]. Information about conditionals is gathered ahead of execution, then used to update labels at runtime, as if all branching alternatives had been taken. They also statically determine when the current security effect can be lowered again after a conditional. Performing an effect analysis statically to drive runtime monitoring is appealing as it could obviate the extra assignment check in GSLRef that compromised the dynamic gradual guarantee. However, in the setting of a higher-order imperative language, the effect analysis could easily become too conservative or too demanding for programmers. Combining gradual security and gradual effects [Bañados Schwerter et al. 2016] may temper this issue, but represents a considerable challenge in itself.

Shroff et al. [2007] present a dynamic information flow system based on runtime tracking of indirect dependencies between program points, allowing a lazier, hence more flexible, detection of implicit flows. In particular, they track indirect dependency between dereference points and branching points. They present two languages, one that captures dependencies statically, and one that uses multiple executions of a program to record dependencies. This is yet another approach
to runtime tracking that is worth considering in order to achieve a more flexible gradual security language that fully respects the dynamic gradual guarantee.

Hybrid approaches can also support programmer-controlled flexibility. Buiras et al. [2015] propose Hybrid LIO (HLIO), a flexible monadic information-flow control library for Haskell. HLIO is not gradual in the sense that it does not include an unknown security label; instead, HLIO provides a primitive to explicitly and selectively defer label-ordering checks to runtime. Their approach to defer static typing constraints to runtime can even be exploited to postpone type checks beyond security label constraints, opening the door to hybrid type checking in Haskell. In contrast, as a gradual security language, GSLRef supports a notion of unknown security information and implicitly mediates the interactions between static and dynamic security checking.

**Gradual security typing.** Most directly related to our proposal is prior work on gradual security typing, which combines static and dynamic checking with the express intent of supporting a smooth migration between both checking disciplines by introducing a dynamic (i.e. statically unknown) security label. Disney and Flanagan [2011] and Fennell and Thiemann [2013] pioneered what we describe in Sec. 1 as a check-driven approach to gradual security typing, starting from dynamic checking. Both develop notions of blame tracking and prove blame theorems for their semantics. It is important to recall that these approaches, while dubbed “gradual”, are based on explicit security casts, and are therefore more akin to cast calculi than to gradual languages. In particular, this means that these languages do not respect the gradual guarantees by design, including the static one, because changing the precision of type annotations requires adding/removing explicit casts. Additionally, as discussed in the introduction, both proposals break type-based reasoning about noninterference.

Recently, Fennell and Thiemann [2016] extend their prior work on gradual security typing with references to the object-oriented setting, in a language called LJGS. Like Jif, LJGS performs local inference of security labels, and supports polymorphic security signatures. Local variables in LJGS are typed in a flow-sensitive manner, whereas both SSLRef and GSLRef are flow insensitive regarding security levels. Although LJGS is based on explicit casts like prior work, its semantics differ in important ways. For instance, recall the example given in Sec. 1:

```plaintext
let mix : IntL →L IntH →L IntL =
  fun pub priv => if pub < (IntL \rightleftharpoons IntH) priv then 1L else 2L
  mix 1L 5L
```

This example does not type check in LJGS because the target type of a security cast cannot be less secure than the source type. The only way to write this example is to go through the dynamic security level explicitly:

```plaintext
let mix : IntL →L IntH →L IntL =
  fun pub priv => if pub < (IntL \rightleftharpoons IntH) (IntL \rightleftharpoons IntH) priv then 1L else 2L
  mix 1L 5L
```

This well-typed program fails at runtime because (IntL \rightleftharpoons IntH) upgrades 5L to 5H, but (IntL \rightleftharpoons IntH)5H is not defined. This approach to upgrade the security level of values that are cast to the dynamic label using the statically-determined source label seems to restore type-based reasoning about noninterference in LJGS. Interestingly, the change in semantics in LJGS is solely motivated by the design goal to avoid having to dynamically track security labels of statically-typed program fragments, so the relation with type-based reasoning appears to be accidental.

Similar to the approach of Russo and Sabelfeld [2010] and Shroff et al. [2007] discussed above, LJGS relies on a side-effect analysis to tracks the updated variables in method bodies. More precisely, when typing a method, LJGS generates a set of constraints that represent the information flow
dependencies between parameters and return values, as well as two sets of effects: a local effect that
lists the variables modified in branches of a conditional, used to update local variables of untaken
branches; and a global effect that records the security types whose fields may be updated with
sensitive information. This type analysis and constraint/effect inference is facilitated by the fact
that classes in LJGS are not first-class entities, i.e. all class definitions are top-level and known
ahead-of-time. This means in particular that at every call site, one statically knows the precise
inferred constraints and effects of methods (modulo a standard subsumption criteria to account
for subtyping). In a setting with higher-order types, this information would be more complex to
track. Additionally, the inferred global effect of a method is insufficient information per se for the
dynamic information flow control part of LJGS. Therefore, LJGS also appeals to an external effect
analysis (left opaque) to obtain precise information about heap write effects.

**Gradualizing expressive typing disciplines.** Since the initial formulation of gradual typ-
ing [Siek and Taha 2006], there has been many efforts to gradualize advanced typing disciplines,
like typestates [Garcia et al. 2014; Wolff et al. 2011], ownership types [Sergey and Clarke 2012],
annotated type systems [Thiemann and Fennell 2014], effects [Bañados Schweter et al. 2014, 2016;
Toro and Tanter 2015], refinement types [Jafery and Dunfield 2017; Lehmann and Tanter 2017],
parametric polymorphism [Ahmed et al. 2017; Igarashi et al. 2017], and the security type systems
discussed above, among others.

Since the formulation of the refined criteria for gradually-typed languages [Siek et al. 2015],
however, only refinement types [Jafery and Dunfield 2017; Lehmann and Tanter 2017] have been
shown to fully respect such guarantees. This work contributes to the general research agenda of
gradual typing disciplines by explicitly attempting to achieve both the gradual guarantees and a
rich semantic property, like noninterference. Indeed, noninterference is not implied by type safety;
in contrast, soundness of refinement types directly follows from type safety. We have shown that
GSL$_{Ref}$ does respect the static gradual guarantee (as opposed to other gradual security type systems);
but GSL$_{Ref}$ must sacrifice the dynamic gradual guarantee due to a modification of the runtime
semantics that is necessary to enforce noninterference in the presence of mutable references.

Initial work on gradual parametricity [Igarashi et al. 2017] also suggests that parametricity
may be incompatible with the dynamic gradual guarantee, unless one is willing to tweak the type
precision relation; even then, the dynamic gradual guarantee is left as a conjecture. Ahmed et al.
[2017] prove parametricity for a polymorphic cast calculus—not a source language—and also leave
the gradual guarantees as an open question. Therefore, further work is needed to fully understand
if and how the gradual guarantees can be reconciled with rich semantic typing disciplines, and if
additional design criteria for such gradual languages should be devised.

8 CONCLUSION

We develop a novel, type-driven approach to gradual security typing, in which gradual security
types provide strong security invariants, while admitting flexible programming idioms. This is the
first work to address the gradualization of a rich typing discipline in which type safety does not
imply type soundness, while pursuing the most elaborate formulation of criteria for gradually-typed
languages [Siek et al. 2015], and preserving type-based reasoning principles. This means that the
amount of static checking is entirely driven by the precision of static security annotations, and that
programmers can reason modularly about the noninterference guarantees of program fragments
by just looking at types.

Using the AGT methodology [Garcia et al. 2016] to derive the gradual security language GSL$_{Ref}$,
this work sheds light on key semantic issues in the design of gradual languages. AGT was central
in our endeavor to separate the elements of the design that follow by systematically following the
methodology from those that require careful consideration. In particular, we identify a tension between the smooth continuum on the static-to-dynamic spectrum that the gradual guarantees mandate, and the semantic property of noninterference, which manifests in GSL_{Ref} because of mutable references. This tension also raises interesting questions for the principled design of gradually-typed languages, whenever the semantics of types has a relational flavor. In particular, while we have addressed noninterference, relational parametricity remains to be addressed. Overall, this work suggests that it might be necessary to extend AGT to integrate the purely static type soundness proof—as opposed to only the type safety proof—as a source for the design of the dynamic semantics of a gradual language.

Within the context of gradual security typing, our work leaves open the question of whether it is possible to reconcile both noninterference and the dynamic gradual guarantee. Specifically, it would be informative to study whether other approaches to sound dynamic information flow control could help us recover the dynamic gradual guarantee. We believe that there might be an inherent incompatibility between the strictness required to enforce a hyper-property like noninterference, and the optimistic flexibility dictated by the dynamic gradual guarantee.

Another interesting track for future work is to explore a “pay-as-you-go” [Siek and Taha 2006] semantics, which only introduces runtime checks for imprecisely-typed expressions, as well as scaling the security discipline to other language-based security features such as integrity, flow sensitivity and declassification. Additionally, we want to explore the applicability of Garcia and Cimini [2015]’s approach to type inference in gradual languages to address security label inference [Pottier and Simonet 2003] in GSL_{Ref}.

Acknowledgments. We thank the anonymous reviewers of this paper and previous submissions for their helpful comments, questions, and detailed readings. We also thank Alison M. Clark, Joshua Dunfield, Chris Martens, and Jeremy Siek.

REFERENCES


Alonzo Church. 1940. A Formulation of the Simple Theory of Types. J. Symbolic Logic 5, 2 (06 1940), 56–68.


\[
S := \text{Bool}_\ell \mid S \xrightarrow{\ell} S \mid \text{Ref}_\ell S \mid \text{Unit}_\ell \quad \text{(types)} \\
b := \text{true} \mid \text{false} \quad \text{(Booleans)} \\
r := b \mid \lambda^\ell x : S.t \mid \text{unit} \mid o \quad \text{(raw values)} \\
v := r_\ell \\
t := v \mid t \mid t \oplus t \mid \text{if } t \text{ then } t \text{ else } t \quad \text{(terms)} \\
\oplus := \land \mid \lor \\
\]

Fig. 11. SSLRef: Syntax

\[
\begin{array}{ll}
(Sx) & x : S \in \Gamma \\
& \Gamma; \Sigma; \ell_c; \ell \vdash x : S \\
(Sb) & o : S \in \Sigma \\
& \Gamma; \Sigma; \ell_c; \ell \vdash o_\ell : \text{Ref}_\ell S \\
(S\lambda) & \Gamma; x : S_1; \Sigma; \ell' \vdash t : S_2 \\
& \Gamma; \Sigma; \ell_c; \ell \vdash (\lambda^\ell x : S_1.t_\ell : S_1 \xrightarrow{\ell} S_2) \\
(Sprot) & \Gamma; \Sigma; \ell_c \lor \ell \vdash t : S \\
& \Gamma; \Sigma; \ell_c; \ell \vdash \text{prot}_\ell(t) : S \lor \ell \\
(Sapp) & \Gamma; \Sigma; \ell_c; \ell \vdash t_1 : S_1 \xrightarrow{\ell} S_2 \\
& \Gamma; \Sigma; \ell_c; \ell \vdash t_2 : S_2 \\
& \Gamma; \Sigma; \ell_c; \ell \vdash S_2 \ll S_1 \\
& \Gamma; \Sigma; \ell_c; \ell \vdash c : S_1 \lor \ell \ll \ell' \\
(Sif) & \Gamma; \Sigma; \ell_c; \ell \vdash t : \text{Bool}_\ell \\
& \Gamma; \Sigma; \ell_c; \ell \vdash \text{if } t \text{ then } t_1 \text{ else } t_2 : (S_1 \lor S_2) \lor \ell \\
(Sderef) & \Gamma; \Sigma; \ell_c; \ell \vdash t : \text{Ref}_\ell S \\
& \Gamma; \Sigma; \ell_c; \ell \vdash \text{!}t : S \lor \ell \\
(Sasgn) & \Gamma; \Sigma; \ell_c; \ell \vdash t : \text{Ref}_\ell S_1 \\
& \Gamma; \Sigma; \ell_c; \ell \vdash t_2 : S_2 \\
& S_2 \ll S_1 \\
& \Gamma; \Sigma; \ell_c; \ell \vdash \text{!}t : \text{Unit}_\ell \\
& \Gamma; \Sigma; \ell_c; \ell \vdash t : S_2 \\
(S:) & \Gamma; \Sigma; \ell_c; \ell \vdash t : S_1 \\
& \Gamma; \Sigma; \ell_c; \ell \vdash t : S_2 \\
& S_1 \ll S_2 \\
& \ell \ll \ell' \\
& \text{Bool}_\ell \ll \text{Bool}_{\ell'} \\
& \text{Unit}_\ell \ll \text{Unit}_{\ell'} \\
& S_1 \ll S_2 \\
& \ell \ll \ell' \\
& \ell' \ll \ell' \\
& S_1 \ll S_2 \\
& \text{Ref}_\ell S \ll \text{Ref}_{\ell'} S \\
\end{array}
\]

Fig. 12. SSLRef: Static Semantics

A  FULL DEFINITIONS FOR THE STATIC AND GRADUAL LANGUAGE

In this section we present the full definition of SSLRef (sections A.1 and A.2) and the full definition of GSLRef (sections A.4 and A.6). Section A.8 presents the full definitions of noninterference presented in the paper.
A.1 SSLRef: Static semantics

In this section we present the full definition of the static semantics of SSLRef. Figure 11 presents the syntax of SSL-Ref. Figure 12 presents the complete static semantics of SSLRef, where the join between types and labels is defined as follows

\[
\begin{align*}
\text{Bool}_\ell \triangleleft \ell' &= \text{Bool}_{(\ell \lor \ell')} \\
(S_1 \xrightarrow{\ell} S_2) \triangleleft \ell' &= (S_1 \xrightarrow{\ell'} S_2) \\
\text{Ref}_\ell S \triangleleft \ell' &= \text{Ref}_{(\ell \lor \ell')} S
\end{align*}
\]

Figure 13 presents the join and meet type functions.

![Fig. 13. SSLRef: Join and meet type functions](image)

**Definition A.1 (Valid Type Sets).**

\[
\begin{align*}
\text{valid}(&\{ \text{Bool}_{\ell_i} \}) \\
&\text{valid}(\{ S_{11} \}) & \text{valid}(\{ S_{12} \}) & \text{valid}(\{ S_i \}) \\
&\text{valid}(\{ S_{11} \xrightarrow{\ell_c} S_{12} \}) & \text{valid}(\{ \text{Ref}_{\ell} S_i \}) \\
&\text{valid}(\{ \text{Unit}_{\ell_i} \})
\end{align*}
\]

A.2 SSLRef: Dynamic semantics

In this section we present in Figure 14 the full definition of the dynamic semantics of SSLRef.

A.3 SSLRef: Noninterference definitions

In this section we present definitions and properties of noninterference for SSLRef. Figure 15 presents the full definition of step-indexed logical relations. The proofs can be found in Appendix B.4.

**Definition A.2.** Let \( \rho \) be a substitution, \( \Gamma \) and \( \Sigma \) a type substitutions. We say that substitution \( \rho \) satisfy environment \( \Gamma \) and \( \Sigma \), written \( \rho \models \Gamma; \Sigma \), if and only if \( \text{dom}(\rho) = \Gamma \) and \( \forall \ell \in \text{dom}(\Gamma), \forall \ell_c, \Gamma; \Sigma; \ell_c \vdash \rho(x) : S' \), where \( S' <: \Gamma(x) \).

**Definition A.3 (Related substitutions).** Tuples \( \langle \ell_1, \rho_1, \mu_1 \rangle \) and \( \langle \ell_2, \rho_2, \mu_2 \rangle \) are related on \( k \) steps, notation \( \Gamma; \Sigma \vdash \langle \ell_1, \rho_1, \mu_1 \rangle \approx_k^{\ell_{\ell_o}} \langle \ell_2, \rho_2, \mu_2 \rangle \), if \( \rho_1 \models \Gamma; \Sigma \vdash \mu_1 \approx_k^{\ell_{\ell_o}} \rho_2 \).
Notion of Reduction

\[ t \mid \mu \xrightarrow{\ell_e} t \mid \mu \]

Reduction

\[
\begin{array}{c}
\begin{array}{c}
b_1\ell_1 \oplus b_2\ell_2 \mid \mu \xrightarrow{\ell_e} (b_1 \oplus b_2)(\ell_1 \lor \ell_2) \mid \mu \\
\text{if } \text{true}_\ell \text{ then } t_1 \mid \mu \xrightarrow{\ell_e} \text{prot}_\ell(t_1) \mid \mu \\
\text{if } \text{false}_\ell \text{ then } t_2 \mid \mu \xrightarrow{\ell_e} \text{prot}_\ell(t_2) \mid \mu \\
\text{prot}_\ell(v) \mid \mu \xrightarrow{\ell_e} v \lor \ell \mid \mu \\
\text{ref}^S v \mid \mu \xrightarrow{\ell_e} \bot \mid \mu[o \mapsto v \lor \ell_c] \text{ where } o \notin \text{dom}(\mu) \\
!o_\ell \mid \mu \xrightarrow{\ell_e} v \lor \ell \mid \mu \text{ where } \mu(o) = v \\
o_\ell := v \mid \mu \xrightarrow{\ell_e} \text{unit}_\bot \mid \mu[o \mapsto v \lor \ell_c \lor \ell] \\
\end{array}
\end{array}
\]

\[ v : S \mid \mu \xrightarrow{\ell_e} v \lor \text{label}(S) \mid \mu \]

Fig. 14. SSL\_Ref: Label Tracking Dynamic Semantics

\[ \mu_2 \text{ and } \forall x \in \Gamma.\Sigma \vdash \langle \ell_1, \rho_1(x), \mu_1 \rangle \approx^k \langle \ell_2, \rho_2(x), \mu_2 \rangle : \Gamma(x) \]

**Definition A.4 (Semantic Security Typing).**

\[ \Gamma; \Sigma; \ell_c \models t : S \iff \forall \ell_o \in \text{Label}, k \geq 0, \rho_1, \rho_2 \in \text{Subst} \text{ and } \mu_1, \mu_2 \in \text{Store} \]

\[ \text{such that } \Sigma \vdash \mu_1 \text{ and } \Gamma; \Sigma \vdash \langle \ell_c, \rho_1, \mu_1 \rangle \approx^k \langle \ell_c, \rho_2, \mu_2 \rangle, \text{ we have } \]

\[ \Sigma \vdash \langle \ell_c, \rho_1(t), \mu_1 \rangle \approx^k \langle \ell_c, \rho_2(t), \mu_2 \rangle : C(S) \]

**Proposition A.5 (Security Type Soundness).** If \( \Gamma; \Sigma; \ell_c \vdash t : S' \) \( \Rightarrow \forall S, S' : S, \Gamma; \Sigma; \ell_c \models t : S \)
$$\Sigma \vdash \langle \ell_1, v_1, \mu_1 \rangle \approx_{\ell_o}^k \langle \ell_2, v_2, \mu_2 \rangle : S \iff \ell_1 \approx_{\ell_o} \ell_2 \land \Sigma \vdash \mu_1 \approx_{\ell_o}^k \mu_2 \land \Sigma; \ell_i \vdash v_i : S_i', S_i' \prec S.$$ 

$$\text{obsRel}_{k, \ell_o}^{\Sigma, S} (\ell_1, v_1, \mu_1, \ell_2, v_2, \mu_2) \iff (\text{rval}(v_1) = \text{rval}(v_2)) \quad \text{if } S \in \{\text{Bool}, \text{Unit}, \text{Ref}_o S'\}$$

$$\text{obsRel}_{k, \ell_o}^{\Sigma, S_1 \mapsto \ell S_2} (\ell_1, v_1, \mu_1, \ell_2, v_2, \mu_2) \iff \forall j \leq k. \forall \Sigma \subseteq \Sigma', \Sigma' \vdash \langle \ell_1, v_1', \mu_1' \rangle \approx_{\ell_o} \langle \ell_2, v_2', \mu_2' \rangle : S_1,$n

$$\Sigma' \vdash \langle \ell_1, v_1', \mu_1' \rangle \approx_{\ell_o} \langle \ell_2, v_2', \mu_2' \rangle : C(S_2 \triangleright g)$$

$$\Sigma \vdash \langle \ell_1, t_1, \mu_1 \rangle \approx_{\ell_o}^k \langle \ell_2, t_2, \mu_2 \rangle : C(S) \iff \ell_1 \approx_{\ell_o} \ell_2 \land \Sigma \vdash \mu_1 \approx_{\ell_o}^k \mu_2 \land \Sigma; t_1 : S_1', S_1' \prec S, \forall j < \ell_o$$

$$\langle t_1 | \mu_i \mapsto t_i' | \mu_i' \rangle \rightarrow \Sigma \subseteq \Sigma', \Sigma' \vdash \mu_1' \approx_{\ell_o} \mu_2' \land (\text{irred}(t_i') \rightarrow \Sigma' \vdash \langle \ell_1, t_1', \mu_1' \rangle \approx_{\ell_o} \langle \ell_2, t_2', \mu_2' \rangle : S)$$

$$\Sigma \vdash \mu_1 \approx_{\ell_o}^k \mu_2 \iff \Sigma \vdash \mu_1 \land \forall \ell_1, \ell_1 \approx_{\ell_o} \ell_2, j < k, \forall \nu \in \text{dom}(\mu_1) \cap \text{dom}(\mu_2)$$

$$\Sigma \vdash \langle \ell_1, \mu_1(o), \mu_1 \rangle \approx_{\ell_o}^j \langle \ell_2, \mu_2(o), \mu_2 \rangle : \Sigma(o)$$

$$\ell_1 \approx_{\ell_o} \ell_2 \iff \text{obs}_{\ell_o} (\ell_1) \lor \neg \text{obs}_{\ell_o} (\ell_1)$$

$$\mu_1 \rightarrow \mu_2 \iff \text{dom}(\mu_1) \subseteq \text{dom}(\mu_2)$$

$$\text{obs}_{\ell_o}(\ell, S) \iff \text{obs}_{\ell_o}(\ell) \land \text{obs}_{\ell_o}(\text{label}(S))$$

$$\text{obs}_{\ell_o}(\ell) \iff \ell \leq \ell_o$$

Fig. 15. Security logical relations
\[
g, g_c, g_r \in \text{GLABEL}, \quad U \in \text{GTYPE}, \quad x \in \text{VAR}, \quad b \in \text{BOOL}, \quad \oplus \in \text{BOOLOP} \\
l \in \text{LOC}, \quad t \in \text{GTERM}, \quad r \in \text{RAWVALUE}, \quad v \in \text{VALUE} \\
\Gamma \in \text{VAR} \xrightarrow{\text{fin}} \text{GTYPE}, \quad \Sigma \in \text{LOC} \xrightarrow{\text{fin}} \text{GTYPE}
\]
\[
U ::= \text{Bool}_g \mid U \xrightarrow{g_c} U \mid \text{Ref}_g U \mid \text{Unit}_g \quad \text{(gradual types)} \\
g ::= \ell \mid ? \quad \text{(gradual labels)} \\
b ::= \text{true} \mid \text{false} \quad \text{(Booleans)} \\
r ::= b \mid \lambda^b \cdot x : U \cdot t \mid \text{unit} \mid o \quad \text{(base values)} \\
v ::= r_g \quad \text{(values)} \\
t ::= v \mid t \mid t \oplus t \mid \text{if} \ t \ \text{then} \ t \ \text{else} \ t \quad \text{(terms)} \\
\oplus ::= \land \mid \lor \quad \text{(operations)}
\]

Fig. 16. GSL\textsubscript{Ref}: Syntax

\[
\begin{align*}
(Ux) & : \quad \frac{x : U \in \Gamma}{\Gamma; \Sigma; g \vdash x : U} \\
(Ub) & : \quad \frac{\alpha : U \in \Sigma}{\Gamma; \Sigma; g_c \vdash \alpha : \text{Ref}_g U} \\
(Uo) & : \quad \frac{\gamma : \text{Ref}_g U}{\Gamma; \Sigma; g_c \vdash \gamma g \vdash t : U} \\
(U\text{prot}) & : \quad \frac{t \vdash \text{prot}_g (t) : U \lor g}{\Gamma; \Sigma; g_c \vdash \text{prot}_g (t) : U \lor g} \\
(U\text{app}) & : \quad \frac{U_2 \leq U_1}{\Gamma; \Sigma; g_c \vdash t_1 : U_1 \xrightarrow{g_c} g U_2} \\
(U:;) & : \quad \frac{U_2 \leq U_2}{\Gamma; \Sigma; g_c \vdash t : U_2 \vdash U_2 \vdash U_2} \\
(U\text{ref}) & : \quad \frac{U' \leq U}{\Gamma; \Sigma; g_c \vdash \text{ref}_U t : \text{Ref}_1 U} \\
(U\text{deref}) & : \quad \frac{U \vdash t : U \lor g}{\Gamma; \Sigma; g_c \vdash \text{Ref}_g U} \\
(U\text{asgn}) & : \quad \frac{\Gamma; \Sigma; g_c \vdash t_1 : U_1 \quad \text{Ref}_U U_1 \quad \Gamma; \Sigma; g_c \vdash t_2 : U_2 \quad U_2 \leq U_1}{\Gamma; \Sigma; g_c \vdash t_1 := t_2 : \text{Unit}_1} \\
\end{align*}
\]

Fig. 17. GSL\textsubscript{Ref}: Static Semantics

A.4 GSL\textsubscript{Ref}: Static semantics

In this section we present the syntax and static semantics of GSL\textsubscript{Ref}. The syntax of GSL\textsubscript{Ref} is given in Figure 16 and is otherwise identical to that of SSL\textsubscript{Ref}. Figure 17 presents the type system of GSL\textsubscript{Ref}. Each typing rule is derived from a corresponding SSL\textsubscript{Ref} rule (Figure 12) by lifting labels, types, predicates, and functions to their gradual counterparts. We also present some additional definitions needed in gradualizing SSL\textsubscript{Ref}, which are not included in the paper. Finally we present some example typing derivations in Figure 19.
A.4.1 Additional Definitions.

**Definition A.6 (Type Concretization).** \( \gamma_S : \mathcal{G} \rightarrow \mathcal{P}(\mathcal{X}) \)

\[
\begin{align*}
\gamma_S(\text{Bool}_r) &= \{ \text{Bool}_r | \ell \in \gamma(g) \} \\
\gamma_S(\text{Unit}_r) &= \{ \text{Unit}_r | \ell \in \gamma(g) \} \\
\gamma_S(\text{Ref}_r U) &= \{ \text{Ref}_r S | \ell \in \gamma(g), S \in \gamma_S(U) \}
\end{align*}
\]

Type concretization induces notions of precision and abstraction.

**Definition A.7 (Type Precision).** \( U_1 \sqsubseteq U_2 \), if and only if \( \gamma_S(U_1) \subseteq \gamma_S(U_2) \).

**Definition A.8 (Type Abstraction).** \( \alpha_S : \mathcal{P}(\mathcal{X}) \rightarrow \mathcal{G} \)

\[
\begin{align*}
\alpha_S(\{ \text{Bool}_r \}) &= \text{Bool}_r(\gamma) \\
\alpha_S(\{ \text{Unit}_r \}) &= \text{Unit}(\gamma) \\
\alpha_S(\{ \text{Ref}_r S \}) &= \text{Ref}(\gamma_S(S))
\end{align*}
\]

**Proposition A.9 (\( \alpha_S \) is Sound and Optimal).** Assuming \( \hat{S} \) valid:

(i) \( \hat{S} \subseteq \gamma_S(\alpha_S(\hat{S})) \)

(ii) If \( \hat{S} \subseteq \gamma_S(U) \) then \( \alpha_S(\hat{S}) \subseteq U \).

**Definition A.10 (Gradual label meet).**

\( g_1 \alpha g_2 = \alpha(\{ \ell_1 \land \ell_2 | (\ell_1, \ell_2) \in \gamma(g_1) \times \gamma(g_2) \}) \). Algorithmically:

\[
\ell_1 \alpha \ell_2 = \ell_1 \land \ell_2
\]

**Fig. 18. GSLRef:** consistent join and consistent meet

**Definition A.11 (Gradual label join).** \( g_1 \alpha \gamma g_2 = \alpha(\{ \ell_1 \lor \ell_2 | (\ell_1, \ell_2) \in \gamma(g_1) \times \gamma(g_2) \}) \)

Algorithmically:

\[
\ell_1 \alpha \ell_2 = \ell_1 \lor \ell_2
\]

**Definition A.12 (Label Meet).** \( g_1 \land g_2 = \alpha(\gamma(g_1) \cap \gamma(g_2)) \).

Algorithmically:

\[
g \land g = g
\]

\[
g \lor g = g
\]
Definition A.13 (Type Meet). \( U_1 \sqcap U_2 = \alpha_S(\gamma_S(U_1) \cap \gamma_S(U_2)) \).
Algoritmically:

\[
\begin{array}{c}
g \cap g' \\
\text{Bool}_g \sqcap \text{Bool}_{g'} \\
.U_1 \sqcap U'_1 \quad U_2 \sqcap U'_2 \quad g_1 \sqcap g'_1 \quad g_2 \sqcap g'_2 \\
\text{Ref}_g U_1 \sqcap \text{Ref}_{g'} U_2 \\
\end{array}
\]

Also, we introduce a function \( \text{label} \), which yields the security label of a given type:

\[
\text{label} : \text{GType} \rightarrow \text{Label}
\]

\[
\begin{array}{c}
\text{label}(\text{Bool}_g) = g \\
\text{label}(\text{Unit}_g) = g \\
\text{label}(U_1 \rightarrow g U_2) = g \\
\text{label}(\text{Ref}_g U) = g \\
\end{array}
\]

Definition A.14 (Type Precision (inductive definition)).

\[
\begin{array}{c}
g_1 \sqsubseteq g_2 \\
\text{Bool}_{g_1} \sqsubseteq \text{Bool}_{g_2} \\
\text{Unit}_{g_1} \sqsubseteq \text{Unit}_{g_2} \\
U_{11} \sqsubseteq U_{21} \quad U_{12} \sqsubseteq U_{22} \quad g_1 \sqsubseteq g_2 \quad g_{c1} \sqsubseteq g_{c2} \\
\text{Ref}_{g_1} U_1 \sqsubseteq \text{Ref}_{g_2} U_2 \\
\end{array}
\]

Definition A.15 (Consistent label ordering (inductive definition)).

\[
\begin{array}{c}
? \preceq g \\
\text{Bool}_{?} \preceq \text{Bool}_{g'} \\
\text{Unit}_{?} \preceq \text{Unit}_{g'} \\
\text{Ref}_{g} U_1 \preceq \text{Ref}_{g'} U_2 \\
\end{array}
\]

Definition A.16 (Consistent subtyping (inductive definition)).

\[
\begin{array}{c}
g \preceq g' \\
\text{Bool}_{g} \preceq \text{Bool}_{g'} \\
\text{Unit}_{g} \preceq \text{Unit}_{g'} \\
\text{Ref}_{g} U_1 \preceq \text{Ref}_{g'} U_2 \\
\end{array}
\]

A.5 \( \text{GSL}^\epsilon_{\text{Ref}} \): Static semantics

In this section we present the full definition of the static semantics of \( \text{GSL}^\epsilon_{\text{Ref}} \).

Definition A.17 (Interval). An interval is a bounded unknown label \([\ell_1, \ell_2]\) where \( \ell_1 \) is the upper bound and \( \ell_2 \) is the lower bound.

\[
\begin{array}{c}
i \in \text{Label}^2 \\
i ::= [\ell_1, \ell_2] \quad \text{(interval)}
\end{array}
\]

Definition A.18 (Evidence for labels).

\[
\epsilon ::= \langle i, i \rangle
\]

Definition A.19 (Type Evidence). An evidence type is a gradual type labeled with an interval:

\[
\begin{array}{c}
E \in \text{GEType}, \quad i \in \text{Label}^2 \\
E ::= \text{Bool}_i \mid E \rightarrow_i E \mid \text{Ref}_i E \mid \text{Unit}_i \\
\text{(type evidences)}
\end{array}
\]

Definition A.20 (Evidence for types).

\[
\epsilon ::= \langle E, E \rangle
\]

We present the syntax of \( \text{GSL}^\epsilon_{\text{Ref}} \) in Figure 20 and the static semantics in Figure 21.
The initial evidence function for consistent label ordering is presented in Figure 28. The initial evidence function for consistent subtyping is presented in Figure 29 using the following definition:

In this section we present the translation from terms of GSL

\[ A.7 \text{ GSL} \]

The initial evidence function for consistent label ordering is presented in Figure 28. The initial evidence function for consistent subtyping is presented in Figure 29 using the following definition of operation pattern:

Fig. 19. \text{GSL}_{\text{Ref}}$: Example typing derivations

\[
t ::= v | et @ e | et \oplus et | \text{if } et \text{ then } et \text{ else } et | \text{ref}^U \text{ } et | !et | et := e \text{ } et | \text{prot}_e, eg(et) | et
\]

\[
r ::= b | (\lambda^x. t) | \text{unit} | o
\]

\[
u ::= r_g | x
\]

\[
v ::= u | \epsilon u
\]

Fig. 20. \text{GSL}^e_{\text{Ref}}$: Syntax

A.6 \text{GSL}^e_{\text{Ref}}$: Dynamic semantics

In this section we present the full definition of the dynamic semantics of \text{GSL}^e_{\text{Ref}}.

We extend the syntax of \text{GSL}_{\text{Ref}} with frames defined as follows:

\[
f ::= h[\epsilon]
\]

\[
h ::= \Box @ et | ev \oplus \Box | \Box @ e et | ev @ e \Box | \epsilon \Box | \text{if } \Box \text{ then } et \text{ else } et | !\Box | \Box := \epsilon \text{ et } | ev := \epsilon \Box | \text{ref}^U \epsilon \Box
\]

We present the complete dynamic semantics in Figure 22, and the evaluation frames and reduction in Figure 23. Auxiliary functions for evidence for labels is presented in Figure 24. Auxiliary functions for evidence for types is shown in Figure 25, and the inversion functions for evidence in Figure 26.

A.7 \text{GSL}_{\text{Ref}}$: Translation to \text{GSL}^e_{\text{Ref}}

In this section we present the translation from terms of \text{GSL}_{\text{Ref}} into terms of \text{GSL}^e_{\text{Ref}} in Figure 27. The initial evidence function for consistent label ordering is presented in Figure 28. The initial evidence function for consistent subtyping is presented in Figure 29 using the following definition of operation pattern:
A.8 Noninterference definitions

Definition A.22 (Related substitutions). Tuples \( \langle \hat{g}_1, \rho_1, \mu_1 \rangle \) and \( \langle \hat{g}_2, \rho_2, \mu_2 \rangle \) are related on \( k \) steps under \( \Gamma \) and \( \Sigma \), notation \( \Gamma; \Sigma \vdash \langle \hat{g}_1, \rho_1, \mu_1 \rangle \approx_{k, \ell_\alpha}^k \langle \hat{g}_2, \rho_2, \mu_2 \rangle \), if \( \rho_1 \models \Gamma; \Sigma \vdash \mu_1 \approx_{k, \ell_\alpha}^k \mu_2 \) and

\[ \forall x \in \text{dom}(\Gamma). \Sigma \vdash \langle \hat{g}_1, \rho_1(x), \mu_1 \rangle \approx_{k, \ell_\alpha}^k \langle \hat{g}_2, \rho_2(x), \mu_2 \rangle : \Gamma(x) \]
\( (r1) \quad \varepsilon_1(b_1 g_1 \oplus \varepsilon_2 b_2 g_2) \mid \mu \xrightarrow{\varepsilon_1 g_1} (\varepsilon_1 \triangleright \varepsilon_2)(b_1 [\oplus] b_2) (g_1 \triangleright g_2) \mid \mu \quad \rightarrow : C \times (C \cup \{\text{error}\}) \)

\( (r2) \quad \text{prot}_{\varepsilon_1 g_1} \varepsilon_2 g_2 (\varepsilon_3 u) \mid \mu \xrightarrow{\varepsilon_2 g_2} (\varepsilon_3 \triangleright \varepsilon_1)(u \triangleright g_1) \mid \mu \)

\( (r3) \quad \varepsilon_1 (\lambda x : U.t)_g @ \varepsilon_2 u \mid \mu \xrightarrow{\varepsilon_2 g} \begin{cases} \text{prot}_{\text{ilbl}(\varepsilon_1) g} \varepsilon' g'(\text{icod}(\varepsilon_1)([\varepsilon_2 u/x]t)) \mid \mu \\ \text{error} \quad \text{if } \varepsilon'_1 \text{ or } \varepsilon'_2 \text{ are not defined} \end{cases} \)

where:
\( \varepsilon'_1 = (\varepsilon_1 \triangleright \text{ilbl}(\varepsilon_1)) \circ \varepsilon_3 \circ \text{lat}(\varepsilon_1) \)
\( \varepsilon'_2 = \varepsilon_2 \circ \text{ilbl}(\varepsilon_1) \)
\( g_1' = (g_c \triangleright g) \)

\( (r4) \quad \text{if } \varepsilon_1 b g_1 \text{ then } t_2 \text{ else } t_3 \mid \mu \xrightarrow{\varepsilon_1 g} \begin{cases} \text{prot}_{\text{ilbl}(\varepsilon_1) g} \varepsilon' g'(\varepsilon_2 t_2) \mid \mu \quad \text{if } b = \text{true} \\ \text{prot}_{\text{ilbl}(\varepsilon_1) g} \varepsilon' g'(\varepsilon_3 t_3) \mid \mu \quad \text{if } b = \text{false} \end{cases} \)

where:
\( \varepsilon' = \varepsilon_1 \triangleright \text{ilbl}(\varepsilon_1) \)
\( g' = g_c \triangleright g_1 \)

\( (r5) \quad \text{ref}_{\text{ilbl}(\varepsilon_1) g} \text{ } !\varepsilon_1 u \mid \mu \xrightarrow{\varepsilon_2 g} \begin{cases} o_\bot \mid \mu[o \mapsto \varepsilon'(u \triangleright g_c)] \\ \text{error} \quad \text{if } (\varepsilon \circ \varepsilon_2) \text{ is not defined} \end{cases} \)

where:
\( o \notin \text{dom}(\mu) \)
\( \varepsilon' = \varepsilon_1 \triangleright (\varepsilon \circ \varepsilon_2) \)

\( (r6) \quad 1 : \varepsilon_1 \mu g \mid \mu \xrightarrow{\text{prot}_{\text{ilbl}(\varepsilon_1) g} \varepsilon' g'(\text{iref}(\varepsilon_1)v)} \)

where:
\( \mu(o) = v \)
\( \varepsilon' = \varepsilon_1 \triangleright \text{ilbl}(\varepsilon_1) \)
\( g' = g_c \triangleright g \)

\( (r7) \quad \varepsilon_1 o g := \varepsilon_2 u \mid \mu \xrightarrow{\varepsilon_2 g} \begin{cases} \text{unit}_\bot \mid \mu[o \mapsto \varepsilon'(u \triangleright (g_c \triangleright g))] \\ \text{error} \quad \text{if } \varepsilon' \text{ is not defined, or } \varepsilon \preceq \text{ilbl}(\varepsilon') \text{ does not hold} \end{cases} \)

where:
\( \mu(o) = \varepsilon'' u' \)
\( \varepsilon' = (\varepsilon_2 \circ \text{ilbl}(\varepsilon_1)) \triangleright ((\varepsilon \triangleright \text{ilbl}(\varepsilon_1)) \circ \varepsilon_3 \circ \text{ilbl}(\text{iref}(\varepsilon_1))) \)
\( \varepsilon_1(\varepsilon_2 u) \rightarrow_{\varepsilon} \begin{cases} (\varepsilon_2 \circ \varepsilon_1) u \\ \text{error} \quad \text{if not defined} \end{cases} \rightarrow_{\varepsilon} : \text{EvTERM} \times (\text{EvTERM} \cup \{\text{error}\}) \)

Fig. 22. GSL* \( \text{Ref} \) : Dynamic semantics

**Definition A.23 (Semantic Security Typing).**

\( \Gamma; \Sigma; \hat{g} \models t : U \iff \forall \ell_o \in \text{LABEL}, k \geq 0, \rho_1, \rho_2 \in \text{SUBST} \) and \( \mu_1, \mu_2 \in \text{STORE} \)

such that \( \Sigma \vdash \mu_1 \) and \( \Gamma; \Sigma \vdash \langle \hat{g}, \rho_1, \mu_1 \rangle \approx_{\ell_o} \langle \hat{g}, \rho_2, \mu_2 \rangle \), we have
\( \Sigma \vdash \langle \hat{g}, \rho_1(t), \mu_1 \rangle \approx_{\ell_o} \langle \hat{g}, \rho_2(t), \mu_2 \rangle : C(U) \)
Proof in Appendix E.
Type-Driven Gradual Security with References

\[ \text{Boolean} \cap \text{Boolean} = \text{Boolean} \cap \text{Boolean} \]

\[ (E_1 \xrightarrow{i_1} i_1E_{12}) \cap (E_2 \xrightarrow{i_2} i_2E_{22}) = (E_1 \xrightarrow{i_1} i_1E_{12}) \cap (E_2 \xrightarrow{i_2} i_2E_{22}) \]

\[ E \cap E' \text{ undefined otherwise} \]

\[ \text{Ref}_1 \ E_1 \cap \text{Ref}_1 \ E_2 = \text{Ref}_1 \ E_1 \cap \text{Ref}_1 \ E_2 \]

\[ \langle E_1, E_2 \rangle \cap \langle t_1, t_1 \rangle = \langle E_1 \cap E_2 \rangle \]

\[ \langle E_1, E_2 \rangle \cap \langle t_1, t_2 \rangle = \langle E_1 \cap E_2 \rangle \]

\[ \langle E_1, E_2 \rangle \cap \langle t_2, t_2 \rangle = \langle E_1 \cap E_2 \rangle \]

\[ \Delta^<\langle (t_1, t_2, t_3) \rangle = \langle t'_1, t'_3 \rangle \]

\[ \Delta^<\langle (E_1, E_2, E_{11}) \rangle = \langle E'_1, E'_{11} \rangle \]

\[ \Delta^<\langle (E_2, E_{22}, E_{33}) \rangle = \langle E'_2, E'_{33} \rangle \]

\[ \Delta^<\langle (Ref_1, E_1, Ref_2, E_2, Ref_3, E_3) \rangle = \langle Ref'_1, E'_1, Ref'_2, E'_2, Ref'_3, E'_3 \rangle \]

\[ \langle E_1, E_2 \rangle \circ \Delta^<: \langle E_{22}, E_3 \rangle = \Delta^<\langle E_1, E_2 \cap E_{22}, E_3 \rangle \]

Fig. 25. GSI<sup>E_ref</sup> Auxiliary functions for the dynamic semantics (Types)
\[ilbl((\text{Bool}_i, \text{Bool}_{i_2})) = \langle i_1, i_2\rangle\]
\[ilbl((\text{Unit}_i, \text{Unit}_{i_2})) = \langle i_1, i_2\rangle\]
\[ilbl((\text{Ref}_i, U_{i_1}, \text{Ref}_{i_2} U_{i_2})) = \langle i_1, i_2\rangle\]
\[ilbl(\langle E\xrightarrow{i_{i_1}} E_1, E\xrightarrow{i'_{i_2}} E'_1\rangle) = \langle i_{i_1}, i'_1\rangle\]

\[iref((\text{Ref}_i, E_1, \text{Ref}_{i_2} E_2)) = \langle E_1, E_2\rangle\]
\[iref(\langle E_1, E_2\rangle) = \text{undefined otherwise}\]

\[idom(\langle E\xrightarrow{i_{i_1}} E_1, E\xrightarrow{i'_{i_2}} E'_1\rangle) = \langle E'_1, E_1\rangle\]
\[idom(\langle E_1, E_2\rangle) = \text{undefined otherwise}\]

\[icod(\langle E\xrightarrow{i_{i_1}} E_1, E\xrightarrow{i'_{i_2}} E'_1\rangle) = \langle E_2, E'_2\rangle\]
\[icod(\langle E_1, E_2\rangle) = \text{undefined otherwise}\]

Fig. 26. GSL^Ref: Inversion functions for evidence
\[ \Gamma; \Sigma; g_c + t \leadsto t' : U \]

\((T_x)\) \quad \Gamma(x) = U \\
\quad \Gamma; \Sigma; g_c + x \leadsto x : U

\((T_b)\) \quad \Gamma; \Sigma; g_c + b_g \leadsto b_g : \text{Bool}_g

\((T_u)\) \quad \Gamma; \Sigma; g_c + \text{unit}_g \leadsto \text{unit}_g : \text{Unit}_g

\((T_\lambda)\) \quad \Gamma; \Sigma; g_c + \lambda x : U_1. t \leadsto (\lambda x : U_1. t')_g : U_1 \rightarrow_U U_2

\((T)\) \quad \Gamma; \Sigma; g_c + t \leadsto t'_1 : \text{Bool}_g \\
\quad \Gamma; \Sigma; g_c + t_2 \leadsto t'_2 : \text{Bool}_g \\
\quad \epsilon_1 = g^{\subseteq}[\text{Bool}_g] \\
\quad \epsilon_2 = g^{\subseteq}[\text{Bool}_g]

\((T_\top)\) \quad \Gamma; \Sigma; g_c + t_1 \leadsto t'_1 : U_1 \\
\quad \Gamma; \Sigma; g_c + t_2 \leadsto t'_2 : U_2 \\
\quad \epsilon_1 = g^{\subseteq}[U_1] \\
\quad \epsilon_2 = g^{\subseteq}[U_2 \leq U_1] \\
\quad \epsilon_3 = g^{\subseteq}[U_2 \leq U_3] \\
\quad \epsilon_4 = g^{\subseteq}[U_3 \leq U_2 \hat{v} U_3]

\((T_{\text{if}})\) \quad \Gamma; \Sigma; g_c + \text{if } t_1 \text{ then } t_2 \text{ else } t_3 \leadsto \text{if } \epsilon_1 \epsilon_2 \epsilon_3 \epsilon_4 \text{ then } \epsilon_5 \epsilon_6 \epsilon_7 \epsilon_8 \text{ else } \epsilon_9 \epsilon_{10} \epsilon_{11} \epsilon_{12} \text{ if } \epsilon_{13} \epsilon_{14} \epsilon_{15} \epsilon_{16} \text{ then } \epsilon_{17} \epsilon_{18} \epsilon_{19} \epsilon_{20} \text{ else } \epsilon_{21} \epsilon_{22} \epsilon_{23} \epsilon_{24} \text{ : } (U_2 \hat{v} U_3) \hat{v} g

\((T_{\text{assign}})\) \quad \Gamma; \Sigma; g_c + t_1 := t_2 \leadsto t'_1 := \epsilon_1 \epsilon_2 \epsilon_3 t'_2 : \text{Unit}_\bot

\((T_{\text{ref}})\) \quad \Gamma; \Sigma; g_c + r \leadsto \epsilon_1 \epsilon_2 \epsilon_3 t'_1 : \text{Ref}_U

\((T_{\text{deref}})\) \quad \Gamma; \Sigma; g_c + !t \leadsto !t' : U \hat{v} g

\[ g^{\subseteq}[g] = g^{\subseteq}[g \hat{<} g] \text{ and } g^{\subseteq}[U] = g^{\subseteq}[U \leq U] \]

Fig. 27. GSLRef: translation to GSLRef terms
bounds(?) = [⊥, ⊤]
bounds(ℓ) = [ℓ, ℓ]

bounds(x₁ ∨ x₂) = bounds(x₁) ∨ bounds(x₂)
bounds(x₁ ∧ x₂) = bounds(x₁) ∧ bounds(x₂)

bounds(F₁(∀₁) ≺ bounds(F₂(∀₂))

bounds(F₁(∀₁) ∨ F₂(∀₂)) = bounds(F₁(∀₁)) ∨ bounds(F₂(∀₂))

bounds(F₁(∀₁) ∧ F₂(∀₂)) = bounds(F₁(∀₁)) ∧ bounds(F₂(∀₂))

bounds(F₁(∀₁) ⊓ F₂(∀₂)) = bounds(F₁(∀₁)) ⊓ bounds(F₂(∀₂))

bounds(F₁(∀₁) ≺ F₂(∀₂)) = bounds(F₁(∀₁)) ≺ bounds(F₂(∀₂))

bounds(F₁(∀₁) ⊓ F₂(∀₂)) = bounds(F₁(∀₁)) ⊓ bounds(F₂(∀₂))

where F₁ : GLABELⁿ → GLABEL and F₂ : GLABELᵐ → GLABEL.

Fig. 28. GSLᵣ: Initial evidence for gradual labels
\[
\begin{align*}
\text{liftP(\_)} & = _\text{\_} \\
\text{liftP}(P_1^T \vee P_2^T) & = \text{liftP}(P_1^T) \vee \text{liftP}(P_2^T) \\
\text{liftP}(P_1^T \wedge P_2^T) & = \text{liftP}(P_1^T) \wedge \text{liftP}(P_2^T) \\
\text{liftP}(P_1^T \sqcap P_2^T) & = \text{liftP}(P_1^T) \sqcap \text{liftP}(P_2^T) \\
\text{invert(\_)} & = _\text{\_} \\
\text{invert}(P_1^T \vee P_2^T) & = \text{invert}(P_1^T) \vee \text{invert}(P_2^T) \\
\text{invert}(P_1^T \wedge P_2^T) & = \text{invert}(P_1^T) \wedge \text{invert}(P_2^T) \\
\text{invert}(P_1^T \sqcap P_2^T) & = \text{invert}(P_1^T) \sqcap \text{invert}(P_2^T) \\
\text{tomeet(\_)} & = _\text{\_} \\
\text{tomeet}(P_1^T \vee P_2^T) & = \text{tomeet}(P_1^T) \sqcup \text{tomeet}(P_2^T) \\
\text{tomeet}(P_1^T \wedge P_2^T) & = \text{tomeet}(P_1^T) \sqcap \text{tomeet}(P_2^T) \\
\text{tomeet}(P_1^T \sqcap P_2^T) & = \text{tomeet}(P_1^T) \sqcap \text{tomeet}(P_2^T) \\
\end{align*}
\]

\[\theta[[\text{liftP}(G_1(\bar{T}_1)) <: \text{liftP}(G_2(\bar{T}_j))] = \langle t_1, t_2^j \rangle\]

\[\theta[[G_1(\text{Bool}_{g_1}) \triangleleft G_2(\text{Bool}_{g_2})]] = \langle \text{Bool}_{t_1}, \text{Bool}_{t_2} \rangle\]

\[\theta[[\text{invert}(G_2(\bar{U}_{j_1})) <: \text{invert}(G_1(\bar{U}_{i_1}))]] = \langle E_{21}', E_{11}' \rangle\]

\[\theta[[G_1(\bar{U}_{i_2}) <: G_2(\bar{U}_{j_2})]] = \langle E_{12}, E_{22} \rangle \]

\[\theta[[\text{liftP}(G_1(\bar{T}_1)) <: \text{liftP}(G_2(\bar{T}_{j_2}))]] = \langle t_{i_1}, t_{j_2} \rangle\]

\[\theta[[\text{liftP}(\text{invert}(G_2)(\bar{T}_{j_2})) <: \text{liftP}(\text{invert}(G_1)(\bar{T}_{i_2}))]] = \langle t_{i_2}, t_{j_2} \rangle\]

\[\theta[[G_1(\bar{U}_{i_1} \xrightarrow{g_1} u_{i_2}) <: G_2(\bar{U}_{j_1} \xrightarrow{g_1} u_{j_2})]] = \langle E_{11}(t_{i_1} \xrightarrow{g_1} e_{i_2})_{i_1}, E_{12}, E_{21}(t_{j_1} \xrightarrow{g_1} e_{j_2})_{j_2} \rangle\]

\[\theta[[\text{tomeet}(G_1(\bar{U}_i)) <: \text{tomeet}(G_2(\bar{U}_j))]] = \langle E_{1}, E_{2} \rangle\]

\[\theta[[\text{tomeet}(G_1(\bar{U}_j)) <: \text{tomeet}(G_2(\bar{U}_i))]] = \langle E_{2}, E'_{1} \rangle\]

\[\theta[[G_1(\text{Ref}_{g_1} \bar{U}_i) <: G_2(\text{Ref}_{g_2} \bar{U}_j)]] = \langle \text{Ref}_{g_1} E_{1} \cap E'_{1}, \text{Ref}_{g_2} E_{2} \cap E'_{2} \rangle\]

where \(G_1: \text{GLABEL}^m \rightarrow \text{GLABEL}\) and \(G_2: \text{GLABEL}^m \rightarrow \text{GLABEL}\), and \(G_1(x_1, ..., x_n) = P_1^T(x_1, ..., x_n)\), \(G_2(x_1, ..., x_m) = P_2^T(x_1, ..., x_m)\).

\[\theta_\cup(F(U_1, ..., U_n)) = \theta[[F(U_1, ..., U_n) <: F(U_1, ..., U_n)]]\]

Fig. 29. GSL_{\text{Ref}}^\cup: Initial evidence for gradual types
\[ \Sigma \vdash (\hat{g}_1, v_1, \mu_1) \approx^k_{\ell_o} (\hat{g}_2, v_2, \mu_2) : U \iff \hat{g}_1 \approx_{\ell_o} \hat{g}_2 \land \Sigma \vdash \mu_1 \approx^k_{\ell_o} \mu_2 \land \vdash; \Sigma; \hat{g}_1 \vdash v_1 : U \land \\
(\text{obsVal}^U_{\ell_o}(v_1) \lor \neg \text{obsVal}^U_{\ell_o}(v_1)) \land ((\text{obsVal}^U_{\ell_o}(v_1) \land \text{obsEv}^U_{\ell_o}(\epsilon_1)) \implies \text{obsRel}_{\Sigma, \ell_o}^U(\hat{g}_1, v_1, \mu_1, \hat{g}_2, v_2, \mu_2) \)
\]
where \( \hat{g}_i = \epsilon_i g_i \), and \( \epsilon_i \vdash g_i \leq \hat{g}_i' \).

\[ \text{obsRel}_{\Sigma, \ell_o}^U(\hat{g}_1, v_1, \mu_1, \hat{g}_2, v_2, \mu_2) \iff \text{rval}(v_1) = \text{rval}(v_2) \quad \text{if} \ U \in \{\text{Bool}_g, \text{Unit}_g, \text{Ref}_g U'\} \]

\[ \text{obsRel}_{\Sigma, \ell_o}^U(\hat{g}_1, v_1, \mu_1, \hat{g}_2, v_2, \mu_2) \implies \forall j \leq k. \forall U' = U'_1 \cdot g_{31}^j \cdot U'_2, \forall U'_1, \forall \hat{g}_1', \text{ s.t. } \hat{g}_1 \leq_{\ell_o} \hat{g}_1', \\
\text{and } \epsilon_{11} \vdash U_1^j \cdot g_{31}^j \cdot U_2 \leq U', \text{ and } \epsilon_{12} \vdash U'_1 \leq U'_1', \text{ and } g_{31}^j \cdot \hat{g}_1' \land \forall \hat{g}_1' \text{ we have:} \\
\forall v_1', \mu_1', \Sigma', \Sigma \subseteq \Sigma'. \forall (\hat{g}_1, v_1', \mu_1') \approx_{\ell_o}^j (\hat{g}_2, v_2', \mu_2') : U'_1', \text{ dom}(\mu_1) \subseteq \text{dom}(\mu_1'), \\
\Sigma' \vdash (\hat{g}_1, (\epsilon_{11} v_1 \cdot \epsilon_{31}^j \cdot \epsilon_{12} v_1'), \mu_1') \approx_{\ell_o}^j (\hat{g}_2, (\epsilon_{11} v_2 \cdot \epsilon_{32} \cdot \epsilon_{12} v_2'), \mu_2') : C(U'_1' \lor g_{31}^j) \)
\]
where \( \hat{g}_1' = \epsilon_1' g_1 \), and \( \epsilon_1' \vdash g_i' \leq g_{31}' \).

\[ \text{Fig. 30. Related values} \]

\[ \Sigma \vdash (\hat{g}_1, t_1, \mu_1) \approx^k_{\ell_o} (\hat{g}_2, t_2, \mu_2) : C(U) \iff \hat{g}_1 \approx_{\ell_o} \hat{g}_2 \land \mu_1 \approx_{\ell_o} \mu_2 \land \forall \hat{g}_1', \text{ s.t. } \hat{g}_1 \leq_{\ell_o} \hat{g}_1' \text{ and} \\
\vdash; \Sigma; \hat{g}_1' \vdash t_1 : U, \forall j < k, (t_1 | \mu_1) \rightarrow_{\ell_o}^j t_1' | \mu_1' \implies \exists \Sigma', \Sigma \subseteq \Sigma' \\
\Sigma' \vdash \mu_1' \approx_{\ell_o}^{k-j} \mu_2' \land ((\text{irred}(t_1') \land \text{irred}(t_2'))) \implies \Sigma' \vdash (\hat{g}_1, t_1', \mu_1') \approx_{\ell_o}^{k-j} (\hat{g}_2, t_2', \mu_2') : U) \]

\[ \text{Fig. 31. Related computations for intrinsic terms} \]
B STATIC SECURITY TYPING WITH REFERENCES

In this section we present the proof of type preservation for SSLRef in Sec. B.1, and the definitions and proof of noninterference for SSLRef in Sec. B.2.

B.1 SSLRef: Static type safety

In this section we present the proof of type safety for SSLRef.

Definition B.1 (Well typeness of the store). A store \( \mu \) is said to be well typed with respect to a typing context \( \Gamma \) and a store typing \( \Sigma \), written \( \Gamma; \Sigma \vdash \mu \), if \( \text{dom}(\mu) = \text{dom}(\Sigma) \) and \( \forall o \in \text{dom}(\mu), \Gamma; \Sigma; \perp \vdash \mu(o) : S \text{ and } S <:\Sigma(o) \).

Lemma B.2. If \( \Gamma; \Sigma; \ell_c \vdash t : S \) then \( \forall \ell_c' \leq \ell_c, \Gamma; \Sigma; \ell_c' \vdash t : S \).

Proof. By induction on the derivation of \( \Gamma; \Sigma; \ell_c \vdash t : S \). Noticing that none of the inferred types of the type rules depend on \( \ell_c \).

Case (Sx, Sb, Su, Sl). Trivial because neither the premises and the inferred type depend on the security effect.

Case (S\( \otimes \)). Then \( t = b_1\ell_1 \oplus b_2\ell_2 \) and

\[
\begin{align*}
\text{(Sb)} & \quad \Gamma; \Sigma; \ell_c \vdash b_1\ell_1 \text{ : } \text{Bool}_{\ell_1} \\
\text{(Sb)} & \quad \Gamma; \Sigma; \ell_c \vdash b_2\ell_2 \text{ : } \text{Bool}_{\ell_2} \\
\text{(S\( \otimes \))} & \quad \Gamma; \Sigma; \ell_c \vdash b_1\ell_1 \oplus b_2\ell_2 \text{ : } \text{Bool}_{(\ell_1,\ell_2)}
\end{align*}
\]

Suppose \( \ell_c' \) such that \( \ell_c' \leq \ell_c \), then by induction hypotheses on the premises:

\[
\begin{align*}
\text{(Sb)} & \quad \Gamma; \Sigma; \ell_c' \vdash b_1\ell_1 \text{ : } \text{Bool}_{\ell_1} \\
\text{(Sb)} & \quad \Gamma; \Sigma; \ell_c' \vdash b_2\ell_2 \text{ : } \text{Bool}_{\ell_2} \\
\text{(S\( \otimes \))} & \quad \Gamma; \Sigma; \ell_c' \vdash b_1\ell_1 \oplus b_2\ell_2 \text{ : } \text{Bool}_{(\ell_1',\ell_2')}
\end{align*}
\]

where \( \ell_1' = \ell_1 \) and \( \ell_2' = \ell_2 \) and the result holds.

Case (Sprot). Then \( t = \text{prot}_\ell(t) \) and

\[
\begin{align*}
\text{(Sprot)} & \quad \Gamma; \Sigma; \ell_c \triangleright \ell \vdash t : S \\
\Gamma; \Sigma; \ell_c \vdash \text{prot}_\ell(t) : S \triangleright \ell
\end{align*}
\]

Suppose \( \ell_c' \) such that \( \ell_c' \leq \ell_c \). Considering that \( \ell_c' \triangleright \ell \leq \ell_c \triangleright \ell \), then by induction hypotheses on the premise:

\[
\begin{align*}
\text{(Sprot)} & \quad \Gamma; \Sigma; \ell_c' \triangleright \ell \vdash t : S \\
\Gamma; \Sigma; \ell_c' \vdash \text{prot}_\ell(t) : S \triangleright \ell
\end{align*}
\]

and therefore the result holds.

Case (Sapp). Then \( t = t_1 \backslash t_2 \) and

\[
\begin{align*}
\text{(S\&)} & \quad D_1 \\
\text{\( D_2 \))} & \quad \Gamma; \Sigma; \ell_c \vdash t_1 : S_{11} \xrightarrow{\ell_c'} S_{12} \\
\text{(Sapp)} & \quad \Gamma; \Sigma; \ell_c \vdash t_2 : S_2 \quad \ell_c \triangleright \ell \leq \ell_c'' \quad S_2 <: S_{11} \\
\Gamma; \Sigma; \ell_c \vdash t_1 \backslash t_2 : S_{12} \triangleright \ell
\end{align*}
\]
Suppose $\ell'_c$ such that $\ell'_c \leq \ell_c$. Then by using induction hypotheses on the premises, considering $S_{11} \xrightarrow{\ell''_c} S_{12}' < S_{11} \xrightarrow{\ell''_c} S_{12}$ and $S_{1}'' : S_2$. As $S_2 : S_{11}$ and $S_{11} : S_1''$ then $S_2' : S_{11}$. Also, by definition of the join operator $\ell'_c \land \ell' \leq \ell_c \land \ell \leq \ell''_c \leq \ell'''_c$, and then:

\[ \frac{{(S_d)}}{{\Gamma; \Sigma; \ell'_c + t_1 : S_{11} \xrightarrow{\ell''_c} S_{12}^{'}}}
\]

\[ \frac{{(S_{app})}}{{\Gamma; \Sigma; \ell'_c + t_2 : S_2'' ; \ell'_c \land \ell' \leq \ell''_c \leq \ell'''_c ; S_2' : S_{11}^{'}}}
\]

Where $S_1'' \land \ell' = S_{12} \land \ell$ and the result holds.

**Case (Sif-true).** Then $t = \text{if true}_\ell$ then $t_1$ else $t_2$ and

\[ \frac{{(Sif)}}{{\Gamma; \Sigma; \ell_c \land \ell \leq t_2 : S_2}}
\]

Suppose $\ell'_c$ such that $\ell'_c \leq \ell_c$. As $\ell'_c \land \ell \leq \ell_c \land \ell$, by induction hypotheses in the premises:

\[ \frac{{(Sif)}}{{\Gamma; \Sigma; \ell'_c \land \ell \leq t_2 : S_2'}}
\]

where $S_1' = S_1, S_2' = S_2$. Then $(S_1' \lor S_2') \land \ell = (S_1 \lor S_2) \land \ell$ and therefore the result holds.

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

**Case (Sref).** Then $t = \text{ref}^S \nu$ and

\[ \frac{{(Sref)}}{{\Gamma; \Sigma; \ell_c \land \ell \leq \text{ref}^S \nu : \nu \land \ell}}
\]

Suppose $\ell'_c$ such that $\ell'_c \leq \ell_c$. By using induction hypotheses in the premise, considering $\ell'_c \leq \ell_c \leq \text{label}(S)$:

\[ \frac{{(Sref)}}{{\Gamma; \Sigma; \ell'_c \land \ell \leq \text{ref}^S \nu : \nu \land \ell'}}
\]

and the result holds.

**Case (Sderef).** Then $t = !\sigma_\ell$ and

\[ \frac{{(Sderef)}}{{\sigma : S \in \Sigma}}
\]

Suppose $\ell'_c$ such that $\ell'_c \leq \ell_c$, then by using induction hypotheses in the premise:

\[ \frac{{(Sderef)}}{{\sigma : S \in \Sigma}}
\]

where $\ell' = \ell$. and the result holds.
Case (Sassoc). Then \( t = o_\ell := v \) and

\[
\begin{array}{c}
o : S \in \Sigma \\
\Gamma; \Sigma, \ell_c \vdash o_\ell : \text{Ref}_\ell S \\
S_2 <: S
d\end{array}
\]

\[
\begin{array}{c}
\Gamma; \Sigma, \ell_c \vdash o_\ell := v : \text{Unit}_{\bot} \\
\end{array}
\]

\[
\begin{array}{c}
\Gamma; \Sigma, \ell_c \vdash o_\ell := v : \text{Unit}_{\bot}
\end{array}
\]

and therefore the result holds.

Case (S:). Then \( t = v :: S \) and

\[
\begin{array}{c}
\Gamma; \Sigma, \ell_c \vdash v : S_1 \\
S_1 <: S \\
\end{array}
\]

\[
\begin{array}{c}
\Gamma; \Sigma, \ell_c \vdash v :: S : S \\
\end{array}
\]

Suppose \( \ell'_c \) such that \( \ell'_c \leq \ell_c \). Considering that \( \ell'_c \vdash \ell \leq \ell_c \land \ell \leq \text{label}(S) \), and \( S'_2 <: S_2 <: S \), then:

\[
\begin{array}{c}
o : S \in \Sigma \\
\Gamma; \Sigma, \ell'_c \vdash o_\ell : \text{Ref}_\ell S \\
S'_2 <: S \\
\end{array}
\]

\[
\begin{array}{c}
\Gamma; \Sigma, \ell'_c \vdash v : S'_2 \\
\ell'_c \vdash \ell \leq \text{label}(S) \\
\end{array}
\]

\[
\begin{array}{c}
\Gamma; \Sigma, \ell'_c \vdash o_\ell := v : \text{Unit}_{\bot}
\end{array}
\]

but

\[
\begin{array}{c}
\text{Unit}_{\bot} <: \text{Unit}_{\bot}
\end{array}
\]

and therefore the result holds.

Lemma B.3 (Substitution). If \( \Gamma; x : S_1; \Sigma, \ell_c \vdash t : S \) and \( \Gamma; \Sigma, \ell_c \vdash v : S'_1 \) such that \( S'_1 <: S_1 \), then \( \Gamma; \Sigma, \ell_c \vdash [v/x]t : S' \) such that \( S' <: S \).

Proof. By induction on the derivation of \( \Gamma; x : S_1; \Sigma, \ell_c \vdash t : S \). □

Lemma B.4. If \( \Gamma; \Sigma, \ell_c \vdash v : S \) then \( \forall \ell'_c, \Gamma; \Sigma, \ell'_c \vdash v : S \).

Proof. By induction on the derivation of \( \Gamma; \Sigma, \ell_c \vdash v : S \) observing that for values, there is no premise that depends on \( \ell_c \). □

Proposition B.5 (\( \rightarrow \) is well defined). If \( \vdash \Sigma, \ell_c \vdash t : S, \vdash \Sigma \vdash \mu \) and \( \forall \ell_r, \) such that \( \ell_r \leq \ell_c \), \( t \mid \mu \rightarrow^{\ell} t' \mid \mu' \) then, for some \( \Sigma' \supseteq \Sigma, \vdash \Sigma'; \ell_c \vdash t' : S' \), where \( S' <: S \) and \( \vdash \Sigma' \vdash \mu' \).

Proof.

Case (S@). Then \( t = b_1_{\ell_1} \oplus b_2_{\ell_2} \) and

\[
\begin{array}{c}
\vdash \Sigma, \ell_c \vdash b_1_{\ell_1} : \text{Bool}_{\ell_1} \\
\vdash \Sigma, \ell_c \vdash b_2_{\ell_2} : \text{Bool}_{\ell_2} \\
\end{array}
\]

\[
\begin{array}{c}
\vdash \Sigma, \ell_c \vdash b_1_{\ell_1} \oplus b_2_{\ell_2} : \text{Bool}_{(\ell_1 \lor \ell_2)}
\end{array}
\]
Suppose $\ell_r$ such that $\ell_r \ll \ell_c$, then

\[
\frac{
\ell_r \quad b_1\ell_1 \oplus b_2\ell_2 \mid \mu \\
}{
(\mathcal{S}_\oplus) 
\ell_c \vdash (b_1 [\oplus] b_2)_{(\ell_1 \lor \ell_2)} : \text{Bool}_{(\ell_1 \lor \ell_2)}
}
\]

Then

\[
\frac{
\ell_r \quad (b_1 [\oplus] b_2)_{(\ell_1 \lor \ell_2)} : \text{Bool}_{(\ell_1 \lor \ell_2)} \\
}{
\mathcal{S}_\oplus 
\ell_c \vdash (b_1 [\oplus] b_2)_{(\ell_1 \lor \ell_2)} : \text{Bool}_{(\ell_1 \lor \ell_2)}
}
\]

Case (Sprot). Then $t = \text{prot}_\ell(v)$ and

\[
\frac{
\vdash; \Sigma; \ell_c \lor \ell \vdash v : S \\
}{
\vdash; \Sigma; \ell_c \vdash \text{prot}_\ell(v) : S \lor \ell
}
\]

Suppose $\ell_r$ such that $\ell_r \ll \ell_c$, then

\[
\text{prot}_\ell(v) \mid \mu \xrightarrow{\ell_r} v \lor \ell \mid \mu
\]

But by Lemma B.2, $\vdash; \Sigma; \ell_c \vdash v : S$.

and the result holds.

Case (Sapp). Then $t = (\lambda^{\ell'}x : S_{11}, t)_{\ell} v$ and

\[
\frac{
D_1 \quad x : S_{11}, \Sigma; \ell_c \vdash t : S_{12} \\
}{
\vdash; \Sigma; \ell_c \vdash \lambda^{\ell'} x : S_{11}, t : S_{12} \quad \ell_c \lor \ell \ll \ell'_c \quad S_2 \ll S_{11}
}
\]

Suppose $\ell_r$ such that $\ell_r \ll \ell_c$, and

\[
\text{true}_\ell \mid \mu \xrightarrow{\ell_r} \text{prot}_\ell([v/x]t) \mid \mu
\]

But as $\ell_c \lor \ell \ll \ell'_c$ then by Lemma B.2, $\vdash; \Sigma; \ell_c \lor \ell \vdash t : S'_{12}$, where $S'_{12} \ll S_{12}$.

By Lemma B.3 and Lemma B.4, $\vdash; \Sigma; \ell_c \lor \ell \vdash [v/x]t : S''_{12}$, where $S''_{12} \ll S'_{12} \ll S_{12}$. Then

\[
\frac{
D'_1 \quad \vdash; \Sigma; \ell_c \lor \ell \vdash [v/x]t : S''_{12} \\
}{
\vdash; \Sigma; \ell_c \lor \ell \vdash \text{prot}_\ell([v/x]t) : S''_{12} \lor \ell
}
\]

Where $S''_{12} \lor \ell \ll S_{12} \lor \ell$ and the result holds.

Case (Sif-true). Then $t = \text{true}_\ell$ then $t_1$ else $t_2$ and

\[
\frac{
\vdash; \Sigma; \ell_c \vdash \text{true}_\ell : \text{Bool}_\ell \\
D_1 \quad \vdash; \Sigma; \ell_c \lor \ell \vdash t_1 : S_1 \\
D_2 \\
\vdash; \Sigma; \ell_c \lor \ell \vdash t_2 : S_2 \\
(\text{Sif}) 
\vdash; \Sigma; \ell_c \lor \ell \vdash \text{true}_\ell \text{ else } t_1 \text{ else } (S_1 \lor S_2) \lor \ell
}
\]

Suppose $\ell_r$ such that $\ell_r \ll \ell_c$, then if

\[
\text{true}_\ell \text{ then } t_1 \text{ else } t_2 \mid \mu \xrightarrow{\ell_r} \text{prot}_\ell(t_1) \mid \mu
\]
Then

Then
\[
D_1 \quad \Rightarrow \quad \vdash \Sigma; \ell_c \land \ell \vdash t_1 : S_1
\]

\[
\vdash \Sigma; \ell_c \vdash \text{prot}_\ell(t_1) : S_1 \land \ell
\]

and by definition of the join operator, \(S_1 \land \ell \prec (S_1 \lor S_2) \land \ell\) and the result holds.

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

**Case (Sref).** Then \(t = \text{ref}^S \, v\) and

\[
(Sref) \quad \vdash \Sigma; \ell_c \vdash v : S' \quad S' \prec S \quad \ell_c \leq \text{label}(S)
\]

Suppose \(\ell_r \leq \ell_c\), then

\[
\text{ref}^S \, v \mid \mu \xrightarrow{\ell_r} o_\perp \mid \mu[o \mapsto v \lor \ell_r]
\]

where \(o \not\in \text{dom}(\mu)\).

Let us take \(\Sigma' = \Sigma, o : S\) and let us call \(\mu' = \mu[o \mapsto v \lor \ell_r]\). Then as \(\text{dom}(\mu) = \text{dom}(\Sigma)\) then \(\text{dom}(\mu') = \text{dom}(\Sigma')\). Also, as \(\ell_r \leq \ell_c \leq \text{label}(S)\) then by Lemma B.4, \(\vdash \Sigma'; \bot \vdash v : S' \land \ell_r\) and \(S' \land \ell_r \prec (\Sigma(o) = S)\). Therefore \(\vdash \Sigma' \vdash \mu'\).

Then

\[
(Si) \quad \vdash o : S \in \Sigma'
\]

and the result holds.

**Case (Sderef).** Then \(t = !o_\ell\) and

\[
(Sderef) \quad \vdash \Sigma; \ell_c \vdash !o_\ell : \text{Ref}_\ell S
\]

Suppose \(\ell_r \leq \ell_c\), then

\[
!o_\ell \mid \mu \xrightarrow{\ell_r} v \lor \ell \mid \mu \quad \text{where} \quad \mu(o) = v
\]

Also \(\vdash \Sigma \vdash \mu\) then \(\vdash \Sigma; \bot \vdash \mu(o) : S'\) and \(S' \prec S\). By Lemma B.4, \(\vdash \Sigma; \ell_c \vdash v : S'\)

\[
\vdash \Sigma; \ell_c \vdash v \lor \ell : S' \lor \ell
\]

But \(S' \lor \ell \prec S \lor \ell\) and the result holds.

**Case (Sassgn).** Then \(t = o_\ell := v\) and

\[
\text{Dassgn} \quad \vdash o : S \in \Sigma
\]

\[
\vdash \Sigma; \ell_c \vdash !o_\ell : \text{Ref}_\ell S
\]

\[
\vdash \Sigma; \ell_c \vdash o_\ell := v : \text{Unit}_\perp
\]

Suppose \(\ell_r \leq \ell_c\), then

\[
o_\ell := v \mid \mu \xrightarrow{\ell_r} \text{unit}_\perp \mid \mu[o \mapsto v \lor \ell_r \lor \ell]
\]

Let us call \(\mu' = \mu[o \mapsto v \lor \ell_r \lor \ell]\). Also \(\vdash \Sigma \vdash \mu\) then \(\text{dom}(\mu') = \text{dom}(\Sigma)\), and \(\vdash \Sigma; \ell_c \vdash v : S_2\) where \(S_2 \prec S\). Therefore \(\vdash \Sigma; \ell_c \vdash v \lor \ell : S_2 \lor \ell_r \lor \ell\). But \(\ell_r \lor \ell \leq \ell_c \lor \ell \leq \text{label}(S)\), then \(S_2 \lor \ell_r \lor \ell \prec S\) and therefore \(\vdash \Sigma \vdash \mu'\). Also

\[
(Su) \quad \vdash \Sigma; \ell_c \vdash \text{unit}_\perp : \text{Unit}_\perp
\]
but

\[
\text{Unit}_\perp \ll: \text{Unit}_\perp
\]

and therefore the result holds.

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

\[
\begin{array}{l}
\Rightarrow \Sigma; \ell_c + v :: S_1 \\
\; ; \Sigma; \ell_c + v :: S : S
\end{array}
\]

Suppose \( \ell_r \) such that \( \ell_r \ll \ell_c \), then

\[
v :: S | \mu \quad \ell_r \triangleright v \triangleright \text{label}(S) | \mu
\]

But \( S_1 \ll: S \) then \( S_1 \ll S \) and therefore \( S_1 \ll \text{label}(S) = S \). Therefore:

\[
\Gamma; \Sigma; \ell_c + v \triangleright \text{label}(S) : S
\]

and the result holds.

\[\square\]

**Proposition B.6 (Canonical Forms).** Consider a value \( v \) such that \( :: \Sigma; \ell_c + v :: S \). Then:

1. If \( S = \text{Bool} \ell \) then \( v = b \ell \) for some \( b \).
2. If \( S = \text{Unit} \ell \) then \( v = \text{unit} \ell \).
3. If \( S = \text{S} \cdot \ell' \cdot c \cdot \ell \cdot t \cdot \ell \) then \( v = (\lambda x :: \text{S} \cdot \ell' \cdot c \cdot \ell \cdot t) \) for some \( t \) and \( \ell' \).
4. If \( S = \text{Ref} \ell S \) then \( v = o \ell \) for some location \( o \).

**Proof.** By inspection of the type derivation rules.

\[\square\]

**Proposition 3.1 (Type Safety).** If \( :: \Sigma; \ell_c + t :: S \) then either

- \( t \) is a value \( v \)
- for any store \( \mu \) such that \( \Sigma + \mu \) and any \( \ell' \ll \ell_c \), we have \( t \mid \mu \triangleright t' \mid \mu' \) and \( :: \Sigma' + \ell_c + t' :: S' \)

\( \) for some \( S' \ll: S \), and some \( \Sigma' \supseteq \Sigma \) such that \( \Sigma' + \mu' \).

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

**Case** (Sb, Su, Sλ, Sl). \( t \) is a value.

**Case** (Sprot). Then \( t = \text{prot}_\ell(t) \) and

\[
\begin{array}{l}
\Rightarrow \Sigma; \ell_c \triangleright \ell + t :: S_1 \\
\; ; \Sigma; \ell_c + \text{prot}_\ell(t) :: S_1 \triangleright \ell
\end{array}
\]

By induction hypotheses, one of the following holds:

1. \( t_1 \) is a value. Then by \( \text{(R→)} \) and Canonical Forms (Lemma B.6), \( t \mid \mu \triangleright t' \mid \mu \) and by Prop B.5, \( :: \Sigma; \ell_c + t' :: S' \) where \( S' \ll: S \) and the result holds.
2. Suppose \( \ell_r \) such that \( \ell_r \ll \ell_c \), then

\[
\begin{array}{l}
\Rightarrow t_1 \mid \mu \triangleright t_2 \mid \mu' \\
\; ; \text{prot}_\ell(t_1) \mid \mu \triangleright \text{prot}_\ell(t_2) \mid \mu'
\end{array}
\]

As \( \ell_r \ll \ell_c \) then \( \ell_r \ll \ell \ll \ell_c \triangleright: \ell \). Using induction hypotheses \( :: \Sigma' + \ell_c \triangleright \ell + t_2 :: S'_1 \) where \( S'_1 \ll: S_1 \) and \( :: \Sigma' + \mu' \). Therefore
By induction hypotheses, one of the following holds:

\[ (S\text{app}) \]

Case \((S\otimes)\). Then \(t = t_1 \oplus t_2\) and

\[
\begin{array}{c}
\vdash \Sigma; \ell_c \vdash t_1 : \text{Bool}_{\ell_1} \\
\vdash \Sigma; \ell_c \vdash t_2 : \text{Bool}_{\ell_2}
\end{array}
\]

By induction hypotheses, one of the following holds:

\[ (S\otimes) \]

(1) \(t_1\) is a value. Then by induction on \(t_2\) one of the following holds:

(a) \(t_2\) is a value. Then by Canonical Forms (Lemma B.6)

\[
\begin{array}{c}
t | \mu \xrightarrow{\ell_r} t' | \mu
\end{array}
\]

and by Prop B.5, \(\vdash \Sigma; \ell_c \vdash t' : S'\), where \(S' \prec \prec S\), therefore the result holds.

(b) \(t_2 \mid \mu \xrightarrow{\ell_r} t'_2 \mid \mu'\) for all \(\ell_{r'}\) such that \(\ell_{r'} \ll \ell_c\), in particular we pick \(\ell_{r'} = \ell_r\). Then by induction hypothesis, \(\vdash \Sigma'; \ell_c \vdash t_2 : \text{Bool}_{\ell_2'}\), where \(\text{Bool}_{\ell_2'} < : \text{Bool}_{\ell_2}\) and \(\vdash \Sigma \vdash \mu'\).

Then by \((Sf)\), \(t \mid \mu \xrightarrow{\ell_r} t_1 \oplus t'_2 \mid \mu'\) and:

\[
\begin{array}{c}
\vdash \Sigma; \ell_c \vdash t_1 : \text{Bool}_{\ell_1} \\
\vdash \Sigma; \ell_c \vdash t'_2 : \text{Bool}_{\ell_2'}
\end{array}
\]

\[
\vdash \Sigma; \ell_c \vdash t_1 \oplus t'_2 : \text{Bool}_{(\ell_1 \lor \ell_2')}
\]

but

\[
(S\otimes) \quad (\ell_1 \lor \ell_2') \ll (\ell_1 \lor \ell_2)
\]

and the result holds.

(2) \(t_1 \mid \mu \xrightarrow{\ell_r} t'_1 \mid \mu'\) for all \(\ell_{r'}\) such that \(\ell_{r'} \ll \ell_c\), in particular we pick \(\ell_{r'} = \ell_r\). Then by induction hypotheses, \(\vdash \Sigma'; \ell_c \vdash t_1 : \text{Bool}_{\ell_1'}\) where \(\text{Bool}_{\ell_1'} < : \text{Bool}_{\ell_1}\), and \(\vdash \Sigma \vdash \mu'\).

Then by \((Sf)\), \(t \mid \mu \xrightarrow{\ell_r} t'_1 \oplus t_2 \mid \mu'\) and:

\[
\begin{array}{c}
\vdash \Sigma; \ell_c \vdash t'_1 : \text{Bool}_{\ell_1'} \\
\vdash \Sigma; \ell_c \vdash t_2 : \text{Bool}_{\ell_2}
\end{array}
\]

\[
\vdash \Sigma; \ell_c \vdash t'_1 \oplus t_2 : \text{Bool}_{(\ell_1' \lor \ell_2)}
\]

but

\[
(S\otimes) \quad (\ell_1' \lor \ell_2) \ll (\ell_1 \lor \ell_2)
\]

and the result holds.

Case \((S\text{app})\). Then \(t = t_1 \cdot t_2\), \(S = S_{t_1} \lor \ell\) and

\[
\begin{array}{c}
\vdash \Sigma; \ell_c \vdash t_1 : S_{t_1} \xrightarrow{\ell_c} S_{t_2} \\
\vdash \Sigma; \ell_c \vdash t_2 : S_2
\end{array}
\]

By induction hypotheses, one of the following holds:

(1) \(t_1\) is a value. Then by Canonical Forms (Lemma B.6), and induction on \(t_2\) one of the following holds:
(a) \( t_2 \) is a value. Then by Canonical Forms (Lemma B.6)

\[
\frac{t \mid \mu \xrightarrow{\ell_r} t' \mid \mu}{t \mid \mu \xrightarrow{\ell_r} t' \mid \mu}
\]

and by Prop B.5 \( \vdash \Sigma; \ell_c \vdash t' : S' \), where \( S' <: S \), therefore the result holds.

(b) \( t_2 \mid \mu \xrightarrow{\ell_r} t_2' \mid \mu' \) for all \( \ell_r' \) such that \( \ell_r' \ll \ell_c \), in particular we pick \( \ell_r' = \ell_r \). Then by induction hypothesis, \( \vdash \Sigma'; \ell_c \vdash t_2' : S_2' \), where \( S_2' <: S_2 \) and \( \vdash \Sigma' \vdash \mu' \).

Then by (Sf), \( t \mid \mu \xrightarrow{\ell_r} t_1' t_2' \mid \mu' \). But \( S_2' <: S_2 <: S_{11} \) and then:

\[
\vdash \Sigma; \ell_c \vdash t_1 : S_{11} \xrightarrow{\ell_r} t_{12} ; S_2' <: S_{11} \quad \vdash \Sigma; \ell_c \vdash t_2' : S_2' \quad \ell_c \ll \ell \ll \ell_c'
\]

and the result holds.

(2) \( t_1 \mid \mu \xrightarrow{\ell_r} t_1' \mid \mu' \) for all \( \ell_r' \) such that \( \ell_r' \ll \ell_c \), in particular we pick \( \ell_r' = \ell_r \). Then by induction hypothesis, \( \vdash \Sigma'; \ell_c \vdash t_1' : S_{11} \xrightarrow{\ell_r} t_{12} ; S'_{12} \) where \( S_{11} \xrightarrow{\ell_r} t_{12} ; S'_{12} <: S_{11} \xrightarrow{\ell_r} S_{12} \), and \( \vdash \Sigma' \vdash \mu' \). Then by (Sf), \( t \mid \mu \xrightarrow{\ell_r} t_1' t_2' \mid \mu' \). By definition of subtyping, \( S_2 <: S_{11} <: S_{11}' \), \( \ell_c' \ll \ell' \ll \ell_c \). Therefore \( \ell_c \ll \ell \ll \ell_c \ll \ell_c' \). Then

\[
\vdash \Sigma; \ell_c \vdash t_1' : S_{11} \xrightarrow{\ell_r} t_{12} ; S'_{12} \quad \vdash \Sigma; \ell_c \vdash t_2 : S_2 \quad S_2' <: S_{11} \quad \ell_c \ll \ell' \ll \ell_c'
\]

and the result holds.

Case (Sif). Then \( t = \text{if} \ t_0 \text{ then } t_1 \text{ else } t_2 \) and

\[
\vdash \Sigma; \ell_c \vdash t_0 : \text{Bool}_{\ell_c}
\]

and by Prop B.5, \( \vdash \Sigma; \ell_c \vdash t' : S' \), where \( S' <: S \), therefore the result holds.

(2) \( t_0 \mid \mu \xrightarrow{\ell_r} t_0' \mid \mu' \) for all \( \ell_r' \) such that \( \ell_r' \ll \ell_c \), in particular we pick \( \ell_r' = \ell_r \). Then by induction hypothesis, \( \vdash \Sigma; \ell_c \vdash t_0' : \text{Bool}_{\ell_c} \), where \( \text{Bool}_{\ell_c} <: \text{Bool}_{\ell} \) and \( \vdash \Sigma \vdash \mu' \). Then by (Sf), \( t \mid \mu \xrightarrow{\ell_r} \text{if} \ t_0' \text{ then } t_1 \text{ else } t_2 \mid \mu' \). As \( \ell_c \ll \ell' \ll \ell_c \), by Lemma B.2, \( \vdash \Sigma; \ell_c \ll \ell' \ll t_1 : S_{1}' \) and \( \vdash \Sigma; \ell_c \ll \ell' \ll t_2 : S_{2}' \) where \( S_1' <: S_1 \) and \( S_2' <: S_2 \). Therefore:

\[
\vdash \Sigma; \ell_c \vdash t_0' : \text{Bool}_{\ell_c}
\]

but by definition of join and subtyping \( (S_1' \vee S_2') \ll \ell' <: (S_1 \vee S_2) \ll \ell \) and the result holds.
Case (S::). Then \( t = t_1 :: S_2 \) and

\[
\frac{}{\cdot \vdash \Sigma; \ell_c + t_1 : S_1 \quad S_1 <: S_2}
\]

By induction hypotheses, one of the following holds:

(1) \( t_1 \) is a value. Then

\[
\frac{t \mid \mu \xrightarrow{\ell_r} t' | \mu}{t \mid \mu \xrightarrow{\ell_r} t' | \mu}
\]

and by Prop B.5, \( \cdot \vdash \Sigma; \ell_c + t : S', \) where \( S' <: S \), therefore the result holds.

(2) \( t_1 \mid \mu \xrightarrow{\ell_r} t_1' \mid \mu' \) for all \( \ell_r' \), such that \( \ell_r' \ll \ell_c \), in particular we pick \( \ell_r' = \ell_r \). Then by induction hypothesis, \( \cdot \vdash \Sigma; \ell_c + t_1' : S_1' \), where \( S_1' <: S_1 \) and \( \cdot \vdash \Sigma + \mu' \). Then by (Sf), \( t \mid \mu \xrightarrow{\ell_r} t_1' :: S_2 \mid \mu'. \)

Also, \( S_1' <: S_1 <: S_2 \) and therefore:

\[
\frac{}{\cdot \vdash \Sigma; \ell_c + t_1' : S_1' \quad S_1' <: S_2}
\]

and the result holds.

Case (Sref). Then \( t = \text{ref}^S t \) and

\[
\frac{}{\cdot \vdash \Sigma; \ell_c + t_1 : S_1' \quad S_1' <: S_1 \quad \ell_c \ll \text{label}(S_1)}
\]

By induction hypotheses, one of the following holds:

(1) \( t_1 \) is a value. Then

\[
\frac{t \mid \mu \xrightarrow{\ell_r} t' | \mu}{t \mid \mu \xrightarrow{\ell_r} t' | \mu}
\]

and by Prop B.5, \( \cdot \vdash \Sigma; \ell_c + t : S', \) where \( S' <: S \) and \( \cdot \vdash \Sigma + \mu' \), therefore the result holds.

(2) \( t_1 \mid \mu \xrightarrow{\ell_r} t_1' \mid \mu' \) for all \( \ell_r' \), such that \( \ell_r' \ll \ell_c \), in particular we pick \( \ell_r' = \ell_r \). Then by induction hypothesis, \( \cdot \vdash \Sigma; \ell_c + t_1' : S_1'' \), where \( S_1'' <: S_1 \) and \( \cdot \vdash \Sigma + \mu' \). Then by (Sf), \( t \mid \mu \xrightarrow{\ell_r} \text{ref}^S t_1' \mid \mu' \) and:

\[
\frac{}{\cdot \vdash \Sigma; \ell_c + t_1' : S_1'' \quad S_1'' <: S_1 \quad \ell_c \ll \text{label}(S_1)}
\]

and the result holds.

Case (Sderef). Then \( t = !t_1 \) and

\[
\frac{}{\cdot \vdash \Sigma; \ell_c + t_1 : \text{Ref}_F S_1}
\]

By induction hypotheses, one of the following holds:

(1) \( t_1 \) is a value. Then by Canonical Forms (Lemma B.6)

\[
\frac{t \mid \mu \xrightarrow{\ell_r} t' | \mu}{t \mid \mu \xrightarrow{\ell_r} t' | \mu}
\]

and by Prop B.5, \( \cdot \vdash \Sigma; \ell_c + t : S', \) where \( S' <: S \), therefore the result holds.
(2) \( t_1 | \mu \xrightarrow{\ell_r} t'_1 | \mu' \) for all \( \ell_r' \) such that \( \ell_r' \leq \ell_c \), in particular we pick \( \ell_r' = \ell_r \). Then by induction hypothesis, \( \vdash; \Sigma; \ell_c \vdash t'_1 : \text{Ref}_\ell S_1 \) where \( \text{Ref}_\ell S_1 < : \text{Ref}_\ell S_1 \) and \( \vdash; \Sigma' \vdash \mu' \). Then by (Sf), \( t | \mu \xrightarrow{\ell_r} t' | \mu' \) and:

\[
\frac{\vdash; \Sigma; \ell_c \vdash t'_1 : \text{Ref}_\ell S_1}{\vdash; \Sigma; \ell_c \vdash t'_1 : S_1 \forall \ell'}
\]

but \( S_1 \forall \ell' < : S_1 \forall \ell \) and the result holds.

**Case (Sasgn).** Then \( t = t_1 := t_2 \) and

\[
\frac{\vdash; \Sigma; \ell_c \vdash t_1 : \text{Ref}_\ell S_1 \quad \vdash; \Sigma; \ell_c \vdash t_2 : S_2}{S_2 < : S_1 \quad \ell_c \forall \ell \leq \text{label}(S_1) \quad \vdash; \Sigma; \ell_c \vdash t_1 := t_2 : \text{Unit}_\perp}
\]

By induction hypotheses, one of the following holds:

(a) \( t_2 \) is a value. Then by Canonical Forms (Lemma B.6), and induction on \( t_2 \) one of the following holds:

\[
\frac{t | \mu \xrightarrow{\ell_c} t' | \mu'}{t | \mu \xrightarrow{\ell_c} t' | \mu'}
\]

and by Prop B.5, \( \vdash; \Sigma; \ell_c \vdash t' : S' \), where \( S' < : S \) and \( \vdash; \Sigma' \vdash \mu' \), therefore the result holds.

(b) \( t_2 | \mu \xrightarrow{\ell_r} t_2' | \mu' \) for all \( \ell_r' \) such that \( \ell_r' \leq \ell_c \), in particular we pick \( \ell_r' = \ell_r \). Then by induction hypothesis, \( \vdash; \Sigma' ; \ell_c \vdash S_2' \) where \( S_2' < : S_2 \) and \( \vdash; \Sigma' \vdash \mu' \).

Then by (Sf), \( t | \mu \xrightarrow{\ell_r} t_1 := t_2' | \mu' \). As \( S_2' < : S_2 < : S_1 \), then:

\[
\frac{\vdash; \Sigma; \ell_c \vdash t_1 : \text{Ref}_\ell S_1 \quad \vdash; \Sigma; \ell_c \vdash t_2' : S_2'}{S_2' < : S_1 \quad \ell_c \forall \ell \leq \text{label}(S_1) \quad \vdash; \Sigma; \ell_c \vdash t_1 := t_2' : \text{Unit}_\perp}
\]

and the result holds.

(2) \( t_1 | \mu \xrightarrow{\ell_r} t'_1 | \mu' \) for all \( \ell_r' \) such that \( \ell_r' \leq \ell_c \), in particular we pick \( \ell_r' = \ell_r \). Then by induction hypotheses, \( \vdash; \Sigma' ; \ell_c \vdash t'_1 : \text{Ref}_\ell S_1 \), where \( \text{Ref}_\ell S_1 < : \text{Ref}_\ell S_1 \) and \( \vdash; \Sigma' \vdash \mu' \). Then by (Sf), \( t | \mu \xrightarrow{\ell_r} t_1 := t_2 | \mu' \). As \( \ell' \leq \ell \) then \( \ell_c \forall \ell' \leq \ell_c \forall \ell \leq \text{label}(S_1) \), and therefore:

\[
\frac{\vdash; \Sigma; \ell_c \vdash t'_1 : \text{Ref}_\ell S_1 \quad \vdash; \Sigma; \ell_c \vdash t_2 : S_2}{S_2 < : S_1 \quad \ell_c \forall \ell' \leq \text{label}(S_1) \quad \vdash; \Sigma; \ell_c \vdash t_1 := t_2 : \text{Unit}_\perp}
\]

and the result holds.

\( \square \)

### B.2 SSL\textsubscript{Ref}: Noninterference

In this section we present the proof of noninterference for SSL\textsubscript{Ref}. Section B.3 present some auxiliary definitions and section B.4 present the proof of noninterference.
To define the fundamental property of the step-indexed logical relations we first define how to relate substitutions:

**Definition B.7.** Let \( \rho \) be a substitution, \( \Gamma \) and \( \Sigma \) a type substitutions. We say that substitution \( \rho \) satisfy environment \( \Gamma \) and \( \Sigma \), written \( \rho \models \Gamma; \Sigma \), if and only if \( \text{dom}(\rho) = \Gamma \) and \( \forall x \in \text{dom}(\Gamma), \forall_\ell_c, \Gamma; \Sigma; \ell \vdash \rho(x) : S' \), where \( S' \ll S \).

**Definition B.8 (Related substitutions).** Tuples \( \langle \ell_1, \rho_1, \mu_1 \rangle \) and \( \langle \ell_2, \rho_2, \mu_2 \rangle \) are related on \( k \) steps, notation \( \Gamma; \Sigma \vdash \langle \ell_1, \rho_1, \mu_1 \rangle \approx^k_{\ell_o} \langle \ell_2, \rho_2, \mu_2 \rangle \), if \( \rho_1 \models \Gamma ; \Sigma ; \ell \vdash \mu_1 \approx^k_{\ell_o} \mu_2 \) and

\[
\forall x \in \Gamma . \exists ! \langle \ell_1, \rho_1(x), \mu_1 \rangle \approx^k_{\ell_o} \langle \ell_2, \rho_2(x), \mu_2 \rangle : \Gamma(x)
\]

**B.3 Definitions**

To define the fundamental property of the step-indexed logical relations we first define how to relate substitutions:

**Definition B.7.** Let \( \rho \) be a substitution, \( \Gamma \) and \( \Sigma \) a type substitutions. We say that substitution \( \rho \) satisfy environment \( \Gamma \) and \( \Sigma \), written \( \rho \models \Gamma; \Sigma \), if and only if \( \text{dom}(\rho) = \Gamma \) and \( \forall x \in \text{dom}(\Gamma), \forall_\ell_c, \Gamma; \Sigma; \ell \vdash \rho(x) : S' \), where \( S' \ll S \).

**Definition B.8 (Related substitutions).** Tuples \( \langle \ell_1, \rho_1, \mu_1 \rangle \) and \( \langle \ell_2, \rho_2, \mu_2 \rangle \) are related on \( k \) steps, notation \( \Gamma; \Sigma \vdash \langle \ell_1, \rho_1, \mu_1 \rangle \approx^k_{\ell_o} \langle \ell_2, \rho_2, \mu_2 \rangle \), if \( \rho_1 \models \Gamma ; \Sigma ; \ell \vdash \mu_1 \approx^k_{\ell_o} \mu_2 \) and

\[
\forall x \in \Gamma . \exists ! \langle \ell_1, \rho_1(x), \mu_1 \rangle \approx^k_{\ell_o} \langle \ell_2, \rho_2(x), \mu_2 \rangle : \Gamma(x)
\]

**B.4 Proof of noninterference**

**Lemma B.9 (Substitution preserves typing).** If \( \Gamma; \Sigma; \ell \vdash t : S \) and \( \rho \models \Gamma; \Sigma \) then \( \Gamma; \Sigma; \ell \vdash \rho(t) : S' \) and \( S' \ll S \).

**Proof.** By induction on the derivation of \( \Gamma; \Sigma; \ell \vdash t : S \).

**Lemma B.10.** Consider stores \( \mu_1, \mu_2, \mu'_1, \mu'_2 \) such that \( \mu_1 \rightarrow \mu'_1 \) and substitutions \( \rho_1 \) and \( \rho_2 \), such that \( \Gamma; \Sigma \vdash \langle \ell_1, \rho_1, \mu_1 \rangle \approx^k_{\ell_o} \langle \ell_2, \rho_2, \mu_2 \rangle \), then if \( \forall j \leq k \), if \( \Sigma \subseteq \Sigma' \), \( \Sigma' + \mu_1 \approx^j_{\ell_o} \mu'_2 \) then \( \Gamma; \Sigma' \vdash \langle \ell_1, \rho_1, \mu'_1 \rangle \approx^j_{\ell_o} \langle \ell_2, \rho_2, \mu'_2 \rangle \)
Lemma B.11 (Substitution preserves typing). If $\Gamma; \Sigma; \ell \vdash t : S$ then $\forall \ell' \leq \ell$, $\Gamma; \Sigma; \ell' \vdash t : S$.

Proof. By induction on the derivation of $\Gamma; \Sigma; \ell \vdash t : S$.

Lemma B.12 (Downward Closed / Monotonicity). If

1. $\Sigma \vdash \langle \ell_1, v_1, \mu_1 \rangle \approx^k_{\ell_o} \langle \ell_2, v_2, \mu_2 \rangle : S$ then
   $\forall j \leq k, \Sigma \vdash \langle \ell_1, v_1, \mu_1 \rangle \approx^j_{\ell_o} \langle \ell_2, v_2, \mu_2 \rangle : S$

2. $\Sigma \vdash \langle \ell_1, t_1, \mu_1 \rangle \approx^k_{\ell_o} \langle \ell_2, t_2, \mu_2 \rangle : C(S)$ then
   $\forall j \leq k, \Sigma \vdash \langle \ell_1, t_1, \mu_1 \rangle \approx^j_{\ell_o} \langle \ell_2, t_2, \mu_2 \rangle : C(S)$

3. $\Sigma \vdash \mu_1 \approx^k_{\ell_o} \mu_2$ then $\forall j \leq k, \Sigma \vdash \mu_1 \approx^j_{\ell_o} \mu_2$

Proof. By induction on type $S$ and the definition of related stores.

Lemma B.13. Consider simple values $v_1 : S_i$ and

$\Sigma \vdash \langle \ell_1, v_1, \mu_1 \rangle \approx^k_{\ell_o} \langle \ell_2, v_2, \mu_2 \rangle : S$.

Then

$\Sigma \vdash \langle \ell_1, (v_1 \lor \ell), \mu_1 \rangle \approx^k_{\ell_o} \langle \ell_2, (v_2 \lor \ell), \mu_2 \rangle : S \lor \ell$

Proof. By induction on type $S$. We proceed by definition of related values and observational-monotonicity of the join, considering that the label stamping can only make values non observable.

Lemma B.14 (Reduction preserves relations). Consider $\Sigma; \ell_1 \vdash t_1 \in T[S], \mu_1 \in \text{STORE}, \Sigma \vdash \mu_1,$

and $\Sigma \vdash \mu \approx^k_{\ell_o} \mu_2$. Consider $j < k$, posing $t_1 \mid \mu_1 \vdash^j_{\ell_o} \mu'_1, \Sigma \subseteq \Sigma', \Sigma' \vdash \mu'_1$ we have

$\Sigma \vdash \langle \ell_1, t_1, \mu_1 \rangle \approx^k_{\ell_o} \langle \ell_2, t_2, \mu_2 \rangle : C(S)$ if and only if $\Sigma' \vdash \langle \ell_1, t'_1, \mu'_1 \rangle \approx^{k-j}_{\ell_o} \langle \ell_2, t'_2, \mu'_2 \rangle : C(S)$

Proof. Direct by definition of

$\Sigma \vdash \langle \ell_1, t_1, \mu_1 \rangle \approx^k_{\ell_o} \langle \ell_2, t_2, \mu_2 \rangle : C(S)$ and transitivity of $\vdash^j_{\ell}$.

Lemma B.15. Consider term $\Sigma; \ell \vdash t : S$, store $\mu$ and $j > 0$,

such that $t \mid \mu \vdash^j_{\ell} t' \mid \mu'$. Then $\mu \rightarrow \mu'$.

Proof. Trivial by induction on the derivation of $t$. The only rules that change the store are the ones for reference and assignment, neither of which remove locations.

Lemma B.16. Suppose that $\Sigma \vdash \langle \ell_1 \lor \ell'_1, t_1, \mu_1 \rangle \approx^k_{\ell_o} \langle \ell_2 \lor \ell'_2, t_2, \mu_2 \rangle : C(S)$, and that $\ell_1 \vdash \text{prot}_{\ell'_1}(t) : $ $S_i' \lor \ell'_i, S_i' \lor \ell'_i : S \lor \ell$ for $i \in \{1, 2\}$. If $\ell_1 \approx^{k}_{\ell_o} \ell_2$, and $\ell'_1 \approx^{k}_{\ell_o} \ell'_2$,

then $\Sigma \vdash \langle \ell_1, \text{prot}_{\ell'}(t_1), \mu_1 \rangle \approx^k_{\ell_o} \langle \ell_2, \text{prot}_{\ell'_2}(t_2), \mu_2 \rangle : C(S \lor \ell)$

Proof. Consider $j < k$, we know by definition of related computations that

$t_1 \mid \mu_1 \vdash^j_{\ell_o} t'_1 \mid \mu'_1$

then $\mu'_1 \approx^k_{\ell_o} \mu'_2$, and by Lemma B.15 $\mu_1 \rightarrow \mu'_1$. If $t'_1$ are reducible after $k - 1$ steps, then the result holds immediately by (Rprot()). The interest case if $t'_1$ are irreducible after $j < k$ steps:
Suppose that after $j$ steps $t'_j = v_i$, then $\Sigma' \vdash (\ell_1 \land \ell'_1, v_i, \mu'_i) \approx^{k_j}_{\ell_o} (\ell_2 \land \ell'_2, v_2, \mu'_2) : S$, for some $\Sigma'$ such that $\Sigma \subseteq \Sigma'$.

Therefore:

$$
\begin{align*}
&\text{Let us suppose } \Sigma'; \ell_i \vdash v_i : S'_i, \text{ where } S'_0 \prec : S'_i \prec : S. \text{ Then } \Sigma'; \ell_i \vdash v_i \land \ell'_i : S'_i \land \ell'_i, \text{ and } S'_j \land \ell'_i \prec : S \land \ell. \\
&\text{If } \neg \text{obs}_{\ell_o}(\ell_i \land \ell'_i) \text{ by monotonicity of the join either } \neg \text{obs}_{\ell_o}(\ell'_i) \text{ or } \neg \text{obs}_{\ell_o}(\ell_i). \text{ If } \neg \text{obs}_{\ell_o}(\ell'_i) \text{ then } \\
&\neg \text{obs}_{\ell_o}(S \land \ell_i) \text{ and the result holds. If } \neg \text{obs}_{\ell_o}(\ell_i) \text{ the result holds immediately. If obs}_{\ell_o}(\ell_i \land \ell'_i, S) \\
&\text{then obs}_{\ell_o}(\ell_i, S \land \ell'_i), \text{ then the result follows by Lemma B.13, and by backward preservation of the relations (Lemma B.14).}
\end{align*}
$$

\[\square\]

Lemma B.17. Consider $\ell$, such that $\neg \text{obs}_{\ell_o}(\ell)$, then then $\forall k > 0$, such that, $\Sigma; \ell \vdash t : S, \Sigma \vdash \mu$

$t | \mu \xrightarrow{\ell} k t' | \mu'$, then $\forall \ell'$,

1. $\forall o \in \text{dom}(\mu') \setminus \text{dom}(\mu), \neg \text{obs}_{\ell_o}(\ell', \mu'(o))$.
2. $\forall o \in \text{dom}(\mu') \cap \text{dom}(\mu) \land \mu'(o) \neq \mu(o), \neg \text{obs}_{\ell_o}(\text{label}(\Sigma(o)))$.

Proof. We use induction on the derivation of $t$. The interest cases are the last step of reduction rules for references and assignments.

Case ($t = o_{\ell''} := v$). We are only updating the heap so we only have to prove (1) and (2). Then

$$
\begin{align*}
o_{\ell''} := v & \quad \xrightarrow{\ell} \text{ unit}_\perp | \mu[o \mapsto (v \lor (\ell \lor \ell''))] \\
\end{align*}
$$

Next we have to prove that obs$_{\ell_o}(\text{label}(\Sigma(o)))$ is not defined. As $\Sigma; \ell \vdash t : S$, then we know that $\ell \land \ell'' \prec : \text{label}(\Sigma(o))$, and as $\neg(\text{obs}_{\ell_o}(\ell))$ by monotonicity of the join the result holds.

Case ($t = \text{ref}^S v$). We are extending the heap, so we need to only prove (1). Then

$$
\begin{align*}
\text{ref}^S \, v & \quad \| \mu \xrightarrow{\ell} o_\perp | \mu[o \mapsto (v \lor \ell)] \\
\end{align*}
$$

where $o \notin \text{dom}(\mu)$. We need to prove that obs$_{\ell_o}(\text{label}(v \lor \ell))$ does not hold, which follows directly by monotonicity of the join.

\[\square\]

Lemma B.18. Consider $\ell$, such that obs$_{\ell_o}(\ell)$ does not hold, then then $\forall k > 0$, such that $\Sigma; \ell \vdash t_1 : S_1$, and that $t_1 \vdash \mu_1 \xrightarrow{\ell} k t'_1 | \mu'_1$, then if $\Sigma \vdash \mu_1 \approx^k_{\ell_o} \mu_2$, then $\Sigma' \vdash \mu'_1 \approx^k_{\ell_o} \mu'_2$ for some $\Sigma'$ such that $\Sigma \subseteq \Sigma'$ and that $\Sigma'; \ell \vdash t'_1 : S'_1$, where $S'_0 \prec : S_1$.

Proof. By Lemma B.17 we know three things:

1. $\forall o \in \text{dom}(\mu'_1) \setminus \text{dom}(\mu_1), \text{obs}_{\ell_o}(\ell, \mu'(o))$ does not hold, i.e. new locations are not observable and therefore as $\Sigma'; \ell \vdash \mu'_1(o) : S$ and $S \prec : \Sigma'(o)$, then $\neg \text{obs}_{\ell_o}(\text{label}(\Sigma(o)))$.
2. $\forall o \in \text{dom}(\mu'_1) \cap \text{dom}(\mu_1) \land \mu'_1(o) \neq \mu(o), \neg \text{obs}_{\ell_o}(\text{label}(\Sigma(o)))$
   
   i.e. for all updated references they have to be previously not observable, and by definition therefore related, and second they are still non observable after the update, and by definition those locations are still related under $\ell$ because $\Sigma(o) = \Sigma'(o)$.

Therefore $\Sigma' \vdash \mu'_1 \approx^k_{\ell_o} \mu'_2$ and the result holds.

\[\square\]
Lemma B.19. Suppose that $\Sigma; \ell_1 \vdash \text{prot}_{\ell_1'}(t_1): S' \vee \ell_1', S' \vee \ell_1' <: S$ for $i \in \{1, 2\}$, where $\neg \text{obs}_{\ell_\rho}(\ell_1 \vee \ell_i')$. Moreover, consider two stores $\mu_1$ such that $\Sigma \vdash \mu_1 \equiv_{\ell_\rho} \mu_2$.

Then $\Sigma \vdash \langle \ell_1, \text{prot}_{\ell_1'}(t_1), \mu_1 \rangle \approx_{\ell_\rho}^k \langle \ell_2, \text{prot}_{\ell_2'}(t_2), \mu_2 \rangle : C(S)$

Proof. Suppose that after at least $j$ more steps, where $j < k$, both subterms reduce to a value:

$$t \parallel \mu_i \xrightarrow{\ell_1 \vee \ell_i'} j \quad v_i \parallel \mu_i'$$

Therefore:

$$\text{prot}_{\ell_1'}(t) \parallel \mu_i'$$

$$\xrightarrow{\ell_1} j \quad \text{prot}_{\ell_1'}(v_i) \parallel \mu_i'$$

$$\xrightarrow{\ell_i} 1 \quad (v_i \vee \ell_i') \parallel \mu_i'$$

As the values can be radically different we have to make sure that both values are not observables. If $\neg \text{obs}_{\ell_\rho}(\ell_i)$ then the values are not observables because the security context is not observable. Let us assume that $\text{obs}_{\ell_\rho}(\ell_i)$ holds, but $\neg \text{obs}_{\ell_\rho}(\ell_i')$ not. Then by monotonicity of the join, $\neg \text{obs}_{\ell_\rho}(\text{label}(v_i) \vee \ell_i')$ and the result follows.

Now we have to prove that the resulting stores are related, for some $\Sigma'$ such that $\Sigma \subseteq \Sigma'$. But by Lemma B.18 the result follows immediately.

\[\Box\]

Next, we present the Noninterference proposition.

Proposition A.5 (Security Type Soundness). If $\Gamma; \Sigma; \ell_{\xi} \vdash t : S_1' \implies \forall S, S_2' <: S, \Gamma; \Sigma; \ell_{\xi} \parallel t : S$

Proof. We proceed by proving a more general proposition instead:

If $\Gamma; \Sigma; \ell_1 \vdash t : S_1', S_2' <: S$, then $\forall \mu_1 \in \text{STORE}, \Sigma \vdash \mu_1$, and $\forall \rho_1 \in \text{SUBST}, \Gamma; \Sigma \vdash \langle \ell_1, \rho_1, \mu_1 \rangle \approx_{\ell_\rho}^k \langle \ell_2, \rho_2, \mu_2 \rangle$, we have $\Sigma \vdash \langle \ell_1, \rho_1(t), \mu_1 \rangle \approx_{\ell_\rho}^k \langle \ell_2, \rho_2(t), \mu_2 \rangle : C(S)$.

By induction on the derivation of term $t$. Let us take an arbitrary index $k \geq 0$.

Case (x). $t = x$ and $\Gamma(x) = S$. $\Gamma; \Sigma \vdash \langle \ell_1, \rho_1, \mu_1 \rangle \approx_{\ell_\rho}^k \langle \ell_2, \rho_2, \mu_2 \rangle$ implies by definition that $\Sigma \vdash \langle \ell_1, \rho_1(x), \mu_1 \rangle \approx_{\ell_\rho}^k \langle \ell_2, \rho_2(x), \mu_2 \rangle : S$, and the result holds immediately.

Case (b). $t = b_y$. By definition of substitution, $\rho_1(b_y) = \rho_2(b_y) = b_y$. By definition, $\Sigma \vdash \langle \ell_1, b_y, \mu_1 \rangle \approx_{\ell_\rho}^k \langle \ell_2, b_y, \mu_2 \rangle : \text{BOOL}_y$ as required.

Case (o). $t = o_{y_1}$ and $\Sigma(o) = S$, where $S = \text{Ref}_{y_1} S_1$. By definition of substitution, $\rho_1(o_{y_1}) = \rho_2(o_{y_1}) = o_{y_1}$. We know that $\Sigma; \ell_1 \vdash o_{y_1} : \text{Ref}_{y_1} S_1$. By definition of related stores, $\Sigma \vdash \langle \ell_1, o_{y_1}, \mu_1 \rangle \approx_{\ell_\rho}^k \langle \ell_2, o_{y_1}, \mu_2 \rangle : \text{Ref}_{y_1} S_1$ as required, and the result holds.

Case (\lambda). $t = (\lambda^x \ell_{\xi} x : S_1', t_1)$. Then $S_1' = \ell_\rho \xrightarrow{\ell_1} S_1''$, and $S = S_1 \xrightarrow{\ell_\rho} S_2$, where $S' <: S$.

By definition of substitution, assuming $x \notin \text{dom}(\rho_1)$, and Lemma B.9:

$$\Gamma; \Sigma; \ell_1 \vdash \rho_1(t) = \Gamma; \Sigma; \ell_1 \vdash (\lambda^x \ell_{\xi} x : S_1', \rho_1(t_1)) \vdash S_1' \xrightarrow{\ell_\rho} \ell_{\xi} S_2$$

where $S_1'' <: S_2$. Consider $j \leq k$, $u_1, u_2$ such that $\mu_1 \rightarrow u_1'$ and $\Sigma \subseteq \Sigma' \Sigma' \vdash u_1' \approx_{\ell_\rho}^l u_2'$, and assume two values $v_1$ and $v_2$ such that $\Sigma' \vdash \langle \ell_1, v_1, \mu_1 \rangle \approx_{\ell_\rho}^l \langle \ell_2, v_2, \mu_2 \rangle : S_1$.
We need to show that:

\[ \Sigma' \vdash \langle \ell_1, (\lambda^\ell_{x} x : S'_1, \rho_1(t_1))_{\ell'} \mid v_1, \mu'_1 \rangle \]

\[ \approx_{\ell_o}^j \langle \ell_2, (\lambda^\ell_{x} x : S'_1, \rho_2(t_2))_{\ell'} \mid v_2, \mu'_2 \rangle \quad : C(S_2) \]

Then:

\[ (\lambda^\ell_{x} x : S'_1, \rho_1(t_1))_{\ell'} \mid v_1 \mid \mu'_1 \]

\[ \stackrel{\ell_o}{\longrightarrow} \text{prot}_{\ell'}([v_1/x]\rho_1(t_1)) \mid \mu'_1 \]

We then extend the substitutions to map \( x \) to the arguments:

\[ \rho'_i = \rho_i \{ x \mapsto v_i \} \]

We know that \( \Sigma' \vdash \langle \ell_1, v_1, \mu'_1 \rangle \approx_{\ell_o}^j \langle \ell_2, v_2, \mu'_2 \rangle : S_1 \). So as \( \mu_i \rightarrow \mu'_i \) then by Lemma B.10, \( \Gamma, x : S_1; \Sigma' \vdash \langle \ell_1, \rho'_i(t_1), \mu'_1 \rangle \approx_{\ell_o}^j \langle \ell_2, \rho'_2(t_2), \mu'_2 \rangle \).

By Lemma B.9, \( \Gamma; \Sigma', \ell'_i \vdash \rho_i(t_1) : S'_1 \) where \( S'_1 \ll S_1 \ll S_2 \). We know that \( \ell_i \ll \ell'_i \ll \ell''_i \), therefore by Lemma B.2, \( \Gamma; \Sigma', \ell_i \ll \ell \vdash \rho_i(t_1) : S'_1 \). Then by induction hypothesis and Lemma B.12:

\[ \Sigma' \vdash \langle \ell_1 \ll \ell', \rho'_1(t_1), \mu'_1 \rangle \approx_{\ell_o}^{j-1} \langle \ell_2 \ll \ell', \rho'_2(t_2), \mu'_2 \rangle : C(S_2) \]

Finally, by Lemma B.16:

\[ \Sigma' \vdash \langle \ell_1, \text{prot}_{\ell'}(\rho'_1(t_1)), \mu'_1 \rangle \]

\[ \approx_{\ell_o}^j \langle \ell_2, \text{prot}_{\ell'}(\rho'_2(t_2)), \mu'_2 \rangle : C(S_2) \]

and finally the result holds by backward preservation of the relations (Lemma B.14).

---

**Case (!).** \( t = !t' \), where \( \Sigma; \ell_i \vdash !t' : \text{Ref}_{\ell''_i} S_1 \), where \( S_1 \ll \ell''_i \ll S = S_1 \ll \ell \).

By definition of substitution:

\[ \rho_i(t) = !\rho_i(t') \]

We have to show that

\[ \Sigma \vdash \langle \ell_1, !\rho_i(t'), \mu_1 \rangle \]

\[ \approx_{\ell_o}^k \langle \ell_2, \rho_i(t'), \mu_2 \rangle : C(S) \]

By Lemma B.9:

\[ \Sigma; \ell_i \vdash !\rho_i(t') : S_1 \ll \ell''_i \]

where \( \ell''_i \ll \ell'_i \ll \ell \). By induction hypotheses on the subterm:

\[ \Sigma \vdash \langle \ell_1, \rho_i(t'), \mu_1 \rangle \approx_{\ell_o}^k \langle \ell_2, \rho_i(t'), \mu_2 \rangle : C(\text{Ref}_\ell S_1) \]

Consider \( j \ll k \), then by definition of related computations

\[ \rho_i(t') \mid \mu_i \stackrel{\ell_i}{\longrightarrow} j \mid t'_i \mid \mu'_i \quad \Rightarrow \quad \Sigma \subseteq \Sigma', \Sigma' \vdash \mu'_i \approx_{\ell_o}^{k-j} \mu'_2 \wedge \text{irred}(t'_i) \Rightarrow \Sigma' \vdash \langle \ell_1, t'_i, \mu'_1 \rangle \approx_{\ell_o}^{k-j} \langle \ell_2, t'_2, \mu'_2 \rangle : \text{Ref}_\ell S_1 \]

If terms \( t'_i \) are reducible after \( j = k - 1 \) steps, then

\[ !\rho_i(t) \mid \mu_i \stackrel{\ell_i}{\longrightarrow} j \mid t'_i \mid \mu'_i \] and the result holds.

If after at most \( j \) steps \( t'_i \) is irreducible it means that for some \( j' \leq j \), \( !\rho_i(t) \mid \mu_i \stackrel{\ell_i}{\longrightarrow} j' \mid v_i \mid \mu'_i \). If \( j' = j \) then we use the same same argument for reducible terms and the result holds.
Let us consider now \( j' < j \). Then \( \Sigma' \vdash \langle \ell_1, v_1, \mu'_1 \rangle \approx_{k-j'} \langle \ell_2, v_2, \mu'_2 \rangle : \text{Ref}_\ell S_1 \). By Lemma B.6, each \( v_i \) is a location \( o_{i \ell'_i} \), such that \( \Sigma'(o_{i \ell'_i}) = \text{Ref}_{\ell'_i} S_1 \) and \( \ell'_i \leq \ell' \). Then:

\[
\rho_i(t) \mapsto_{\ell_i} \mu_i \mapsto_{\ell'_i} j' + 1 \text{Prot}_{\ell'_i}(v'_i) \mapsto_{\ell'_i} 1 \text{Prot}_{\ell'_i}(v') \mapsto_{\ell'_i} \mu'_i
\]

with \( \ell'_i < \ell''_i \), \( v'_i = \mu'_i(o_{i \ell'_i}) \). As \( \Sigma' \vdash \langle \ell_1, v_1, \mu'_1 \rangle \approx_{k-j} \langle \ell_2, v_2, \mu'_2 \rangle : \text{Ref}_\ell S_1 \), then by By monotonicity of the join either both \( \text{obs}_{\ell_o}(\ell'_1) \) or \( \neg \text{obs}_{\ell_o}(\ell'_1) \). Finally as \( \Sigma' \vdash \langle \ell_1, v_1, \mu_1 \rangle \approx_{k-j'} \langle \ell_2, v_2, \mu_2 \rangle : S_1 \), by Lemma E.60,

\[
\Sigma' \vdash \langle \ell_1, \text{Prot}_{\ell_1}(v'_i), \mu'_i \rangle \approx_{\ell_o} \langle \ell_2, \text{Prot}_{\ell_2}(v'_2), \mu_2 \rangle : C(S_1 \lor \ell)
\]

and finally the result holds by backward preservation of the relations (Lemma B.14).

---

**Case (\( = \)).** \( t = t_1 := t_2 \). Then \( S = \text{Unit}_\bot \).

By definition of substitution:

\[
\rho_i(t) = \rho_i(t_1) := \rho_i(t_2)
\]

and Lemma B.9:

\[
\Sigma; \ell_i \vdash \rho_i(t_1) := \rho_i(t_2) : \text{Unit}_\bot
\]

We have to show that

\[
\Sigma \vdash \langle \ell_1, \rho_i(t_1) := \rho_i(t_2), \mu_1 \rangle \approx_{\ell_o} \langle \ell_2, \rho_2(t_1) := \rho_2(t_2), \mu_2 \rangle : C(S)
\]

By induction hypotheses

\[
\Sigma \vdash \langle \ell_1, \rho_i(t_1), \mu_1 \rangle \approx_{\ell_o} \langle \ell_2, \rho_2(t_1), \mu_2 \rangle : C(S_1)
\]

Suppose \( j_1 < k \), and that \( \rho_i(t_1) \) are irreducible after \( j_1 \) steps (otherwise, similar to case !, the result holds immediately). Then by definition of related computations:

\[
\rho_i(t_1) \mid \mu_i \mapsto_{\ell_1} j'_1 v_i \mid \mu'_i \implies \Sigma \subseteq \Sigma', \Sigma' \vdash \mu'_1 \approx_{\ell_o} k-j_1 \mu'_2 \land \Sigma' \vdash \langle \ell_1, v_1, \mu'_1 \rangle \approx_{\ell_o} k-j_1 \langle \ell_2, v_2, \mu'_2 \rangle : \text{Ref}_\ell S_1
\]

By Lemma B.15 \( \mu_i \rightarrow \mu'_i \), and \( \mu'_1 \approx_{\ell_o} k-j_1 \mu'_2 \) then by Lemma E.41, \( \Sigma' \vdash \langle \ell_1, \rho_i(1), \mu'_1 \rangle \approx_{\ell_o} k-j_1 \langle \ell_2, \rho_2(1), \mu'_2 \rangle \).

By induction hypotheses:

\[
\Sigma' \vdash \langle \ell_1, \rho_i(1), \mu'_1 \rangle \approx_{\ell_o} \langle \ell_2, \rho_2(1), \mu'_2 \rangle : C(S_2)
\]

Again, consider \( j_2 = k - j_1 \), if after \( j_2 \) steps \( \rho_i(t_2) \) is reducible or is a value, the result holds immediately. The interest case if after \( j'_2 < j_2 \) steps \( \rho_i(t_{S_2}) \) reduces to values \( v'_2 \):

\[
\rho_i(t_{S_2}) \mid \mu'_1 \mapsto_{\ell_2} j'_2 v'_1 \mid \mu''_1 \implies \Sigma' \subseteq \Sigma'', \Sigma'' \vdash \mu''_1 \approx_{\ell_o} k-j_1-j'_2 \mu''_2 \land \Sigma'' \vdash \langle \ell_1, v'_1, \mu''_1 \rangle \approx_{\ell_o} k-j_1-j'_2 \langle \ell_2, v'_2, \mu''_2 \rangle : S_2
\]

Now consider \( j'_2 + j'_2 \) such that \( v'_2 \), \( \mu''_1 \), \( \mu''_2 \) are irreducible after \( j'_2 \) steps (otherwise, similar to case !, the result holds immediately). Then by definition of substitution:

\[
\rho_i(t_{S_2}) \mid \mu_i \mapsto_{\ell_1} j'_1 v_i := v'_1 \mid \mu''_1 \land \Sigma'' \vdash \mu''_1 \approx_{\ell_o} k-j_1-j'_2 \mu''_2
\]

As both values \( v_i \) are related at some reference type, then by canonical forms (Lemma B.6) they both must be locations \( o_{i \ell'_i} \) for some \( S'_i < S_1 \). We consider when the values are observable and the locations are identical (otherwise the result is trivial):

\[
\begin{align*}
\ell_i & \rightarrow 1 \text{ unit}_\bot \mid \mu''_1 \\
\end{align*}
\]
Where $\mu'''' = \mu''[o \mapsto (v'_1 \lor (\ell_1 \lor \ell'_1))]$. As $\Sigma'' \vdash \langle \ell_1, v'_1, \mu'''' \rangle \approx_{\ell_o} \langle \ell_2, v'_2, \mu'''' \rangle : S_2$, and as $\ell_1, \ell'_1 \leq \text{label}(S_1)$, where $\ell'_1 \leq \ell_1$, and label($v'_1$) $\leq \text{label}(S_1)$, then $\Sigma''; \ell_i \vdash v'_1 \lor (\ell_1 \lor \ell'_1) : S'$ and $S'':= S_1$. Then by monotonicity of the join Lemma B.13,

$$\Sigma'' \vdash \langle \ell_1, (v'_1 \lor (\ell_1 \lor \ell'_1)), \mu'''' \rangle \approx_{\ell_o} \langle \ell_2, (v'_2 \lor (\ell_2 \lor \ell'_2)), \mu'''' \rangle$$

But if $\neg \text{obs}_{\ell_o}(\ell_i)$ then by monotonicity of the join $\neg \text{obs}_{\ell_o}(v'_1 \lor (\ell_1 \lor \ell'_1))$. Therefore, $\forall \ell''''$, such that $\ell'''' \approx_{\ell_o} \ell''$, for all steps $j$, by definition of related stores $\mu'''' \approx_{\ell_o} \mu''$. Then, by induction hypotheses:

$$\Sigma \vdash \langle \ell_1, \mu'''' \rangle \approx_{\ell_o} \langle \ell_2, \mu'''' \rangle$$

As every values are related at type Unit, we only have to prove that $\Sigma'' \vdash \mu'''' \approx \mu''''$, but using monotonicity (Lemma E.47), it is trivial to prove that because either both both stores update the same location $o$ to values that are related, therefore the result holds.

---

**Case (ref).** $t = \text{ref}^{S_1} \cdot t''$. Then $S = \text{Ref}_\bot S_1$.

By definition of substitution:

$$\rho_i(t) = \text{ref}^{S_1} \rho_i(t')$$

and Lemma B.9:

$$\ell_i + \text{ref}^{S_1} \rho_i(t') : \text{Ref}_\bot S_1$$

We have to show that

$$\Sigma \vdash \langle \ell_1, \text{ref}^{S_1} \rho_i(t'), \mu \rangle \approx_{\ell_o} \langle \ell_2, \text{ref}^{S_1} \rho_2(t'), \mu \rangle : C(S_1)$$

As $\Sigma; \ell_i \vdash \rho_i(t') : S'_i$ where $S'_i \leq S_1$, by induction hypotheses:

$$\Sigma \vdash \langle \ell_1, \rho_i(t'), \mu \rangle \approx_{\ell_o} \langle \ell_2, \rho_2(t'), \mu \rangle$$

Consider $j < k$, by definition of related computations

$$\rho_i(t') \mid \mu_i \xrightarrow{t'_j} \rho_i(t'') \mid \mu_i' \implies \Sigma \subseteq \Sigma', \Sigma' \vdash \mu_i' \approx_{\ell_o} \mu_2' \land (\text{irred}(t''_j) \implies \Sigma' \vdash \langle \ell_1, t'_j, \mu_i' \rangle \approx_{\ell_o} \langle \ell_2, t'_j, \mu_2' \rangle : S'_1)$$

If terms $t'_i$ are reducible after $j = k - 1$ steps, then

$$\text{ref}^{S_1} \rho_i(t') \mid \mu_i \xrightarrow{t'_j} \text{ref}^{S_1} t'_j \mid \mu_i'$$

and the result holds.

If after at most $j$ steps $t'_j$ is irreducible, it means that for some $j' \leq j$ \text{ref}^{S_1} \rho_i(t') \mid \mu_i \xrightarrow{t'_j} j' \text{ref}^{S_1} v_i \mid \mu_i'$. If $j' = j$ then we use the same same argument for reducible terms and the result holds.

Let us consider now $j' < j$. Then:

$$\rho_i(t) \mid \mu \xrightarrow{t'_j, j' + 1} \text{ref}_S^{S_1} v_i \mid \mu_i'$$

with, $\mu'''' = \mu''[o \mapsto (v'_1 \lor (\ell_1 \lor \ell'_1))]$. Also, as $\Sigma' \vdash \langle \ell_1, v_1, \mu_i' \rangle \approx_{\ell_o} \langle \ell_2, v_2, \mu_2' \rangle : S_1$, then $\Sigma'' \vdash \langle \ell_1, v_1, \mu'''' \rangle \approx_{\ell_o} \langle \ell_2, v_2, \mu_2'''' \rangle : S_1$, with $\Sigma'' = \Sigma', o : S_1$. And as $\text{label}(v_i) \lor \ell_1 \leq \text{label}(S_1)$, then by Lemma B.13,

$$\Sigma'' \vdash \langle \ell_1, v_1 \lor \ell_1, \mu_i' \rangle \approx_{\ell_o} \langle \ell_2, v_2 \lor \ell_2, \mu_2' \rangle : S_1.$$
Case ($\oplus$). $t = t_1 \oplus t_2$

By definition of substitution:
$$\rho_i(t) = \rho_i(t_1) \oplus \rho_i(t_2)$$

and Lemma B.9:
$$\Sigma; \ell_i \vdash \rho_i(t_1) \oplus \rho_i(t_2) : S''$$

with $S''_1 < S''_1 < S$. We use a similar argument to case := for reducible terms. The interest case is when we suppose some $j_1$ and $j_2$ such that $j_1 + j_2 < k - 3$ where:

$$\rho_i(t_1) \mid \mu_i \xrightarrow{\ell_i} b_{v_{i1}} \mid \mu''_i \implies \Sigma \subseteq \Sigma', \Sigma' \vdash \mu'_1 \approx_{\ell_o}^{k-j_i} \mu'_2 \land \Sigma' \vdash \langle \ell_1, v_{i1}, \mu'_1 \rangle \approx_{\ell_o}^{k-j_i} \langle \ell_2, v_{i1}, \mu'_2 \rangle : S_1$$

$$\rho_i(t_2) \mid \mu'_1 \xrightarrow{\ell_1} b_{v_{i2}} \mid \mu''_1 \implies \Sigma' \subseteq \Sigma'', \Sigma'' \vdash \mu''_1 \approx_{\ell_o}^{k-j_i} \mu''_2 \land \Sigma'' \vdash \langle \ell_1, v_{i2}, \mu''_1 \rangle \approx_{\ell_o}^{k-j_i} \langle \ell_2, v_{i2}, \mu''_2 \rangle : S_2$$

By Lemma B.6, each $v_{ij}$ is a boolean $(b_{ij})_{ij}$ then:

$$\rho_i(t) \mid \mu''_1 \xrightarrow{\ell_1} b_{v_{ij}} \mid \mu''_1$$

with $b_i = b_{i1} \oplus b_{i2}$, $\ell_i = \ell_{i1} \lor \ell_{i2}$, and $\ell_i' \preceq \text{label}(S''_i') \preceq \text{label}(S)$. It remains to show that:

$$\Sigma'' \vdash \langle \ell_1, (b_1)_{ij} \rangle, \langle \ell_2, (b_2)_{ij} \rangle : S$$

If $\neg \text{obs}_{\ell_o}(\ell_i)$, then the result is trivial because the resulting booleans are also related as they are not observable.

If $\text{obs}_{\ell_o}(\ell_i')$, and $\neg \text{obs}_{\ell_o}(\ell_i'')$ or $\neg \text{obs}_{\ell_o}(\ell_i''')$, then by monotonicity of the join, $\neg \text{obs}_{\ell_o}(\ell_i')$ and the result holds. If $\text{obs}_{\ell_o}(\ell_i')$ then $\text{obs}_{\ell_o}(\ell_i'')$ and therefore $b_{i1} = b_{21}$ and $b_{i2} = b_{22}$, so $b_1 = b_2$, and the result holds.

Case (app). $t = t_1 t_2$, with $\Sigma; \ell_i \vdash t_1 : S_{11} \xrightarrow{\ell_{ei}} \ell_i S_{12}$, and $\Sigma; \ell_i \vdash t_2 : S''_{11}$. Also $S_{11} \xrightarrow{\ell_{ei}} \ell_i S_{12} < S_{11} \xrightarrow{\ell_e} \ell S_2$, and $S = S_2$.

By definition of substitution:
$$\rho_i(t) = \rho_i(t_1) \rho_i(t_2)$$

and Lemma B.9:
$$\Sigma; \ell_i \vdash \rho_i(t_1) \rho_i(t_2) : S''_{12}$$

with $S''_{12} < S_{12} < S_2$. We use a similar argument to case := for reducible terms. The interest case is when we suppose some $j_1$ and $j_2$ such that $j_1 + j_2 < k$ where by induction hypotheses and the definition of related computations:

$$\rho_i(t_1) \mid \mu_i \xrightarrow{\ell_i} b_{v_{i1}} \mid \mu''_i \implies \Sigma \subseteq \Sigma', \Sigma' \vdash \mu'_1 \approx_{\ell_o}^{k-j_i} \mu'_2 \land \Sigma' \vdash \langle \ell_1, v_{i1}, \mu'_1 \rangle \approx_{\ell_o}^{k-j_i} \langle \ell_2, v_{i1}, \mu'_2 \rangle : S_1$$

$$\rho_i(t_2) \mid \mu'_1 \xrightarrow{\ell_1} b_{v_{i2}} \mid \mu''_1 \implies \Sigma' \subseteq \Sigma'', \Sigma'' \vdash \mu''_1 \approx_{\ell_o}^{k-j_i} \mu''_2 \land \Sigma'' \vdash \langle \ell_1, v_{i2}, \mu''_1 \rangle \approx_{\ell_o}^{k-j_i} \langle \ell_2, v_{i2}, \mu''_2 \rangle : S_2$$

Then
$$\rho_i(t) \mid \mu_i \xrightarrow{\ell_i} b_{v_{i1}} v_{i2} \mid \mu''_i$$
If \( \text{obs}_{\ell_o}(\ell_i, v_{11}) \) then, by definition of \( \approx_{\ell_o} \) at values of function type, we have:

\[
\Sigma' \vdash_x \langle \ell_i, (v_{11}, v_{12}), \mu_i' \rangle
\]

\[
\approx^{k-j_i-j_h}_{\ell_o} \langle \ell_2, (v_{21}, v_{22}), \mu_2' \rangle : C(S_2 \land \ell)
\]

Finally, by backward preservation of the relations (Lemma B.14) the result holds.

If \( \neg\text{obs}_{\ell_o}(\ell_i, v_{11}) \), and we assume by canonical forms that \( v_{11} = (\lambda t_i.x.t_i)_{\ell_i'} \) then, either \( \neg\text{obs}_{\ell_o}(\ell_i) \) or \( \neg\text{obs}_{\ell_o}(\ell_i') \) and

\[
\approx^{k-j_i-j_h}_{\ell_o} \langle \ell_2, \text{prot}_{\ell_i'}(t_2), \mu_2' \rangle : C(S_2 \land \ell)
\]

If either \( \neg\text{obs}_{\ell_o}(\ell_i) \) or \( \neg\text{obs}_{\ell_o}(\ell_i') \) then by Lemma B.19,

\[
\Sigma'' \vdash_x \langle \ell_i, \text{prot}_{\ell_i'}(t_i), \mu_i'' \rangle
\]

\[
\approx^{k-j_i-j_h}_{\ell_o} \langle \ell_2, \text{prot}_{\ell_i'}(t_2), \mu_2'' \rangle : C(S_2 \land \ell)
\]

Finally, by backward preservation of the relations (Lemma B.14) the result holds.

---

**Case (if)**. \( t = t_1 \) then \( t_2 \) else \( t_3 \), with \( \Sigma; \ell_i + t_1 : S_1; \Sigma; \ell_i' + t_2 : S_2; \Sigma; \ell_i + t_3 : S_3; \ell_i = \ell_i \lor \text{label}(S_1) \), and \( S' = S_2 \lor S_3 : < S \)

By definition of substitution:

\[
\rho_i(t) = \text{if } \rho_i(t_1) \text{ then } \rho_i(t_2) \text{ else } \rho_i(t_3)
\]

We use a similar argument to case := for reducible terms. The interest case is when we suppose some \( j_1 \) and \( j_2 \) such that \( j_1 + j_2 < k \) where by induction hypotheses and related computations we have that:

\[
\rho_i(t_1) \mid \mu_i \vdash_{\ell_i} j_i v_{11} \mid \mu_i' \Longrightarrow \Sigma \subseteq \Sigma', \Sigma' \vdash \mu_i' \approx_{\ell_o}^{k-j_i-j_h} \mu_2' \land \Sigma' \vdash \langle \ell_i, v_{11}, \mu_i' \rangle \approx_{\ell_o}^{k-j_i-j_h} \langle \ell_2, v_{21}, \mu_2' \rangle : S_1
\]

By Lemma B.6, each \( v_{11} \) is a boolean \( (b_{11})_{\ell_{11}} \), such that \( \Sigma' ; \ell_i \vdash (b_{11})_{\ell_{11}} : \text{Bool}_{\ell_{11}} \) and \( \text{Bool}_{\ell_{11}} : < S_1 \), implies \( S_1 = \text{Bool}_{\ell_i} \).

Then:

\[
\rho_i(t) \mid \mu_i \vdash_{\ell_i} j_{i+1} (b_{11})_{\ell_{11}} \text{ if } (b_{11})_{\ell_{11}} \text{ then } \rho_i(t_2) \text{ else } \rho_i(t_3) \mid \mu_i'
\]

Let us consider \( \neg\text{obs}_{\ell_o}(\ell_i, (b_{11})_{\ell_{11}}) \). Let us assume the worst case scenario and that both execution reduce via different branches of the conditional. Then

\[
\rho_i(t) \mid \mu_i \vdash_{\ell_i} j_{i+2} \text{prot}_{\ell_{11}}(\rho_i(t_2)) \mid \mu_i'
\]

\[
\rho_i(t) \mid \mu_i \vdash_{\ell_i} j_{i+2} \text{prot}_{\ell_{21}}(\rho_i(t_3)) \mid \mu_i'
\]

But because \( \neg\text{obs}_{\ell_o}(\ell_i, (b_{11})_{\ell_{11}}) \), then either \( \neg\text{obs}_{\ell_o}(\ell_i) \) or \( \neg\text{obs}_{\ell_o}(\ell_i') \) and therefore, \( \neg\text{obs}_{\ell_o}(\ell_i \lor \ell_{11}) \).

Then by Lemma B.19,

\[
\Sigma' \vdash \langle \ell_i, \text{prot}_{\ell_{11}}(\rho_i(t_2)), \mu_i' \rangle \approx_{\ell_o}^{k} \langle \ell_2, \text{prot}_{\ell_{21}}(\rho_i(t_3)), \mu_2' \rangle
\]

and the result holds by backward preservation of the relations (Lemma B.14).

Now let us consider if \( \text{obs}_{\ell_o}(\ell_i, (b_{11})_{\ell_{11}}) \) holds. Then by definition of \( \approx_{\ell_o} \) on boolean values, \( b_{11} = b_{21} \). Because \( b_{11} = b_{21} \), both \( \rho_i(t) \) and \( \rho_i(t) \) step into the same branch of the conditional. Let us assume the condition is true (the other case is similar):
Then by induction hypothesis $\Sigma' \vdash \langle \ell_1 \gamma \ell_1, \rho_1(t_2), \mu'_1 \rangle \approx_{\ell_1} \langle \ell_2 \gamma \ell_2, \rho_2(t_2), \mu'_2 \rangle : S_2$, and by Lemma B.16,

$$\Sigma' \vdash \langle \ell_1, \text{prot}_{\ell_1}(\rho_1(t_2)), \mu'_1 \rangle \approx^k_{\ell_1} \langle \ell_2, \text{prot}_{\ell_2}(\rho_2(t_2)), \mu'_2 \rangle : S$$

and the result holds by backward preservation of the relations (Lemma B.14).

Case (prot()). Direct by using Lemma B.16.

\[\square\]

**C GRADUALIZING THE STATIC SEMANTICS**

In section C.1, we show the proof of optimality and soundness of the abstraction. In section C.2, we present the proof for the Static Gradual Guarantee.

**C.1 From Gradual Labels to Gradual Types**

**Proposition C.1 (α is Sound).** If $\hat{\ell} \neq \emptyset$ then $\hat{\ell} \subseteq \gamma(\alpha(\hat{\ell}))$.

**Proof.** By case analysis on the structure of $\hat{\ell}$. If $\hat{\ell} = \{ \ell \}$ then $\gamma(\alpha(\{ \ell \})) = \gamma(\ell) = \{ \ell \} = \hat{\ell}$, otherwise $\gamma(\alpha(\ell)) = \gamma(\text{LABEL}) \supseteq \hat{\ell}$.

**Proposition C.2 (α is Optimal).** If $\hat{\ell} \subseteq \gamma(g)$ then $\alpha(\hat{\ell}) \subseteq g$.

**Proof.** By case analysis on the structure of $g$. If $g = \ell$, $\gamma(\ell) = \{ \ell \}$, $\hat{\ell} \subseteq \{ \ell \}$, $\hat{\ell} \neq \emptyset$ implies $\alpha(\hat{\ell}) = \alpha(\{ \ell \}) = \ell \subseteq g$ (if $\hat{\ell} = \emptyset$, $\alpha(\hat{\ell})$ is undefined). If $g = \text{?}$, $g' \subseteq g$ for all $g'$.

**Proposition 6.4 (α is Sound and Optimal).** If $\hat{\ell} \neq \emptyset$ then,

(i) $\hat{\ell} \subseteq \gamma(\alpha(\hat{\ell}))$.

(ii) If $\hat{\ell} \subseteq \gamma(g)$ then $\alpha(\hat{\ell}) \subseteq g$.

**Proof.** Trivial using Prop C.1 and C.2.

**Proposition C.3 (α_S is Sound).** If $\hat{S}$ valid, then $\hat{S} \subseteq \gamma_S(\alpha_S(\hat{S}))$.

**Proof.** By well-founded induction on $\hat{S}$ according to the ordering relation $\hat{S} \sqsubseteq \hat{S}$ defined as follows:

$$\hat{\text{dom}}(\hat{S}) \sqsubseteq \hat{S}$$

$$\hat{\text{cod}}(j\hat{S}) \sqsubseteq \hat{S}$$

Where $\hat{\text{dom}}, \hat{\text{cod}} : \mathcal{P}(\text{GType}) \rightarrow \mathcal{P}(\text{GType})$ are the collecting liftings of the domain and codomain functions $\text{dom}, \text{cod}$ respectively, e.g.,

$$\hat{\text{dom}}(\hat{S}) = \{ \text{dom}(S) \mid S \in \hat{S} \}.$$  

We then consider cases on $\hat{S}$ according to the definition of $\alpha_S$.

Case (\{ Bool_\ell_i \}).

$$\gamma_S(\alpha_S(\{ \text{Bool}_\ell_i \})) = \gamma_S(\text{Bool}_\ell_{\alpha(\{ \ell \})})$$

$$\supseteq \{ \text{Bool}_\ell \mid \ell \in \gamma(\alpha(\{ \ell \})) \}$$

by soundness of $\alpha$. 
Case \(\{S_1 \xrightarrow{\ell} S_2\}\).

\[
\gamma_S(\alpha_S(\{S_1 \xrightarrow{\ell} S_2\})) = \gamma_S(\alpha_S(\{S_1 \xrightarrow{\ell} S_2\})) = \gamma_S(\alpha_S(\{S_1 \xrightarrow{\ell} S_2\})) \\
\subseteq \{S_1 \xrightarrow{\ell} S_2\}
\]

by induction hypothesis on \(\{S_1\}\) and \(\{S_2\}\), and soundness of \(\alpha\).

Case \(\{\text{Ref}_\ell S\}\).

\[
\gamma_S(\alpha_S(\{\text{Ref}_\ell S\})) = \gamma_S(\alpha_S(\{S\})) = \{\text{Ref}_\ell S \mid S \in \gamma(\alpha(\{\ell\})), S \in \gamma_S(\{S\})\}
\]

by induction hypothesis on \(\{S\}\) and soundness of \(\alpha\).

\[
\square
\]

**Proposition C.4 (\(\alpha_S\) is optimal).** If \(\hat{S}\) valid and \(\hat{S} \subseteq \gamma_S(U)\) then \(\alpha_S(\hat{S}) \subseteq U\).

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

Case (Bool). \(\gamma_S(\text{Bool}_\ell) = \{\text{Bool}_\ell \mid \ell \in \gamma(g)\}\)

So \(\hat{S} = \{\text{Bool}_\ell \mid \ell \in \ell\}\) for some \(\ell \subseteq \gamma(g)\). By optimality of \(\alpha, \alpha(\hat{\ell}) \subseteq g, \alpha(\{\text{Bool}_\ell \mid \ell \in \ell\}) = \text{Bool}_\alpha(\ell) \subseteq \text{Bool}_g\).

Case (U). \(\gamma_S(U_1 \xrightarrow{\ell} g U_2) = \gamma_S(U_1) \xrightarrow{\gamma(g)} \gamma_S(U_2)\)

So \(\hat{S} = \{S_1 \xrightarrow{\ell} g S_2\}\), with \(\{S_1\} \subseteq \gamma_S(U_1)\), \(\{S_2\} \subseteq \gamma_S(U_2)\), \(\{\ell\} \subseteq \gamma(g)\) and \(\{\ell\} \subseteq \gamma(g)\). By induction hypothesis, \(\alpha_S(\{S_1\}) \subseteq U_1\) and \(\alpha_S(\{S_2\}) \subseteq U_2\), and by optimality of \(\alpha, \alpha(\{\ell\}) \subseteq g\) and \(\alpha(\{\ell\}) \subseteq g\). Hence \(\alpha_S(\{S_1 \xrightarrow{\ell} g S_2\}) = \alpha_S(\{S_1\}) \xrightarrow{\alpha(\{\ell\})} \alpha_S(\{S_2\}) \subseteq U_1 \xrightarrow{\alpha(\{\ell\})} g U_2\).

Case (Ref). \(\gamma_S(\text{Ref}_\ell S) = \{\text{Ref}_\ell S \mid \ell \in \gamma(g), S \in \gamma(U)\}\)

So \(\hat{S} = \{\text{Ref}_\ell S \mid \ell \in \hat{\ell}, S \in \{\hat{S}\}\}\) for some \(\{\hat{S}\} \subseteq \gamma_S(U)\) and some \(\hat{\ell} \subseteq \gamma(g)\). By induction hypothesis \(\alpha_S(\{\hat{S}\}) \subseteq U\) and by optimality of \(\alpha, \alpha(\hat{\ell}) \subseteq g\), so \(\alpha_S(\{\text{Ref}_\ell S \mid \ell \in \hat{\ell}, S \in \{\hat{S}\}\}) = \text{Ref}_\alpha(\hat{\ell}) \alpha_S(\{\hat{S}\}) \subseteq \text{Ref}_g U\).

\[
\square
\]

**Proposition A.9 (\(\alpha_S\) is sound and optimal).** Assuming \(\hat{S}\) valid:

(i) \(\hat{S} \subseteq \gamma_S(\alpha_S(\hat{S}))\)

(ii) If \(\hat{S} \subseteq \gamma_S(U)\) then \(\alpha_S(\hat{S}) \subseteq U\).

**Proof.** Trivial using Prop C.3 and C.4.
C.2 Static Criteria for Gradual Typing

In this section we present the proof of Static Gradual Guarantee for GSLRef.

**Proposition 4.2 (Static Conservative Extension).** Let \( \vdash_S \) denote SSLRef’s type system. Then for any static language term \( t \in \text{TERM}, \vdash_S \ell_c \vdash_S t : S \) if and only if \( \vdash_S \ell_c \vdash t : S \).

**Proof.** By induction over the typing derivations. The proof is trivial because static types are given singleton meanings via concretization. \(\square\)

**Definition C.5 (Term precision).**

\[
\begin{align*}
(Px) & \quad x \equiv x \\
(Pb) & \quad g \equiv g' \quad \frac{b_g \equiv b_{g'}}{b_g \equiv b_{g'}} \\
(Pu) & \quad g \equiv g' \quad \frac{\text{unit}_g \equiv \text{unit}_{g'}}{\text{unit}_g \equiv \text{unit}_{g'}} \\
(Pu) & \quad g \equiv g' \quad \frac{U_1 \equiv U'_1 \quad g \equiv g' \quad (\lambda g' x : U_1. t)_g \equiv (\lambda g' x : U'_1. t')_{g'}}{(\lambda g' x : U_1. t)_g \equiv (\lambda g' x : U'_1. t')_{g'}} \\
(\text{prot}) & \quad t \equiv t' \quad \frac{g \equiv g' \quad \text{prot}_g(t) \subseteq \text{prot}_g(t')}{\text{prot}_g(t) \subseteq \text{prot}_g(t')} \\
(P\oplus) & \quad t_1 \equiv t'_1 \quad t_2 \equiv t'_2 \quad \frac{t_1 \oplus t_2 \equiv t'_1 \oplus t'_2}{t_1 \oplus t_2 \equiv t'_1 \oplus t'_2} \\
(P\text{app}) & \quad t_1 \equiv t'_1 \quad t_2 \equiv t'_2 \quad \frac{t_1 \cdot t_2 \equiv t'_1 \cdot t'_2}{t_1 \cdot t_2 \equiv t'_1 \cdot t'_2} \\
(P\text{ref}) & \quad t \equiv t' \quad U \equiv U' \quad \frac{t : U \equiv t' : U'}{t : U \equiv t' : U'} \\
(P\text{ref}) & \quad t \equiv t' \quad \frac{t \equiv t' \quad \text{ref}_U \equiv \text{ref}_{U'} \quad t \equiv t' \quad \text{ref}_U \equiv t \equiv t'}{t \equiv t' \quad \text{ref}_U \equiv \text{ref}_{U'} \quad t \equiv t' \quad \text{ref}_U \equiv \text{ref}_{U'} \quad t \equiv t'} \\
(P\text{if}) & \quad t \equiv t' \quad \frac{t_1 \equiv t_1' \quad t_2 \equiv t_2' \quad \text{if \; then \; t_1 \; else \; t_2 \; \equiv \; if \; then \; t_1' \; else \; t_2'}{t \equiv t'} \\
(P\text{def}) & \quad t \equiv t' \quad \frac{t \equiv t' \quad \text{ref}_U \equiv \text{ref}_{U'} \quad t \equiv t' \quad \text{ref}_U \equiv \text{ref}_{U'} \quad t \equiv t'}{t \equiv t'} \\
(P\text{pass}) & \quad t_1 \equiv t_1' \quad t_2 \equiv t_2' \quad \frac{t_1 : t_2 \equiv t_1' : t_2'}{t_1 : t_2 \equiv t_1' : t_2'} \\
\end{align*}
\]

**Definition C.6 (Type environment precision).**

\[
\Gamma \equiv \Gamma' \quad U \equiv U' \quad \frac{\Gamma \equiv \Gamma' \quad U \equiv U' \quad \Gamma, x : U \equiv \Gamma', x : U'}{\Gamma, x : U \equiv \Gamma', x : U'}
\]

**Lemma C.7.** If \( \Gamma, \vdash_S \ell_c \vdash t : U \) and \( \Gamma \equiv \Gamma' \), then \( \Gamma, \vdash_S \ell_c \vdash t : U' \) for some \( U \leq U' \).

**Proof.** Simple induction on typing derivations. \(\square\)

**Lemma C.8.** If \( U_1 \leq U_2 \) and \( U_1 \equiv U'_1 \) and \( U_2 \equiv U'_2 \) then \( U'_1 \leq U'_2 \).

**Proof.** By definition of \( \leq \), there exists \( \langle S_1, S_2 \rangle \in \gamma^2(U_1, U_2) \) such that \( S_1 \leq S_2 \). \( U_1 \equiv U'_1 \) and \( U_2 \equiv U'_2 \) mean that \( \gamma(U_1) \subseteq \gamma(U'_1) \) and \( \gamma(U_2) \subseteq \gamma(U'_2) \), therefore \( \langle S_1, S_2 \rangle \in \gamma^2(U'_1, U'_2) \). \(\square\)

**Lemma C.9.** If \( g_1 \leq g_2 \leq g_3 \), \( g_1 \equiv g'_1 \), \( g_2 \equiv g'_2 \) and \( g_3 \equiv g'_3 \), then \( g'_1 \leq g'_2 \leq g'_3 \).

**Proof.** By definition of the consistent judgment, there exists \( \langle \ell_1, \ell_2, \ell_3 \rangle \in \gamma^3(g_1, g_2, g_3) \) such that \( \ell_1 \leq \ell_2 \leq \ell_3 \), \( g_1 \equiv g'_1 \), \( g_2 \equiv g'_2 \) and \( g_3 \equiv g'_3 \) mean that \( \gamma(g_1) \subseteq \gamma(g'_1) \), \( \gamma(g_2) \subseteq \gamma(g'_2) \) and \( \gamma(g_3) \subseteq \gamma(g'_3) \) respectively. Therefore \( \langle \ell_1, \ell_2, \ell_3 \rangle \in \gamma^3(g_1, g_2, g_3) \). \(\square\)

**Lemma C.10.** If \( g_1 \leq g_2 \), \( g_1 \equiv g'_1 \) and \( g_2 \equiv g'_2 \), then \( g'_1 \leq g'_2 \).

**Proof.** Using almost identical argument of Lemma C.9 \(\square\)

**Proposition 4.4 (Static Gradual Guarantee).** Suppose \( g_{c_1} \equiv g_{c_2} \) and \( t_1 \equiv t_2 \).

If \( \vdash_S : g_{c_1} \vdash t_1 : U_1 \) and \( g_{c_1} \equiv g_{c_2} \) and \( t_1 \equiv t_2 \) then \( \vdash_S : g_{c_2} \vdash t_2 : U_2 \) where \( U_1 \equiv U_2 \).

**Proof.** We prove the property on opens terms instead of closed terms: If \( \Gamma, \vdash_S : g_{c_1} \vdash t_1 : U_1 \), \( g_{c_1} \equiv g_{c_2} \) and \( t_1 \equiv t_2 \) then \( \Gamma, \vdash_S : g_{c_2} \vdash t_2 : U_2 \) and \( U_1 \equiv U_2 \).

The proof proceed by induction on the typing derivation.

**Case (Ux, Ub, Uu).** Trivial by definition of \( \equiv \) using (Px), (Pb), (Pu) respectively.
Case \((U \lambda)\). Then \(t_1 = (\lambda^g x : U_1'. t)\) and \(U_1 = U_1' \frac{g}{g'} U_2\). By \((U \lambda)\) we know that:

\[
\begin{align*}
\frac{}{
\begin{array}{c}
\Gamma, x : U_1'; \vdash: g e \vdash: t : U_2' \\
\Gamma; \vdash: g c_1 \vdash (\lambda^g x : U_1'. t) g : U_1' \frac{g}{g'} U_2'
\end{array}
\end{align*}
\]

(1)

Consider \(g c_2\) such that \(g c_1 \sqsubseteq g c_2\) and \(t_2\) such that \(t_1 \sqsubseteq t_2\). By definition of term precision \(t_2\) must have the form \(t_2 = (\lambda^g x : U_1''. t')\) and therefore

\[
\frac{}{
\begin{array}{c}
t \sqsubseteq t' \\
(\lambda^g x : U_1'. t) g \sqsubseteq g' \\
(\lambda^g x : U_1''. t') g' \sqsubseteq g'
\end{array}
\end{align*}

(2)

Using induction hypotheses on the premise of 1, \(\Gamma, x : U_1'; \vdash: g e \vdash: t' : U_2''\) with \(U_2 \sqsubseteq U_2''\). By Lemma C.7, \(\Gamma, x : U_1''; \vdash: g c_2 \vdash: t' : U_2''\) where \(U_2'' \sqsubseteq U_2''\). Then we can use rule \((U \lambda)\) to derive:

\[
\frac{}{
\begin{array}{c}
\Gamma, x : U_1''; \vdash: g c_2 \vdash: t' : U_2'' \\
\Gamma; \vdash: g c_1 \vdash (\lambda^g x : U_1'. t') g' : U_1'' \frac{g'}{g'} U_2''
\end{array}
\end{align*}

Where \(U_2 \sqsubseteq U_2''\). Using the premise of 2 and the definition of type precision we can infer that

\[
U_1' \frac{g}{g'} U_2' \sqsubseteq U_1'' \frac{g'}{g'} U_2''
\]

and the result holds.

Case \((U o)\). This case can not happen because initial programs do not contain locations.

Case \((U \text{ prot})\). Then \(t_1 = \text{prot}_g(t)\) and \(U_1 = U \overrightarrow{\text{v}} g\). By \((U \text{ prot})\) we know that:

\[
\frac{}{
\begin{array}{c}
\Gamma; \vdash: g c_1 \vdash \text{v} g \vdash: t : U \\
\Gamma; \vdash: g c_1 \vdash \text{prot}_g(t) : U \overrightarrow{\text{v}} g
\end{array}
\end{align*}

(3)

Consider \(g c_2\) such that \(g c_1 \sqsubseteq g c_2\) and \(t_2\) such that \(t_1 \sqsubseteq t_2\). By definition of term precision \(t_2\) must have the form \(t_2 = \text{prot}_g(t')\) and therefore

\[
\frac{}{
\begin{array}{c}
t \sqsubseteq t' \\
g \sqsubseteq g'
\end{array}
\end{align*}

(4)

By definition of join on consistent labels, \(g c_1 \overrightarrow{\text{v}} g \sqsubseteq g c_2 \overrightarrow{\text{v}} g'\). Using induction hypotheses on the premises of 3, we can use rule \((U \text{ prot})\) to derive:

\[
\frac{}{
\begin{array}{c}
\Gamma; \vdash: g c_2 \overrightarrow{\text{v}} g' \vdash: t' : U' \\
\Gamma; \vdash: g c_2 \vdash \text{prot}_g(t') : U' \overrightarrow{\text{v}} g'
\end{array}
\end{align*}

For some \(U'\), where \(U \sqsubseteq U'\). Using the premise of 4 and the definition of join we can infer that

\[
U \overrightarrow{\text{v}} g \sqsubseteq U' \overrightarrow{\text{v}} g'
\]

and the result holds.

Case \((U \oplus)\). Then \(t_1 = t'_1 \oplus t'_2\) and \(U_1 = \text{Bool}_{(g_1,\overrightarrow{\text{v}} g_2)}\). By \((U \oplus)\) we know that:

\[
\frac{}{
\begin{array}{c}
\Gamma; \vdash: g c_1 \vdash: t'_1 : \text{Bool}_{g_1} \\
\Gamma; \vdash: g c_1 \vdash: t'_2 : \text{Bool}_{g_2} \\
\Gamma; \vdash: g c_1 \vdash: t'_1 \oplus t'_2 : \text{Bool}_{(g_1,\overrightarrow{\text{v}} g_2)}
\end{array}
\end{align*}

(5)
Consider \( g_{c2} \) such that \( g_{c1} \sqsubseteq g_{c2} \) and \( t_2 \) such that \( t_1 \sqsubseteq t_2 \). By definition of term precision \( t_2 \) must have the form \( t_2 = t'_2 \oplus t''_2 \) and therefore

\[
\begin{array}{c}
\text{(P+)} \quad t'_1 \sqsubseteq t'_1'' \quad t'_2 \sqsubseteq t''_2 \\
t'_1 \oplus t'_2 \sqsubseteq t'_1'' \oplus t''_2 \\
\end{array}
\]

(6)

Using induction hypotheses on the premises of 5, we can use rule \((U+)\) to derive:

\[
\begin{array}{c}
\Gamma;::g_{c2} \vdash t'_1'' : \text{Bool}_{g'_1} \\
\Gamma;::g_{c2} \vdash t''_2 : \text{Bool}_{g'_2}
\end{array}
\]

\[
\Gamma;::g_{c2} \vdash t'_1'' \oplus t''_2 : \text{Bool}_{(g'_1 \lor g'_2)}
\]

Where \( g'_1 \sqsubseteq g'_2 \) and \( g'_2 \sqsubseteq g''_2 \). Using the premise of 6 and the definition of type precision we can infer that

\[
(g'_1 \lor g'_2) \sqsubseteq (g'_1 \lor g''_2)
\]

and the result holds.

**Case** \((U\text{app})\). Then \( t_1 = t'_1 \oplus t'_2 \) and \( U_1 = U_{12} \lor g\). By \((U\text{app})\) we know that:

\[
\Gamma;::g_{c1} \vdash t'_1 : U_{12} \quad \Gamma;::g_{c1} \vdash t'_2 : U_{12}
\]

\[
\Gamma;::g_{c1} \vdash t'_1 \oplus t'_2 : U_{12} \lor g
\]

(7)

Consider \( g_{c2} \) such that \( g_{c1} \sqsubseteq g_{c2} \) and \( t_2 \) such that \( t_1 \sqsubseteq t_2 \). By definition of term precision \( t_2 \) must have the form \( t_2 = t''_1 \oplus t''_2 \) and therefore

\[
\begin{array}{c}
\text{(Papp)} \quad t'_1 \sqsubseteq t'_1'' \quad t'_2 \sqsubseteq t''_2 \\
t'_1 \oplus t'_2 \sqsubseteq t'_1'' \oplus t''_2
\end{array}
\]

(8)

Using induction hypotheses on the premises of 7, \( \Gamma;::g_{c2} \vdash t''_1 : U_{12} \lor g \) and \( \Gamma;::g_{c2} \vdash t''_2 : U_{12} \lor g \), where \( U'_2 \subseteq U''_2 \), \( U_{11} \xrightarrow{g'} U_{12} \subseteq U'_1 \) and \( U_{11} \xrightarrow{g'} U_{12} \). By Lemma C.8, \( U''_2 \sqsubseteq U''_1 \). By definition of precision of types, \( g'_2 \sqsubseteq g''_2 \) and \( g \sqsubseteq g' \), therefore by Lemma C.9, \( g' \lor g_{c2} \sqsubseteq g''_2 \). Then we can use rule \((U\text{app})\) to derive:

\[
\Gamma;::g_{c2} \vdash t''_1 : U_{12} \lor g \quad \Gamma;::g_{c2} \vdash t''_2 : U_{12} \lor g
\]

Using the definition of type precision we can infer that

\( U_{12} \lor g \sqsubseteq U_{12} \lor g' \)

and the result holds.

**Case** \((U\text{if})\). Then \( t_1 = \text{if } t \text{ then } t'_1 \text{ else } t_2 \) and \( U_1 = (U'_1 \lor U'_2) \lor g \). By \((U\text{if})\) we know that:

\[
\Gamma;::g_{c1} \vdash t : \text{Bool}_g
\]

\[
\Gamma;::g_{c1} \lor g \vdash t'_1 : U'_1 \\
\Gamma;::g_{c1} \lor g \vdash t_2 : U'_2
\]

(9)

Consider \( g_{c2} \) such that \( g_{c1} \sqsubseteq g_{c2} \) and \( t_2 \) such that \( t_1 \sqsubseteq t_2 \). By definition of term precision \( t_2 \) must have the form \( t_2 = \text{if } t' \text{ then } t''_1 \text{ else } t''_2 \) and therefore

\[
\begin{array}{c}
\text{(Pif)} \quad t \sqsubseteq t' \quad t'_1 \sqsubseteq t''_1 \quad t'_2 \sqsubseteq t''_2
\\
\text{if } t \text{ then } t'_1 \text{ else } t'_2 \sqsubseteq \text{if } t' \text{ then } t'_1 \text{ else } t'_2
\end{array}
\]

(10)
Consider any \( \ell' \) such that \( \ell \subseteq \ell' \). As \( g_{c_1} \trianglerighteq g \sqsubseteq g_{c_2} \trianglerighteq g' \) then we can use induction hypotheses on the premises of 9 and derive:

\[
\frac{\Gamma; : g_{c_2} + t' : \text{Bool}_g}{\Gamma; : g_{c_2} \trianglerighteq g + t'_{i_1} : U'_{i_1}} \quad \frac{\Gamma; : g_{c_2} \trianglerighteq g' + t'_{i_2} : U''_{i_2}}{\Gamma; : g_{c_2} \trianglerighteq g' + \text{if } t' \text{ then } t'_{i_2} \text{ else } t'_{i_2}' : (U'_{i_1} \trianglerighteq U''_{i_2}) \trianglerighteq g'}
\]

Where \( U'_{i_1} \sqsubseteq U''_{i_1} \) and \( U'_{i_2} \sqsubseteq U''_{i_2} \). Using the definition of type precision we can infer that

\[
(U'_{i_1} \trianglerighteq U'_{i_2}) \trianglerighteq g \sqsubseteq (U''_{i_1} \trianglerighteq U''_{i_2}) \trianglerighteq g'
\]

and the result holds.

**Case (U::).** Then \( t_1 = t :: U_1 \). By (U::) we know that:

\[
\frac{\Gamma; : g_{c_1} \trianglerighteq t : U_1' \quad U_1' \sqsubseteq U_1}{\Gamma; : g_{c_1} \trianglerighteq t :: U_1': U_1}
\]

(11)

Consider \( g_{c_2} \) such that \( g_{c_1} \sqsubseteq g_{c_2} \) and \( t_2 \) such that \( t_1 \sqsubseteq t_2 \). By definition of term precision \( t_2 \) must have the form \( t_2 = t' :: U_2 \) and therefore

\[
\frac{t \sqsubseteq t' \quad U_1 \sqsubseteq U_2}{t :: U_1 \sqsubseteq t' :: U_2}
\]

(12)

Using induction hypotheses on the premises of 11, \( \Gamma; : g_c \trianglerighteq t' : U_2' \) where \( U_1' \sqsubseteq U_2' \). We can use rule (U::) and Lemma C.8 to derive:

\[
\frac{\Gamma; : g_{c_2} \trianglerighteq t' : U_2' \quad U_2' \sqsubseteq U_2}{\Gamma; : g_{c_2} \trianglerighteq t' :: U_2': U_2}
\]

Where \( U_1 \sqsubseteq U_2 \) and the result holds.

**Case (Uref).** Then \( t_1 = \text{ref}^U t \) and \( U_1 = \text{Ref}_{g_c} U \). By (Uref) we know that:

\[
\frac{\Gamma; : g_{c_1} \trianglerighteq t : U_1' \quad U_1' \sqsubseteq U \quad g_{c_1} \trianglerighteq \text{label}(U)}{\Gamma; : g_{c_1} \trianglerighteq \text{ref}^U t :: \text{Ref}_U U}
\]

(13)

Consider \( g_{c_2} \) such that \( g_{c_1} \sqsubseteq g_{c_2} \) and \( t_2 \) such that \( t_1 \sqsubseteq t_2 \). By definition of term precision \( t_2 \) must have the form \( t_2 = \text{ref}^{U'} t' \) and therefore

\[
\frac{t \sqsubseteq t' \quad U \sqsubseteq U'}{\text{ref}^{U'} t \sqsubseteq \text{ref}^{U'} t'}
\]

(14)

Using induction hypotheses on the premises of 13, we can use rule (Uref) and Lemma C.8 and C.10 to derive:

\[
\frac{\Gamma; : g_{c_2} \trianglerighteq t' : U_1'' \quad U_1'' \sqsubseteq U' \quad g_{c_2} \trianglerighteq \text{label}(U')}{\Gamma; : g_{c_2} \trianglerighteq \text{ref}^{U'} t' :: \text{Ref}_U U'}
\]

Where \( U \sqsubseteq U' \) and \( U_1' \sqsubseteq U_1'' \). Using the the definition of type precision we can infer that

\[
U \sqsubseteq U'
\]

and the result holds.

**Case (Uderef).** Then \( t_1 = !t \) and \( U_1 = U \trianglerighteq g \). By (Uderef) we know that:

\[
\frac{\Gamma; : g_{c_1} \trianglerighteq t :: \text{Ref}_g U}{\Gamma; : g_{c_1} \trianglerighteq !t :: U \trianglerighteq g}
\]

(15)
Consider \( g_{c2} \) such that \( g_{c1} \subseteq g_{c2} \) and \( t_2 \) such that \( t_1 \subseteq t_2 \). By definition of term precision \( t_2 \) must have the form \( t_2 = !t' \) and therefore

\[
(Pderef) \quad t \equiv t' \quad !t \not\equiv !t'
\]

Using induction hypotheses on the premises of 15, we can use rule \((Uderef)\) to derive:

\[
(Uderef) \quad \Gamma; :: g_{c2} \vdash t' : \text{Ref}_{g'} U'
\]

Where \( g \equiv g' \) and \( U \subseteq U' \). Using the premise of 16 and the definition of type precision we can infer that

\[
U \triangledown g \equiv U' \triangledown g'
\]

and the result holds.

**Case \((U\text{asgn})\).** Then \( t_1 = t'_1 := t'_2 \) and \( U_1 = \text{Unit}_{\perp} \). By \((U\text{asgn})\) we know that:

\[
\Gamma; :: g_{c1} \vdash t'_1 : \text{Ref}_g U'_1 \quad \Gamma; :: g_{c1} \vdash t'_2 : U'_2
\]

\[
(U\text{asgn}) \quad U'_2 \subseteq U'_1 \quad g \triangledown g_{c1} \ll label(U'_1) \quad \Gamma; :: g_{c1} \vdash t'_1 := t'_2 : \text{Unit}_{\perp}
\]

Using induction hypotheses on the premises of 17, \( \Gamma; :: g_{c2} \vdash t'_1 : \text{Ref}_{g'} U'_{1'} \) and \( \Gamma; :: g_{c2} \vdash t'_2 : U'_{2'} \), where \( \text{Ref}_g U'_1 \ll \text{Ref}_{g'} U'_{1'} \) and \( U'_2 \ll U'_{2'} \). By definition of precision on types and Lemma C.8, \( U'_{2'} \ll U'_{1'} \). Also, as \( g \equiv g' \) and \( U'_1 \ll U'_{1'} \), by Lemma C.9, \( g' \triangledown g_{c2} \ll label(U'_{1'}) \). Then we can use rule \((U\text{asgn})\) to derive:

\[
\Gamma; :: g_{c2} \vdash t'_1 : \text{Ref}_{g'} U'_{1'} \quad \Gamma; :: g_{c2} \vdash t'_2 : U'_{2'} \quad U'_{2'} \ll U'_{1'} \quad g' \triangledown g_{c2} \ll label(U'_{1'})
\]

\[
(U\text{asgn}) \quad \Gamma; :: g_{c2} \vdash t'_1 := t'_2 : \text{Unit}_{\perp}
\]

Using the definition of type precision we can infer that

\[
\text{Unit}_{\perp} \ll \text{Unit}_{\perp}
\]

and the result holds. \(\Box\)
D GRADUALIZING THE DYNAMIC SEMANTICS

In this section we present the formalization of the evidences for GSL\textsubscript{Ref}. Section D.1 presents the structure of evidence and the abstraction and concretization functions. In section D.2, we show how to calculate the initial evidence. In particular we give definition for the initial evidence of consistent judgments for labels and types. In section D.2, we present how to evolve evidence. We define the consistent transitivity operator, the meet operator and join of evidences. In section D.4, we present the algorithmic definitions of initial evidence and consistent transitivity. Finally, in section D.5, we present some of the proofs of the propositions for evidence presented.

D.1 Precise Evidence for Consistent Security Judgments

**Definition D.1 (Interval).** An interval is a bounded unknown label $[\ell_1, \ell_2]$ where $\ell_1$ is the upper bound and $\ell_2$ is the lower bound.

$$i \in \text{Label}^2$$

$$i ::= [\ell, \ell] \quad \text{(interval)}$$

**Definition D.2 (Interval Concretization).** Let $\gamma_i : \text{Label}^2 \rightarrow \mathcal{P}(\text{Label})$ be defined as follows:

$$\gamma_i([\ell_1, \ell_2]) = \{ \ell \mid \ell \in \text{Label}, \ell_1 \leq \ell \leq \ell_2 \}$$

We can only concretize valid intervals:

**Definition D.3 (Valid Gradual Label).**

$$\ell_1 \leq \ell_2 \quad \text{valid}([\ell_1, \ell_2])$$

**Definition D.4 (Label Evidence Concretization).** Let $\gamma_{\varepsilon} : \text{Label}^4 \rightarrow \mathcal{P}(\text{Label}^2)$ be defined as follows:

$$\gamma_{\varepsilon}(\langle \ell_1, \ell_2 \rangle) = \{ \langle \ell_1, \ell_2 \rangle \mid \ell_1 \in \gamma_i(\ell_1), \ell_2 \in \gamma_i(\ell_2) \}$$

**Definition D.5 (Interval Abstraction).** Let $\alpha_i : \mathcal{P}(\text{Label}) \rightarrow \text{Label}^2$ be defined as follows:

$$\alpha_i(\emptyset) \text{ is undefined}$$

$$\alpha_i(\{ \ell \}) = [\ell \leftarrow \ell, \ell \leftarrow \ell] \quad \text{otherwise}$$

**Definition D.6 (Label Evidence Abstraction).** Let $\alpha_{\varepsilon} : \mathcal{P}(\text{Label}^2) \rightarrow \text{Label}^4$ be defined as follows:

$$\alpha_{\varepsilon}(\emptyset) \text{ is undefined}$$

$$\alpha_{\varepsilon}(\{ \langle \ell_1, \ell_2 \rangle \}) = \langle \alpha_i(\{ \ell_1 \}), \alpha_i(\{ \ell_2 \}) \rangle \quad \text{otherwise}$$

**Definition D.7 (Type Evidence).** An evidence type is a gradual type labeled with an interval:

$$E \in \text{GETYPE}, \quad t \in \text{Label}^2$$

$$E ::= \text{Bool}_t \mid E \rightarrow E \mid \text{Ref}_t E \mid \text{Unit}_t \quad \text{(evidence types)}$$

**Definition D.8 (Type Evidence Concretization).** Let $\gamma_E : \text{GETYPE} \rightarrow \mathcal{P}(\text{TYPE})$ be defined as follows:

$$\gamma_E(\text{Bool}_t) = \{ \text{Bool}_t \mid \ell \in \gamma_i(\ell) \}$$

$$\gamma_E(E_1 \rightarrow \ell_1, E_2) = \gamma_E(E_1) \circ \gamma_i(\ell_1) \gamma_E(E_2)$$

$$\gamma_E(\text{Ref}_t E) = \{ \text{Ref}_t S \mid \ell \in \gamma_i(\ell), S \in \gamma_E(E) \}$$

where $\circ$ is the set of all possible combinations of function types, using each member of the sets obtained by the $\gamma_E$ and $\gamma_i$ functions.
Definition D.9 (Evidence Concretization). Let
\( \gamma_{\ell_1} : \text{GETYPE}^2 \to \mathcal{P}(\text{TYPE}^2) \) be defined as follows:

\[ \gamma_{\ell_1}(E_1, E_2) = \{ (S_1, S_2) \mid S_1 \in \gamma_{\ell_1}(E_1), S_2 \in \gamma_{\ell_1}(E_2) \} \]

Definition D.10 (Type Evidence Abstraction). Let the abstraction function \( \alpha_E : \mathcal{P}(\text{TYPE}) \to \text{GETYPE} \) be defined as:

\[
\alpha_E(\{ \text{Bool} \}) = \text{Bool} \\
\alpha_E(\{ S \}) = \alpha_E(\{ \overline{\text{Ref}} \}) = \text{Ref} \\
\alpha_E(\{ \ell \}) = \alpha_{\ell_1}(\text{top})
\]

Definition D.11 (Evidence Abstraction). Let \( \alpha_{\ell_1} : \mathcal{P}(\text{TYPE}^2) \to \text{GETYPE}^2 \) be defined as follows:

\[
\alpha_{\ell_1}(0) \text{ is undefined} \\
\alpha_{\ell_1}(\{ S_1, S_2 \}) = \langle \alpha_E(\{ S_{11} \}), \alpha_E(\{ S_{21} \}) \rangle \text{ otherwise}
\]

We can only abstract \textit{valid} sets of security types, \textit{i.e.} in which elements only defer by security labels.

Definition D.12 (Valid Type Sets).

\[
\begin{align*}
\text{valid}(\{ \text{Bool} \}) & \quad \text{valid}(\{ S \}) & \quad \text{valid}(\{ \text{Ref} \}) \\
\text{valid}(\{ S \}) & \quad \text{valid}(\{ \ell \}) & \quad \text{valid}(\{ S \}) \\
\text{valid}(\{ \ell \}) & \quad \text{valid}(\{ \text{Unit} \})
\end{align*}
\]

Proposition D.13 (\( \alpha_{\ell_1} \text{ is Sound} \)). If \( \ell \) is not empty, then \( \ell \subseteq \gamma_{\ell_1}(\alpha_{\ell_1}(\ell)) \).

Proposition D.14 (\( \alpha_{\ell_1} \text{ is Optimal} \)). If \( \ell \) is not empty, and \( \ell \subseteq \gamma_{\ell_1}(i) \) then \( \alpha_{\ell_1}(\ell) \subseteq \ell \).

Proposition D.15 (\( \alpha_E \text{ is Sound} \)). If valid(\( \bar{S} \)) then \( \bar{S} \subseteq \gamma_E(\alpha_E(\bar{S})) \).

Proposition D.16 (\( \alpha_E \text{ is Optimal} \)). If valid(\( \bar{S} \)) and \( \bar{S} \subseteq \gamma_E(E) \) then \( \alpha_E(\bar{S}) \subseteq E \).

With concretization of security type, we can now define security type precision.

Definition D.17 (Interval and Type Evidence Precision).

1. \( t_1 \) is less imprecise than \( t_2 \), notation \( t_1 \sqsubseteq t_2 \), if and only if \( \gamma_{\ell_1}(t_1) \sqsubseteq \gamma_{\ell_1}(t_2) \); inductively:

\[
\ell_3 \ll \ell_1 \quad \ell_2 \ll \ell_4 \\
[\ell_1, \ell_2] \sqsubseteq [\ell_3, \ell_4]
\]

2. \( E_1 \) is less imprecise than \( E_2 \), notation \( E_1 \sqsubseteq E_2 \), if and only if \( \gamma_E(E_1) \sqsubseteq \gamma_E(E_2) \); inductively:

\[
t_1 \sqsubseteq t_2 \\
\text{Bool}_{t_1} \sqsubseteq \text{Bool}_{t_2} \\
E_{11} \sqsubseteq E_{21} \quad E_{12} \sqsubseteq E_{22} \\
t_1 \sqsubseteq t_2 \\
E_{11} \sqsubseteq E_{12} \sqsubseteq E_{21} \sqsubseteq E_{22}
\]
D.2 Initial evidence

With the definition of concretization and abstraction we can now define the initial evidence of label ordering and subtyping:

Definition D.18 (Initial Evidence of label ordering). Let \( F_1 : \text{LABEL}^n \rightarrow \text{LABEL} \) and \( F_2 : \text{LABEL}^m \rightarrow \text{LABEL} \) be functions over labels. The initial evidence of the judgment \( F_1(\gamma_i) \triangleleft F_2(\gamma_j) \), notation \( \mathcal{G}[F_1(\gamma_i) \triangleleft F_2(\gamma_j)] \), is defined as follows:

\[
\mathcal{G}[F_1(g_1, \ldots, g_n) \triangleleft F_2(g_{n+1}, \ldots, g_{n+m})] = \\
\alpha_{\ell_i}(\{(F_1(\overline{\ell}_i), F_2(\overline{\ell}_j)) \mid \overline{\ell}_i \in \gamma_i^{n}(\gamma_i^{1/n}), \overline{\ell}_j \in \gamma_j^{m}(\gamma_j^{1/m}) \mid F_1(\overline{\ell}_i) \triangleleft F_2(\overline{\ell}_j)\})
\]

Suppose \( F_1 = F_{11} \)

Definition D.19 (Initial Evidence of subtyping). Let \( F_1 : \text{TYPE}^n \rightarrow \text{TYPE} \) and \( F_2 : \text{TYPE}^m \rightarrow \text{TYPE} \) be functions over types. The initial evidence of the judgment \( F_1(U_i) \triangleleft F_2(U_j) \), notation \( \mathcal{G}[F_1(U_i) \triangleleft F_2(U_j)] \), is defined as follows:

\[
\mathcal{G}[F_1(U_1, \ldots, U_n) \triangleleft F_2(U_{n+1}, \ldots, U_{n+m})] = \\
\alpha_{\ell_i}(\{(F_1(\overline{S}_i), F_2(\overline{S}_j)) \mid \overline{S}_i \in \gamma_s^{n}(\gamma_s^{1/n}), \overline{S}_j \in \gamma_s^{m}(\gamma_s^{1/m}) \mid F_1(\overline{S}_i) \triangleleft F_2(\overline{S}_j)\})
\]

Proposition D.20. [Elaboration preserves typing] Consider \( \Gamma; \Sigma; g_c \vdash t : U \) then if \( \Gamma; \Sigma; g_c \vdash t \rightsquigarrow t' : U \), and \( e = \mathcal{G}[\ell_i] \), then \( \Gamma; \Sigma ; e g_c \vdash t' : U \)

Proof. Straightforward induction on type \( U \). □

D.3 Evolving evidence: Consistent Transitivity

Now that we know how to extract initial evidence from consistent judgments, we need a way to combine evidences to use during program evaluation, i.e. we need to find a way to evolve evidence. We define consistent transitivity for label ordering and subtyping, \( \circ \triangleleft \) and \( \circ \triangleleft \) respectively, to combine evidences as follows:

Definition D.21 (Consistent transitivity for label ordering). Let function \( \circ \triangleleft : \text{INTERVAL}^2 \times \text{INTERVAL}^2 \rightarrow \text{LABEL}^2 \) be defined as:

\[
(\ell_{11}, \ell_{12}) \circ \triangleleft (\ell_{21}, \ell_{22}) = \alpha_{\ell_i}(\{(\ell_{11}, \ell_{22}) \in \gamma_{\ell_i}(\gamma_{\ell_i}(\ell_{11}, \ell_{22})) \mid \exists \ell \in \gamma_{\ell_1}(\ell_{11}) \cap \gamma_{\ell_2}(\ell_{22}) \land \ell \leq \ell_{11} \land \ell_{22} \leq \ell \})
\]

Proposition 6.14. Suppose \( \varepsilon_1 \vdash F_1(\overline{\gamma}) \triangleleft F_2(\overline{\gamma}) \) and \( \varepsilon_2 \vdash F_2(\overline{\gamma}) \triangleleft F_3(\overline{\gamma}) \).

If \( \varepsilon_1 \circ \triangledown \varepsilon_2 \) is defined, then \( \varepsilon_1 \circ \triangledown \varepsilon_2 \vdash F_1(\overline{\gamma}) \triangleleft F_3(\overline{\gamma}) \)

Proposition D.22. \( \gamma_i(t_{11} \cap t_{21}) = \gamma_i(t_{11}) \cap \gamma_i(t_{21}) \).

where \( t \cap t' = \alpha(\gamma(t) \cap \gamma(t')) \).

Proposition D.23. \( (\ell_{11}, \ell_{22}) \circ \triangledown (\ell_{22}, \ell_{33}) = \Delta(\ell_{11}, \ell_{21} \cap \ell_{22}, \ell_{33}) \)

where

\[
\Delta(\ell_{11}, \ell_{22}, \ell_{33}) = \alpha_{\ell_i}(\{(\ell_{11}, \ell_{33}) \in \gamma_{\ell_i}(\gamma_{\ell_i}(\ell_{11}, \ell_{22})) \mid \exists \ell_{22} \in \gamma_{\ell_2}(\ell_{22}) \land \ell_{11} \leq \ell_{22} \land \ell_{11} \leq \ell_{33} \})
\]
Definition D.24 (Consistent transitivity for subtyping). Suppose
\[(E_{11}, E_{12}) \vdash F_{i}(\overline{U_i}) <: F_{j}(\overline{U_j}) \quad \text{and} \quad (E_{21}, E_{22}) \vdash F_{2}(\overline{U_j}) <: F_{3}(\overline{U_k})\]
We deduce evidence for consistent transitivity for subtyping:
\[(E_{11}, E_{12}) \circ <: (E_{21}, E_{22}) \vdash F_{i}(\overline{U_i}) <: F_{3}(\overline{U_k})\]
where \(\circ <: \) is defined as:
\[(E_{11}, E_{12}) \circ <: (E_{21}, E_{22}) = \alpha_{t}(\{\{S_{11}, S_{22}\} \in \gamma_{t}\langle (E_{11}, E_{12})\rangle \mid \exists S \in \gamma_{t}(E_{12}) \cap \gamma_{t}(E_{21}), S_{1} <: S \land S <: S_{22}\})\]

Proposition D.25. \(\gamma_{E}(E_{1} \cap E_{2}) = \gamma_{E}(E_{2})\)

Then following AGT,
Proposition D.26.
\[(E_{1}, E_{21}) \circ <: (E_{22}, E_{3}) = \Delta_{\circ <:}(E_{1}, E_{21} \cap E_{22}, E_{3})\]
where
\[\Delta_{\circ <:}(E_{1}, E_{2}, E_{3}) = \alpha_{t}(\{\{S_{1}, S_{3}\} \in \gamma_{t}(E_{1}, E_{3}) \mid \exists S_{2} \in \gamma_{t}(E_{2}).S_{1} <: S_{2} \land S_{2} <: S_{3}\})\]

Definition D.27 (Intervals join).
\[[\ell_{1}, \ell_{2}]_{\overline{\gamma}}[\ell_{3}, \ell_{4}] = [\ell_{1} \lor \ell_{3}, \ell_{2} \land \ell_{4}]\]

Definition D.28 (Evidence label join).
\[(t_{1}, t_{2})_{\overline{\gamma}}(t_{3}, t_{4}) = (t_{1} \overline{\gamma} t_{3}, t_{2} \overline{\gamma} t_{4})\]

Definition D.29.
\[
\begin{align*}
\text{Bool}_{t_{1} \overline{\gamma} t_{2}} & = \text{Bool}_{(t_{1} \overline{\gamma} t_{2})} \\
E_{1} & \overrightarrow{t_{1}} E_{2} \overline{\gamma} t_{3} = E_{1} \overrightarrow{t_{1}} (t_{1} \overline{\gamma} t_{2}) E_{2} \\
\text{Ref}_{t_{1}} E \overline{\gamma} t_{2} & = \text{Ref}_{(t_{1} \overline{\gamma} t_{2})} E
\end{align*}
\]

Definition D.30.
\[(E_{1}, E_{2})_{\overline{\gamma}}(t_{1}, t_{2}) = (E_{1} \overline{\gamma} t_{1}, E_{2} \overline{\gamma} t_{2})\]

Proposition D.31. If \(\epsilon_{S} \vdash U_{1} \leq U_{2} \) and \(\epsilon_{1} \vdash g_{1} \leq g_{2}\) then \(\epsilon_{S} \overline{\gamma} \epsilon_{1} \vdash U_{1} \overline{\gamma} g_{1} <: U_{2} \overline{\gamma} g_{2}\)

D.4 Algorithmic definitions
This section gives algorithmic definitions of consistent transitivity and initial evidence for label ordering and subtyping.

D.4.1 Label Evidences.
Definition D.32 (Intervals meet).
\[[\ell_{1}, \ell_{2}]_{\overline{\alpha}}[\ell_{3}, \ell_{4}] = [\ell_{1} \land \ell_{3}, \ell_{2} \land \ell_{4}]\]

Definition D.33 (Intervals meet).
\[[\ell_{1}, \ell_{2}]_{\overline{\alpha}}[\ell_{3}, \ell_{4}] = [\ell_{1} \land \ell_{3}, \ell_{2} \land \ell_{4}]\]
Definition D.34. Let $F_1 : \text{GLABEL}^n \to \text{GLABEL}$ and $F_2 : \text{GLABEL}^m \to \text{GLABEL}$. The initial evidence for consistent judgment $F_1(g_1) \leq F_2(g_2)$ is defined as follows:

\[
\begin{align*}
\text{bounds}(?) &= [\perp, \top] \\
\text{bounds}(\ell) &= [\ell, \ell] \\
\text{bounds}(x_1 \lor x_2) &= \text{bounds}(x_1) \lor \text{bounds}(x_2) \\
\text{bounds}(x_1 \land x_2) &= \text{bounds}(x_1) \land \text{bounds}(x_2) \\
\text{bounds}(x_1 \setminus x_2) &= \text{bounds}(x_1) \setminus \text{bounds}(x_2) \\
\text{bounds}(F_1(x_1) \lor F_2(x_1)) &= \text{bounds}(F_1(x_1)) \lor \text{bounds}(F_2(x_1)) \\
\text{bounds}(F_1(x_1) \land F_2(x_1)) &= \text{bounds}(F_1(x_1)) \land \text{bounds}(F_2(x_1)) \\
\text{bounds}(F_1(x_1) \setminus F_2(x_1)) &= \text{bounds}(F_1(x_1)) \setminus \text{bounds}(F_2(x_1))
\end{align*}
\]

where $F_1 : \text{GLABEL}^n \to \text{GLABEL}$ and $F_2 : \text{GLABEL}^m \to \text{GLABEL}$.

\[
\begin{align*}
\mathcal{G}(F_1(g_1, \ldots g_n) \leq F_2(g_{n+1}, \ldots g_{n+m})) &= \langle [\ell_1, \ell_2, \ell_2'], \langle \ell_1 \lor \ell_2, \ell_1 \land \ell_2' \rangle \rangle
\end{align*}
\]

The algorithmic definition of meet:

\[
[\ell_1, \ell_2] \sqcap [\ell_3, \ell_4] = [\ell_1 \lor \ell_3, \ell_2 \land \ell_4] \quad \text{if valid}([\ell_1 \lor \ell_3, \ell_2 \land \ell_4])
\]

$\sqcap$ undefined otherwise

We calculate the algorithmic definition of $\Delta^\leq$:

\[
\begin{align*}
\Delta^\leq([\ell_1, \ell_2], [\ell_3, \ell_4], [\ell_5, \ell_6]) &= \langle [\ell_1 \lor \ell_3 \land \ell_5, \ell_1 \lor \ell_3 \lor \ell_5, \ell_4 \land \ell_6, \ell_4] \rangle
\end{align*}
\]

D.4.2 Type Evidences. We define a function $\text{liftP}()$ to transform functions over types into functions over labels. Also we define function $\text{invert}()$ to invert the operator on types, used in the domain and latent effect of function types. Finally we define function $\text{tomeet}()$ to transform type operators into meets, given the invariant property of references.

We start defining a pattern of operations:

\[
\begin{align*}
P^T &\in \text{GPATTERN}, P^\ell \in \text{LPATTERN} \\
P^T &::= _- | P^T \text{op}^T P^T \quad \text{(pattern on types)} \\
op^T &::= \lor | \land | \sqcap \quad \text{(operations on types)} \\
P^\ell &::= _- | P^\ell \text{op}^\ell P^\ell \quad \text{(pattern on labels)} \\
op^\ell &::= \lor | \land | \sqcap \quad \text{(operations on labels)}
\end{align*}
\]
where \( G \) is an argument,

We use case-based analysis to calculate the algorithmic rules for the initial evidence of consistent subtyping on gradual security types:

\[
\begin{align*}
G[\text{liftP}(G_1)(\overline{T_1}) &<: \text{liftP}(G_2)(\overline{T_2})] = \langle t_1, t_2 \rangle \\
G[G_1(\text{Bool}_n) &< G_2(\text{Bool}_m)] = \langle \text{Bool}_i, \text{Bool}_i \rangle \\
G[\text{invert}(G_2)(\overline{U_1}) &<: \text{invert}(G_1)(\overline{U_2})] = \langle \overline{E_{11}}, \overline{E_{11}} \rangle \\
G[G_1(\overline{U_{12}}) &< G_2(\overline{U_{12}})] = \langle \overline{E_{12}}, \overline{E_{22}} \rangle \\
G[\text{liftP}(G_1)(\overline{U_{11}}) &<: \text{liftP}(G_2)(\overline{U_{11}})] = \langle \overline{t_{11}}, \overline{t_{11}} \rangle \\
G[G_1(\overline{U_{12}}) &< G_2(\overline{U_{12}})] = \langle \overline{E_{11}}, \overline{E_{12}} \rangle \\
G[\text{tomeet}(G_1)(\overline{U_1}) &<: \text{tomeet}(G_2)(\overline{U_2})] = \langle \overline{E_{1}}, \overline{E_{1}} \rangle \\
G[G_1(\overline{U_1}) &< G_2(\overline{U_1})] = \langle \overline{E_{1}}, \overline{E_{1}} \rangle \\
G[G_1(\text{Ref}_{g_i}(\overline{U_1})) &< G_2(\text{Ref}_{g_j}(\overline{U_1}))] = \langle \overline{\text{Ref}_{g_i} E_1}, \overline{E_{1}} \rangle \\
\end{align*}
\]

where \( G_1 : \text{GLABEL}^n \rightarrow \text{GLABEL} \) and \( G_2 : \text{GLABEL}^m \rightarrow \text{GLABEL} \), and \( G_1(x_1, \ldots, x_n) = P_1(x_1, \ldots, x_n), \) \( G_2(x_1, \ldots, x_n) = P_2(x_1, \ldots, x_m) \).

We calculate a recursive meet operator for gradual types:

\[
\text{Bool}_i \cap \text{Bool}_j = \text{Bool}_{i \cap j}
\]

\[
(E_{11} \sqcap_{t_1} E_{12}) \cap (E_{21} \sqcap_{t_1} E_{22}) = (E_{11} \cap E_{21}) \sqcap_{t_1 \cap t_2} (E_{12} \cap E_{22})
\]

\[
\text{Ref}_i E_1 \cap \text{Ref}_j E_2 = \text{Ref}_{i \cap j} E_1 \sqcap E_2
\]

\( U \sqcap U' \) undefined otherwise.

We calculate a recursive definition for \( \Delta^< \) by case analysis on the structure of the second argument,
Δ ≤(t₁, t₂, t₃) = ⟨t', t₃’⟩

Δ ≤(bool₁, bool₂, bool₃) = ⟨bool₁, bool₂⟩

Δ ≤(E₁ ≤₁₁ E₁₂ E₁₃, E₂₁ E₂₂ E₂₃, E₃₁ E₃₂) = (E₁’ ≤₁₁ E₁₂ E₁₃, E₂₁ E₂₂ E₂₃ ≥₃₁ E₃₂)

D.4.3 Evidence inversion functions. The evidence inversion functions are defined as follows

\[ ilbl((\text{Bool}, \text{Bool})) = ⟨t₁, t₂⟩ \]

\[ ilbl((\text{Unit}, \text{Unit})) = ⟨t₁, t₂⟩ \]

\[ ilbl((\text{Ref}, \text{Ref})) = ⟨t₁, t₂⟩ \]

\[ ilbl((E₁ ≤₁₁ E₁₂ E₁₃, E₂₁ E₂₂ E₂₃) = ⟨t₁, t’₁⟩ \]

\[ iref((\text{Ref}, \text{E₁}, \text{E₂})) = \langle E₁, E₂ \rangle \]

\[ iref((\langle \text{E₁}, \text{E₂} \rangle) = \text{undefined otherwise} \]

\[ idom((E₁ ≤₁₁ E₁₂ E₁₃, E₂₁ E₂₂ E₂₃) = \langle E₁', E₁ \rangle \]

\[ idom((\langle \text{E₁}, \text{E₂} \rangle) = \text{undefined otherwise} \]

\[ icod((E₁ ≤₁₁ E₁₂ E₁₃, E₂₁ E₂₂ E₂₃) = \langle E₂, E₂ \rangle \]

\[ icod((\langle \text{E₁}, \text{E₂} \rangle) = \text{undefined otherwise} \]

D.5 Proofs

PROPOSITION D.13 (αᵢ is Sound). If \( \lambda \) is not empty, then \( \lambda \subseteq Y_i(\alpha(\lambda)) \).

PROOF. Suppose \( \lambda = \{ \lambda_i \} \). By definition of \( \alpha \), \( \alpha(\{ \lambda_i \}) = \lambda \lambda_i, \lambda \lambda_i \). Therefore

\[ Y_i(\alpha(\{ \lambda_i \})) = \{ \ell \mid \ell \in \text{LABEL}, \lambda \lambda_i < \ell < \lambda \lambda_i \} \]

And it is easy to see that if \( \ell \in \{ \lambda_i \} \), then \( \ell \in Y_i(\alpha(\{ \lambda_i \})) \), and therefore the result holds. \( \square \)

PROPOSITION D.14 (αᵢ is Optimal). If \( \lambda \) is not empty, and \( \lambda \subseteq Y_i(\lambda) \) then \( \alpha(\lambda) \subseteq \lambda \).

PROOF. By case analysis on the structure of \( i \). If \( i = [\ell_1, \ell_2], Y_i(\lambda) = \{ \ell \mid \ell \in \text{LABEL}, \ell_1 < \ell < \ell_2 \} \); \( \lambda \subseteq \{ \ell \mid \ell \in \text{LABEL}, \ell_1 < \ell < \ell_2 \} \), \( \lambda \neq \emptyset \) implies \( \alpha(\lambda) = [\ell_3, \ell_4] \), where \( \ell_1 < \ell_3 \) and \( \ell_4 < \ell_2 \), therefore \( [\ell_3, \ell_4] \subseteq \lambda \) if \( \lambda = \emptyset \), \( \alpha(\lambda) \) is undefined. \( \square \)

PROPOSITION D.15 (αₑ is Sound). If \( \text{valid}(\lambda) \) then \( \lambda \subseteq Y_e(\alpha_e(\lambda)) \).

PROOF. By well-founded induction on \( \lambda \). Similar to Prop C.3. \( \square \)
PROPOSITION D.16 (α_E is Optimal). If valid(S) and \( S \subseteq \gamma_E(E) \) then \( \alpha_E(S) \subseteq E \).

PROOF. By induction on the structure of U. Similar to Prop C.4.

PROPOSITION D.22. \( \gamma_i(t_1 \cap t_2) = \gamma_i(t_1) \cap \gamma_i(t_2) \).

PROOF.

\[
\gamma_i(t_1 \cap t_2) = \gamma_i(\alpha_i(\gamma_i(t_1) \cap \gamma_i(t_1))) \\
\subseteq \gamma_i(t_1) \cap \gamma_i(t_1) \quad (\text{soundness of } \alpha_i)
\]

Let \( \ell \in \gamma_i(t_1) \cap \gamma_i(t_2) \). We now that \( \gamma_i(t_1 \cap t_2) \) is defined. Suppose \( t_1 = [\ell_1, \ell_2] \) and \( t_2 = [\ell_3, \ell_4] \).

Therefore \( t_1 \cap t_2 = [\ell_1 \lor \ell_3, \ell_2 \land \ell_4] \).

But \( \gamma_i(t_1) \cap \gamma_i(t_1) = \{ \ell \mid \ell \in \text{LABEL}, \ell_1 \leq \ell \leq \ell_2 \} \cap \{ \ell \mid \ell \in \text{LABEL}, \ell_3 \leq \ell \leq \ell_4 \} \). Which is equivalent to \( \{ \ell \mid \ell \in \text{LABEL}, \ell_1 \leq \ell \leq \ell_2 \lor \ell_3 \leq \ell \leq \ell_4 \} \), equivalent to \( \{ \ell \mid \ell \in \text{LABEL}, \ell_1 \lor \ell_3 \leq \ell \leq \ell_2 \lor \ell_4 \} \). Which is by definition \( \gamma_i([\ell_1 \lor \ell_3, \ell_2 \land \ell_4]) \), and the result holds.

□

PROPOSITION D.23. \( \langle t_1, t_2 \rangle \circ^{\leq} \langle t_{22}, t_3 \rangle = \Delta^{\leq}(t_1, t_2 \cap t_{22}, t_3) \)

PROOF. Follows directly from the definition of consistent transitivity and Prop D.22.

□

PROPOSITION D.25. \( \gamma_E(E_1 \cap E_2) = \gamma_E(E_1) \cap \gamma_E(E_2) \).

PROOF. By induction on evidence types \( \epsilon_1 \) and \( \epsilon_2 \) and Prop D.22.

□

PROPOSITION D.26.

\[
\langle E_1, E_2 \rangle \circ^{\leq} \langle E_{22}, E_3 \rangle = \Delta^{\leq}(E_1, E_2 \cap E_{22}, E_3)
\]

where

\[
\Delta^{\leq}(E_1, E_2, E_3) = \alpha_i(\{ \langle S_1, S_3 \rangle \in \gamma_i(\langle E_1, E_3 \rangle) \mid \exists S_2 \in \gamma_i(\langle E_2 \rangle).S_1 \leq S_2 \land S_2 \leq S_3)\}
\]

PROOF. Follows directly from the definition of consistent transitivity and Prop D.25.

□

PROPOSITION D.31. If \( \epsilon_S \vdash U_1 \leq U_2 \) and \( \epsilon_1 \vdash g_1 \leq g_2 \) then \( \epsilon_S \lor \epsilon_1 \vdash U_1 \lor g_1 \vdash U_2 \lor g_2 \)

PROOF. By induction on types \( U_1 \) and \( U_2 \), using the definition of \( \mathcal{G}_{\leq} \), and Proposition 6.13.

□

PROPOSITION D.36. \( [\ell_1, \ell_2] \lor [\ell_3, \ell_4] = [\ell_1 \lor \ell_3, \ell_2 \lor \ell_4] \)

PROOF. Follows directly by definition of \( \gamma \) and \( \lor \).

□

PROPOSITION D.37.

\[
\langle t_1, t_2 \rangle \lor \langle t_1', t_2' \rangle = \langle t_1 \lor t_1', t_2 \lor t_2' \rangle
\]

PROOF. Follows directly from the definition of consistent join monotonicity and Prop D.36.

□

PROPOSITION D.38.

\[
[\ell_1, \ell_2] \cap [\ell_3, \ell_4] = [\ell_1 \lor \ell_3, \ell_2 \land \ell_4] \quad \text{if } \ell_1 \lor \ell_3 \leq \ell_2 \land \ell_4
\]

\[
1 \cap 1' \text{ undefined otherwise}
\]

PROOF. By definition of meet:

\[
[\ell_1, \ell_2] \cap [\ell_3, \ell_4] = \alpha_i(\{ \ell' \mid \ell' \in \gamma([\ell_1, \ell_2]) \cap \gamma([\ell_3, \ell_4]))
\]

But by definition of intersection on intervals, \( \gamma([\ell_1, \ell_2]) \cap \gamma([\ell_3, \ell_4]) = \gamma([\ell_1 \lor \ell_3, \ell_2 \land \ell_4]) \) if \( \ell_1 \lor \ell_3 \leq \ell_2 \land \ell_4 \) (otherwise the intersection is empty), and the result follows by definition of \( \alpha_i \).

□
PROPOSITION D.39.

\[\ell_1 \preceq \ell_4 \quad \ell_3 \preceq \ell_6 \quad \ell_1 \preceq \ell_6\]

\[\Delta^{\kappa}([\ell_1, \ell_2], [\ell_3, \ell_4], [\ell_5, \ell_6]) = \langle [\ell_1, \ell_2 \land \ell_4 \land \ell_6], [\ell_1 \lor \ell_3 \lor \ell_5, \ell_6] \rangle\]

PROOF. By definition:

\[\Delta^{\kappa}([\ell_1, \ell_2], [\ell_3, \ell_4], [\ell_5, \ell_6]) = \alpha_c(\{\langle \ell_1', \ell_4' \rangle \in y_\alpha([\ell_1, \ell_2], [\ell_3, \ell_4]) \mid \exists \ell_1'' \in y_\alpha([\ell_3, \ell_4]). \ell_1' \preceq \ell_2' \preceq \ell_4'\})\]

It is easy to see that \(\alpha_c(\{\ell_1'\}) = [\ell_1, \ell_1']\), for some \(\ell_1'\). We know that \(\ell_1' \preceq \ell_2, \ell_1' \preceq \ell_4\) and \(\ell_1' \preceq \ell_6\), i.e. \(\ell_1' \preceq \ell_2 \land \ell_4 \land \ell_6\). But \(\ell_2 \land \ell_4 \land \ell_6 \preceq \ell_4 \preceq \ell_6\) therefore

\[\langle \ell_2 \land \ell_4 \land \ell_6, \ell_6 \rangle \in \{\langle \ell_1', \ell_4' \rangle \in y_\alpha([\ell_1, \ell_2], [\ell_3, \ell_4]) \mid \exists \ell_1'' \in y_\alpha([\ell_3, \ell_4]). \ell_1' \preceq \ell_2' \preceq \ell_3'\}\]

and by definition of \(\alpha_c, \ell_2 \land \ell_4 \land \ell_6 \preceq \ell_1'\), then \(\alpha_c(\{\ell_1'\}) = [\ell_1, \ell_2 \land \ell_4 \land \ell_6].\) Similar argument is used to prove that \(\alpha_c(\{\ell_3'\}) = [\ell_1 \lor \ell_3 \lor \ell_5, \ell_6].\)

\[\square \]

LEMMA D.40. Let \(\ell_i \in \text{LABEL},\) then \((\ell_1 \land \ell_2) \triangleright ((\ell_3 \land \ell_4) \preceq (\ell_1 \lor \ell_3) \land (\ell_2 \lor \ell_4)).\)

PROOF. Suppose \(\ell_1 \preceq F_1(\overline{\gamma}) \preceq F_2(\overline{\gamma})\) and \(\ell_2 \preceq F_2(\overline{\gamma}) \preceq F_3(\overline{\gamma}).\)

If \(\ell_1 \triangleright \ell_2\) is defined, then \(\ell_1 \triangleright \ell_2 \triangleright F_1(\overline{\gamma}) \preceq F_3(\overline{\gamma}).\)

PROOF. Suppose \(\bar{\epsilon}_1 = \langle t_{11}, t_{12} \rangle\) and \(\bar{\epsilon}_2 = \langle t_{21}, t_{22} \rangle.\) Then by definition of initial evidence:

\[\langle t_{11}, t_{12} \rangle = \langle [\ell_1, \ell_2], [\ell_3, \ell_4] \rangle \sqsubseteq \mathcal{G}[F_1(\overline{\gamma}) \preceq F_2(\overline{\gamma})] = \langle t_{11}', t_{12}' \rangle\]

and

\[\langle t_{21}, t_{22} \rangle = \langle [\ell_5, \ell_6], [\ell_7, \ell_8] \rangle \sqsubseteq \mathcal{G}[F_2(\overline{\gamma}) \preceq F_3(\overline{\gamma})] = \langle t_{21}', t_{22}' \rangle\]

Suppose that \(\mathcal{G}[F_1(\overline{\gamma}) \preceq F_3(\overline{\gamma})] = \langle t_{11}', t_{12}' \rangle.\) We have to prove that \(\langle t_{11}, t_{12} \rangle \triangleright \langle t_{21}, t_{22} \rangle \sqsubseteq \langle t_{11}', t_{12}' \rangle.\)

If \(\text{bounds}(F_1(\overline{\gamma})) = [\ell_1', \ell_2'], \text{bounds}(F_2(\overline{\gamma})) = [\ell_3', \ell_4'],\) and \(\text{bounds}(F_3(\overline{\gamma})) = [\ell_5', \ell_6']\) We know that

\[\mathcal{G}[F_1(\overline{\gamma}) \preceq F_2(\overline{\gamma})] = \langle [\ell_1', \ell_2' \land \ell_4'], [\ell_1' \lor \ell_3', \ell_4'] \rangle.\] Therefore \(\ell_1' \preceq \ell_1, \ell_2' \preceq \ell_2 \land \ell_4', \ell_1' \lor \ell_3' \preceq \ell_3\) and \(\ell_4' \preceq \ell_4'.\)

Using the same argument,

\[\mathcal{G}[F_2(\overline{\gamma}) \preceq F_3(\overline{\gamma})] = \langle [\ell_5', \ell_6' \land \ell_6'], [\ell_5' \lor \ell_5', \ell_6'] \rangle.\] Therefore \(\ell_5' \preceq \ell_5, \ell_6' \preceq \ell_4' \land \ell_5', \ell_5' \lor \ell_5' \preceq \ell_7\) and \(\ell_8 \preceq \ell_6'.\)

But \(\mathcal{G}[F_1(\overline{\gamma}) \preceq F_3(\overline{\gamma})] = \langle [\ell_1', \ell_2' \land \ell_6'], [\ell_1' \lor \ell_5, \ell_6'] \rangle\)

and

\[\langle t_{11}, t_{12} \rangle \triangleright \langle t_{21}, t_{22} \rangle = \Delta^{\kappa}(t_{11}, t_{12} \sqcap t_{21}, t_{22}) = \Delta^{\kappa}(\ell_1, \ell_2, [\ell_3 \lor \ell_5, \ell_4 \land \ell_6], [\ell_7, \ell_8]) = (\ell_1, \ell_2 \land \ell_4 \land \ell_6 \land \ell_8, \ell_1 \lor \ell_3 \lor \ell_5 \lor \ell_7, \ell_8)\]
we need to prove that
\[
\langle [\ell_1, \ell_2 \land \ell_4 \land \ell_6 \land \ell_8], [\ell_1 \lor \ell_3 \lor \ell_5 \lor \ell_7, \ell_8] \rangle \models \\
\langle [\ell_1', \ell_2' \land \ell_4', \ell_6], [\ell_1' \lor \ell_3', \ell_5', \ell_6'] \rangle
\]
But we know that $\ell_1' \preceq \ell_1$. Also that $\ell_2 \preceq \ell_2' \land \ell_1'$ and therefore $\ell_2 \preceq \ell_2'$. The same for $\ell_6 \preceq \ell_6'$ and therefore $\ell_2 \land \ell_4 \land \ell_6 \land \ell_8 \preceq \ell_2' \land \ell_6'$, i.e., $[\ell_1, \ell_2 \land \ell_4 \land \ell_6 \land \ell_8] \models [\ell_1', \ell_2' \land \ell_6']$. The argument is applied for the second components and the result holds.

\[\square\]

**Proposition 6.13.** Suppose $\varepsilon_1 \vdash F_{11}(\overrightarrow{g}) \preceq F_{12}(\overrightarrow{g})$ and $\varepsilon_2 \vdash F_{21}(\overrightarrow{g}) \preceq F_{22}(\overrightarrow{g})$

Then $\varepsilon_1 \lor \varepsilon_2 \vdash F_{11}(\overrightarrow{g}) \lor F_{21}(\overrightarrow{g}) \preceq F_{12}(\overrightarrow{g}) \lor F_{22}(\overrightarrow{g})$

**Proof.** By definition of initial evidence noticing that $\varepsilon_1 \lor \varepsilon_2$ can be more precise than the initial evidence of judgment

Suppose $\varepsilon_1 = \langle [\ell_1, \ell_2], [\ell_3, \ell_4] \rangle$, and $\varepsilon_2 = \langle [\ell_5, \ell_6], [\ell_7, \ell_8] \rangle$, then $\varepsilon_1 \lor \varepsilon_2 = \langle [\ell_1 \lor \ell_5, \ell_2 \lor \ell_6], [\ell_3 \lor \ell_7, \ell_4 \lor \ell_8] \rangle$.

If $\text{bounds}(F_{11}(\overrightarrow{g})) = [\ell_{111}, \ell_{112}]$, $\text{bounds}(F_{12}(\overrightarrow{g})) = [\ell_{121}, \ell_{122}]$, and $\text{bounds}(F_{22}(\overrightarrow{g})) = [\ell_{221}, \ell_{222}]$, we have

We know that $\mathcal{J}[F_{11}(\overrightarrow{g}) \preceq F_{12}(\overrightarrow{g})] = \langle [\ell_{111}, \ell_{112} \land \ell_{122}], [\ell_{111} \lor \ell_{121}, \ell_{122}] \rangle$. Therefore $\ell_{111} \preceq \ell_1$, $\ell_2 \preceq \ell_{112} \land \ell_{122}$, $\ell_{111} \lor \ell_{121} \preceq \ell_3$ and $\ell_4 \preceq \ell_{122}$. Using the same argument, $\mathcal{J}[F_{21}(\overrightarrow{g}) \preceq F_{22}(\overrightarrow{g})] = \langle [\ell_{211}, \ell_{212} \land \ell_{222}], [\ell_{211} \lor \ell_{221}, \ell_{222}] \rangle$. Therefore $\ell_{211} \preceq \ell_5$, $\ell_6 \preceq \ell_{212} \land \ell_{222}$, $\ell_{211} \lor \ell_{221} \preceq \ell_7$ and $\ell_8 \preceq \ell_{222}$.

But the $\mathcal{J}[F_{11}'(\overrightarrow{g}) \preceq F_{12}'(\overrightarrow{g})] = \langle [\ell_1', \ell_2' \land \ell_4'], [\ell_1' \lor \ell_3', \ell_4'] \rangle$ where $\text{bounds}(F_{11}'(\overrightarrow{g})) = [\ell_{111}', \ell_{112}'][\ell_{121}', \ell_{122}']$ and

\[\text{bounds}(F_{22}'(\overrightarrow{g})) = [\ell_{221}', \ell_{222}'] \text{ bounds}(F_{12}(\overrightarrow{g})) \lor \text{bounds}(F_{22}(\overrightarrow{g})) = [\ell_{211}', \ell_{212}'][\ell_{221}', \ell_{222}'] \]

We need to prove that $[\ell_1 \lor \ell_5, \ell_2 \lor \ell_6] \models [\ell_{121}', \ell_{122}'][\ell_{121}', \ell_{122}']$. But $\ell_{111} \preceq \ell_1$ and $\ell_{211} \preceq \ell_5$, therefore $\ell_{111} \lor \ell_{211} \preceq \ell_1 \lor \ell_5$. Similarly, as $\ell_2 \preceq \ell_{112} \land \ell_{122}$ and $\ell_6 \preceq \ell_{212} \land \ell_{222}$, then $\ell_2 \lor \ell_6 \preceq \ell_{112} \lor \ell_{212}$. Therefore $[\ell_1 \lor \ell_5, \ell_2 \lor \ell_6] \models [\ell_{111} \lor \ell_{211}, \ell_{112} \lor \ell_{212}]$.

Using analogous argument, we also know that $[\ell_3 \lor \ell_7, \ell_4 \lor \ell_8] \models [\ell_{211} \lor \ell_{221}, \ell_{122} \lor \ell_{222}]$. Therefore $\varepsilon_1 \lor \varepsilon_2 \models \mathcal{J}[F_{11}'(\overrightarrow{g}) \preceq F_{12}'(\overrightarrow{g})]$, and the result holds.

\[\square\]

**Lemma D.41.** Let $S_1, S_2 \in \text{TYPE}$. Then

1. If $(S_1 \triangleright S_2)$ is defined then $S_1 \triangleleft (S_1 \triangleright S_2)$.
2. If $(S_1 \nabla S_2)$ is defined then $(S_1 \nabla S_2) \triangleleft S_1$.

**Proof.** We start by proving (1) assuming that $(S_1 \triangleright S_2)$ is defined. We proceed by case analysis on $S_1$.

**Case (Boolean).** If $S_1 = \text{Bool}_{\ell_1}$ then as $(S_1 \triangleright S_2)$ is defined then $S_2$ must have the form $\text{Bool}_{\ell_2}$ for some $\ell_2$. Therefore $(S_1 \triangleright S_2) = \text{Bool}_{\ell_1 \lor \ell_2}$. But by definition of $\preceq$, $\ell_1 \preceq (\ell_1 \lor \ell_2)$ and therefore we use \((\triangleleft_{\text{bool}}\) to conclude that $\text{Bool}_{\ell_1} \triangleleft \text{Bool}_{\ell_1 \lor \ell_2}$, i.e., $S_1 \triangleleft (S_1 \triangleright S_2)$.

**Case ($S \rightarrow \ell \ S$).** If $S_1 = S_{11} \rightarrow_{\ell_1} S_{12}$ then as $(S_1 \triangleright S_2)$ is defined then $S_2$ must have the form $S_{21} \rightarrow_{\ell_2} S_{22}$ for some $S_{21}, S_{22}$ and $\ell_2$.

We also know that $(S_1 \triangleright S_2) = (S_{11} \land S_{21}) \rightarrow_{(\ell_1 \lor \ell_2)} (S_{12} \land S_{22})$. By definition of $\preceq$, $\ell_1 \preceq (\ell_1 \lor \ell_2)$. Yes, it holds.
Also, as \((S_1 \triangledown S_2)\) is defined then \((S_{11} \land S_{21})\) is defined. Using the induction hypothesis of (2) on \(S_{11}\), \((S_{11} \land S_{21}) \leftarrow S_1\). Also, using the induction hypothesis of (1) on \(S_{12}\) we also know that \(S_{12} \leftarrow (S_{12} \land S_{22})\). Then by \(<\ldots\) we can conclude that \(S_{11} \rightarrow \ell_1\), \(S_{12} \leftarrow (S_{11} \land S_{21}) \rightarrow (\ell_1 \lor \ell_2)\) \((S_{12} \land S_{22})\), i.e. \(S_1 \leftarrow (S_1 \triangledown S_2)\).

The proof of (2) is similar to (1) but using the argument that \(\langle \ell_1 \land \ell_2 \rangle \leq \ell_1\). □

**Lemma D.42.** Let \(S \in \text{TYPE}\) and \(\ell \in \text{LABEL}\). Then \(S \leftarrow S \lor \ell\).

**Proof.** Straightforward case analysis on type \(S\) using the fact that \(\ell \leq (\ell' \lor \ell)\) for any \(\ell'\). □

**Lemma D.43.** Let \(S_1, S_2 \in \text{TYPE}\) such that \(S_1 \leftarrow S_2\), and let \(\ell_1, \ell_2 \in \text{LABEL}\) such that \(\ell_1 \leq \ell_2\). Then \(S_1 \lor \ell_1 \leftarrow S_2 \lor \ell_2\).

**Proof.** Straightforward case analysis on type \(S\) using the definition of label stamping on types. □

# E GSL\(_{Ref}\): Dynamic Properties

Notice that for convenience, the proofs and properties are defined over intrinsic terms [Garcia et al. 2016] instead of terms of the internal language. They are actually the same as terms of the internal language, but keeping all static annotations explicitly. First we introduce the static semantics of intrinsic terms in Sec. E.1. Their dynamic semantics in Sec. E.2. The relation between intrinsic and evidence-augmented terms in Sec. E.3. Then the proof of type safety is presented Sec. E.4, the proof of dynamic gradual guarantee for GSL\(_{Ref}\) without the specific check in rule \((r7)\) in section E.5, and the proof of noninterference in Sec. E.6.

## E.1 Intrinsic Terms: Static Semantics

Following Garcia et al. [2016], we develop _intrinsically typed_ terms [Church 1940]: a term notation for gradual type derivations. These terms serve as our internal language for dynamic semantics: they play the same role that cast calculi play in typical presentations of gradual typing [Siek and Taha 2006]. Intrinsically-typed terms \(t^U\) comprise a family \(\mathbb{T}[U]\) of type-indexed sets, such that ill-typed terms do not exist. They are built up from disjoint families \(x^U \in V[U]\) and \(o^U \in L[U]\) of intrinsically typed variables and locations respectively. Unless required, we omit the type exponent on intrinsic terms, writing \(i \in \mathbb{T}[U]\).

To each typing rule corresponds an intrinsic term formation rule that captures all the information needed to ensure that an intrinsic term is isomorphic to a typing derivation. Because intrinsic variables and locations reflect their typings, intrinsic terms do not need explicit type environments \(\Gamma\) or store environments \(\Sigma\); however, the typing judgment depends on a security effect \(g_c\), which intrinsic terms must account for.

Additionally, because intrinsic terms represent typing derivations of programs _as they reduce_, they must account for the possibility that runtime values have more precise types than those used in the original typing derivation. For instance, the term in function position of an application can be a subtype of the function type used to type-check the program originally. The formation rule of the application intrinsic term must permit this extra subtyping leeway, justified by evidence. The same holds for the security information. Therefore, an intrinsic term has the general form \(\phi \triangleright i\), where the context information \(\phi \triangleright (\varepsilon g_c, g_c)\) contains the static program counter label \(g_c\) used to type-check the source term, as well as the runtime program counter label \(g_c\), along with the evidence \(\varepsilon \triangleright g_c \leq g_c\).\(^\dagger\) For simplicity we define accessors \(\phi.g_c \leq g_c\) and \(\phi.\varepsilon \leq \varepsilon\).

\(^\dagger\)We use color to make distinctions when is needed: green is for effects and static information; orange is for the runtime information of the security effect.
\[ \varepsilon \in \text{Evidence}, \quad et \in \text{EvTerm}, \quad ev \in \text{EvValue}, \quad v \in \text{Value}, \quad u \in \text{SimpleValue}, \quad g \in \text{EvFrame}, \quad f \in \text{TmFrame} \]

\[
\begin{align*}
\phi & ::= x^U | b_g | (\lambda \theta x^U.g)_g | o^U | \text{unit}_g \\
v & ::= u | \epsilon \cdot u :: U \\
f & ::= h[\varepsilon] \\
\mu & ::= \mu \cdot \mu, a^U \mapsto v \\
p & ::= x^U | o^U \\
q & ::= p | \eta p :: U \\
\end{align*}
\]

\[ \varepsilon ::= (E_1, E_2) | (t_1, t_2) \]

**Fig. 33.** GSLRef: Syntax of the Intrinsic Term Language

\[
\begin{align*}
(\text{lx}) \quad & \phi \triangleright x^U \in T[U] \\
(\text{lb}) \quad & \phi \triangleright b_g \in T[\text{Bool}_g] \\
(\text{lu}) \quad & \phi \triangleright \text{unit}_g \in T[\text{Unit}_g] \\
(\text{ll}) \quad & \phi \triangleright o^U \in T[\text{Ref}_g U] \\
(\text{lll}) \quad & \phi' \triangleright \tilde{I} \in T[U'] \\
(\text{lref}) \quad & \phi \triangleright \text{Ref}_g U \in T[U] \\
(\text{lapp}) \quad & \phi \triangleright \tilde{I}_1 \in T[U_1] \\
(\text{lif}) \quad & \phi \triangleright \tilde{I}_1 \in T[U'] \\
(\text{lir}) \quad & \phi \triangleright \tilde{I}_1 \in T[\text{Ref}_g U_1'] \\
(\text{lar}) \quad & \phi \triangleright \tilde{I}_1 \in T[\text{Ref}_g U_1] \\
(\text{laref}) \quad & \phi \triangleright \text{Ref}_g U \tilde{I} \in T[U \text{\triangledown g}] \\
\end{align*}
\]

\[ \varepsilon_1 \vdash U' \leq U \quad \varepsilon_2 \vdash g \cdot g' \leq g \]

**Fig. 34.** GSLRef: Gradual Intrinsic Terms

Figure 33, presents the syntax of intrinsic terms. Fig. 34 presents the intrinsic terms formation rules for GSLRef. In rule (lprot), labels \( g \) and \( g' \) represent the static and dynamic information of the label used to increase the program counter label in the subterm, respectively. Evidence \( \varepsilon_1 \) justifies that the type of the subterm is a consistent subtype of \( U \), the static type of the subterm. \( \phi' \) represents
the context information associated to the subterm $\bar{\phi}$. $\phi^\prime(g_c)$ (resp. $\phi^\prime(g_c)$) is the program counter label used to typecheck (resp. evaluate) $\bar{\phi}$.

In the intrinsic term formation rule for applications (Iapp), $U_1$ is the runtime type of the function term. We annotate the initial static type information with $\triangledown$. The evidence $e_2$ for the label ordering premise is also annotated, since it is needed to reconstruct the derivation. The intrinsic term of a conditional, described in Rule (Iif)\(^{20}\), carries the static information of the label of the conditional term $g$. The context information $\phi^\prime$ used for both branches is obtained by joining the term context $\phi$ point-wise with the evidence and labels associated with the consistent subtyping judgment of the conditional. Evidences $e_2$ and $e_3$ justify that the type of each branch is a consistent subtype of the join of both types. Finally, rule (Iassgn) is built similarly to the application rule (Iapp).

### E.2 Intrinsic Terms: Dynamic Semantics

Next we present the full definition of the intrinsic reduction rules in Figure 35, and the full definition of notions of intrinsic reduction in Figure 36.

Because the security context information of a term is maintained at each step, we also adopt the lightweight notation $\bar{\mu}_1 \vdash \bar{\phi} \bar{\mu}_2$, to denote the reduction of the intrinsic term $\phi \triangledown g_c \bar{\mu}_1 \in T[U]$ in store $\mu_1$ to the intrinsic term $\phi \triangledown g_c \bar{\mu}_2 \in T[U]$ in store $\mu_2$. We note $C[U]$ the combination of a term $\bar{\mu}_1 \in T[U]$ (without context) and a store $\mu$. Function applications reduce to to an error if consistent transitivity fails to justify $U_2 < U_1$. Conditionals similarly reduce to a new prot term, which is constructed using the static and dynamic information of the conditional term. Assignments may reduce to an ascribed unit value. Similarly to references, the stored value is ascribed the statically determined type $U$. Therefore consistent transitivity may fail to justify that the actual type of the stored value is a subtype of $U$. As the value is stamped with actual labels, the term may also reduce to an error if consistent transitivity cannot support the judgment $\phi \triangledown g_c \triangledown \ell \triangleleft U$.

### E.3 Relating Intrinsic and Evidence-augmented Terms

In this section we present the translation rules from GSL\(_{\text{Ref}}\) terms to intrinsic terms in Figure 37. Also this section presents the erasure function in in Figure 38—highlighting the syntactics differences between terms in gray—along properties that relates evidence-augmented terms and intrinsic terms.

In particular we identify four important properties. First, that given a source language the erasure of the translation to intrinsic term is equal to the translation of the source term to an evidence-augmented term:

**Proposition E.1.** If $\Gamma; \Sigma; g_c \vdash t \leadsto \bar{\phi} \bar{\mu}_1 : U$ and $\Gamma; \Sigma; g_c \vdash t \leadsto t^\prime : U$, then $|\bar{\phi} \bar{\mu}_1| = |t^\prime|$.  

**Proof.** By induction on the type derivation of $t$. \(\Box\)

Second, given a reducible intrinsic term $\bar{\phi}$, if it reduces to an error, then it erasure also reduces to an error; or, if reduces to an intrinsic term $\bar{\mu}_1$, then the erasure of $\bar{\mu}_1$ also reduces to the erasure of $\bar{\mu}_1^\prime$:

**Proposition E.2.** Consider $\phi = !g_c, \phi \triangledown \bar{\phi} \bar{\mu}_1 \in T[U]$, and $\Gamma; \Sigma; g_c \vdash t : U$, such that $\Sigma \triangledown \mu_2$. Then if $\bar{\phi} = t$ and $\mu_1 = \mu_1^\prime$ then either

- $\bar{\phi} \bar{\mu}_1 \rightarrow_{\phi} \bar{\phi} \bar{\mu}_2 | |\mu_2 | \rightarrow_{\phi} \bar{\phi} \bar{\mu}_1^\prime | |\mu_2^\prime$, or
- $\bar{\phi} \bar{\mu}_1 \rightarrow_{\phi} \text{error} | |\mu_2 | \rightarrow_{\phi} \text{error}$

**Proof.** By induction on the type derivation of $\bar{\phi}$.

---

\(^{20}\)Evidence inversion functions ($\text{idom}$, $\text{icod}$, $\text{iref}$, $\text{ilbl}$ and $\text{ilat}$) manifest the evidence for the inversion principles on consistent subtyping judgments; e.g. starting from the evidence that $U_1 \triangleleft U_2$, $\text{ilbl}$ produces the evidence of the judgment $\text{label}(U_1) \triangleleft \text{label}(U_2)$. 

\[
\phi \mapsto \epsilon; \ C[U] \times (C[U] \cup \{\text{error}\})
\]

Case (I:\). Then \( \bar{i} = \epsilon \bar{i}' :: U \) and by (\( \text{E}_{\bar{i}} \)), \( t = \epsilon \bar{i}' \) for some \( \bar{t}' \) such that \( \bar{i}' = \bar{t}' \). Suppose that \( \epsilon_1 \vdash U' \subseteq U \). By inspection on the type derivations, \( \phi \mapsto \bar{i}' \in T[U'] \) and \( \vdash \Sigma; \epsilon g_c \vdash \bar{t}' : U' \).

Let us suppose that \( \bar{i}' \mid \mu_1 \xrightarrow{\phi} \bar{i}'' \mid \mu_2 \), then by induction hypothesis \( t' \mid \mu_2 \xrightarrow{\epsilon g_c} t'' \mid \mu'_2 \) and \( \bar{i}'' = \bar{t}'' \) and \( \mu'_1 = \mu'_2 \). Then \( \epsilon_1 \bar{i}' :: U \mid \mu_1 \xrightarrow{\phi} \epsilon_1 \bar{i}'' :: U \mid \mu_1' \) and \( \epsilon_1 \bar{t}' : \mu_2 \xrightarrow{\epsilon g_c} \epsilon_1 \bar{t}' : \mu_2' \). But as \( \mu_1' = \mu_2' \) and by (\( \text{E}_{\bar{i}} \)) \( \epsilon_1 \bar{i}'' :: U = \epsilon_1 \bar{t}'' \), the result holds.

Let us suppose now that \( \bar{i}' = \epsilon_2 \bar{u} :: U' \). Then as \( \bar{i}' = \bar{t}' = \epsilon_2 \bar{u}' \), for some \( \bar{u}' \) such that \( u = u' \). If \( \epsilon_2 \circ \epsilon_1 = \epsilon' \), then \( \epsilon_1 (\epsilon_2 \bar{u} :: U') :: U \mid \mu_1 \xrightarrow{\phi} \epsilon' \bar{u} :: U \mid \mu_1 \) and \( \epsilon_1 (\epsilon_2 \bar{u}') \mid \mu_2 \xrightarrow{\epsilon g_c} \epsilon' \bar{u}' \mid \mu_2 \). But as \( \mu_1 = \mu_2 \), and by (\( \text{E}_{\bar{i}} \)) \( \epsilon' \bar{u}' = \epsilon' \bar{u}' \), the result holds.

If \( \bar{i}' = u \), then as \( \bar{i}' = \bar{t}' = \epsilon_2 \bar{u}' \), for some \( \bar{u}' \) such that \( u = u' \), and the result holds immediately.

The other cases proceed analogous.

Fourth, if an intrinsic term type checks, then its erasure also type checks to the same type.

**PROPOSITION E.3.** Consider \( \phi \mapsto \bar{i} \in T[U] \) then, for \( \Gamma \models \bar{i} \) and \( \Sigma \models \bar{i}, \Gamma, \Sigma; |\phi| \vdash |\bar{i}| : U \).

**PROOF.** By induction on the type derivation of \( \bar{i} \).

Finally, if an evidence-augmented term type checks, then there must exists some intrinsic term that have the same type and that it erasure is the original evidence-augmented term.

**PROPOSITION E.4.** Consider \( \Gamma; \Sigma; \epsilon g_c \vdash t : U \). Then \( \exists ! \bar{i}, \exists ! \phi \) such that \( |\bar{i}| = t \) and \( |\phi| = \epsilon g_c \) and \( \phi \mapsto \bar{i} \in T[U] \)

**PROOF.** By induction on the type derivation of \( t \).
Consider the other cases proceed analogous. □

Lemma E.5. Consider $\phi \triangleright \bar{t}_1 \in T[U]$. If $\bar{t}_1 \subseteq \bar{t}_2$ then $|\bar{t}_1| \subseteq |\bar{t}_2|$. 

\[ \phi \rightarrow: C[U] \times (C[U] \cup \{ \text{error} \}) \]
Fig. 37. GSLRef: translation to GSLRef intrinsic terms

\[ \begin{align*}
\text{(Tx)} & \quad \Gamma(x) = U \\
\text{(Tu)} & \quad \Gamma; \Sigma; g_c + \text{unit}_g \leadsto \text{unit}_g : \text{Unit}_g \\
\text{(Ta)} & \quad \Gamma; \Sigma; g' + t \leadsto i : U_2 \\
\text{(T@)} & \quad \Gamma; \Sigma; g_c + t_1 \leadsto \tau_1 : \text{Bool}_{g_1} \\
\text{(Tapp)} & \quad \Gamma; \Sigma; g_c + t_1 \leadsto \tau_1 : U_{11} \xrightarrow{=} g U_{12} \\
\text{(Tref)} & \quad \Gamma; \Sigma; g_c + \text{ref} U \leadsto \text{ref}_U t \leadsto \text{ref}_U i : \text{Ref}_U \\
\text{(T.:)} & \quad \Gamma; \Sigma; g_c + t \leadsto \tau_1 : U_1 \\
\text{Proof.} \quad \text{By induction on the type derivation of } \tilde{i}_1 \text{ and the definition of } [\cdot].
\end{align*} \]

\[ \begin{align*}
\text{Lemma E.6. Consider } \phi \triangleright \tilde{i}_1 \in \mathcal{T}[U]. \text{ If } [\tilde{i}_1] \subseteq \tilde{t}_2, \text{ then } \exists \tilde{i}_2, \text{ such that } \tilde{i}_1 \subseteq \tilde{i}_2 \text{ and that } [\tilde{i}_2] = \tilde{t}_2.
\end{align*} \]

\[ \text{Proof. By induction on } \tilde{i}_1 \text{ and the definition of } [\cdot]. \]

\[ \text{Case (I.:)} \quad \text{Then } \tilde{i}_1 = \epsilon_1 \tilde{i}_1' = U, \text{ and } [\tilde{i}_1] = \epsilon_1[\tilde{i}_1']. \quad \text{By definition of } [\cdot], \text{ } \tilde{t}_2 \text{ has the form } \epsilon_2 \tilde{t}_2', \text{ where } \epsilon_2 \subseteq \epsilon_2 \text{ and } [\tilde{i}_1'] \subseteq t_2'. \text{ By induction hypothesis, } \exists \tilde{i}_2 \text{ such that } \tilde{i}_1' \subseteq \tilde{i}_2' \text{ and that } [\tilde{i}_2'] = \tilde{t}_2'. \text{ By definition of evidence, we can build the term } \epsilon_2 \tilde{i}_2' : ?, \text{ but we know that } \epsilon_1 \tilde{i}_1' : U \not\subseteq \epsilon_2 \tilde{i}_2' : ? \text{ and that } [\epsilon_2 \tilde{i}_2'] = [\epsilon_2 \tilde{i}_2'] = \epsilon_2 \tilde{i}_2'. \quad \text{The other cases proceed analogous.} \]
Also, the store must preserve types between intrinsic locations and underlying values.

In this section we present the proof of type safety for GSL with that depends on the security effect.

Proof.

Lemma E.10 (Canonical forms). Consider a value \( v \in T[U] \). Then either \( v = u \), or \( v = e u :: U \) with \( u \in T[U'] \) and \( e :: U' \leq U \). Furthermore:

(1) If \( U = \text{Bool}\_g \) then either \( v = b_g \) or \( v = e b_g :: \text{Bool}\_g \) with \( b_g \in T[\text{Bool}\_g'] \) and \( e :: \text{Bool}\_g' \leq \text{Bool}\_g \).
If \( U = U_1 \overset{\gamma_c}{\rightarrow} U_2 \) then either \( \nu = (\eta \times U_1, U_2)_\gamma \) with \( U_2 \in \mathbb{T}[U_2] \) or \( \nu = \epsilon(\eta \times U_1, U_2)_\gamma \) :: 
\[ U_1 \overset{\gamma_c}{\rightarrow} U_2 \) with \( U_1 \overset{\gamma_c}{\rightarrow} U_2 \leq U_1 \overset{\gamma_c}{\rightarrow} U_2 \).

If \( U = \text{Ref}_g U_1 \) then either \( \nu = o(U_1) \) or \( \nu = \epsilon o(U_1) \) :: \( \text{Ref}_g U_1 \) with \( o(U_1) \in \text{Ref}_g U_1 \) and \( \epsilon \mapsto \text{Ref}_g U_1 \).

**Proof.** By direct inspection of the formation rules of gradual intrinsic terms (Figure 34).

**Lemma E.11 (Substitution).** If \( \phi \mapsto t^U \in \mathbb{T}[U] \) and \( \phi \mapsto \nu \in \mathbb{T}[U] \), then \( \phi \mapsto [\nu/x] \) :: \( t^U \in \mathbb{T}[U] \).

**Proof.** By induction on the derivation of \( \phi \mapsto t^U \).

**Proposition E.12 (\( \mapsto \) is well defined).** If \( \nu^U \mid \mu \mapsto r \) and \( t^U \mid \mu \mapsto \mu' \), then \( r \in \text{Config}_U \cup \{ \text{error} \} \) and if \( r = t^U \mid \mu' \), then \( t^U \mid \mu' \) and \( \text{dom}(\mu) \subseteq \text{dom}(\mu') \).

**Proof.** By induction on the structure of a derivation of \( t^U \mid \mu \mapsto r \), considering the last rule used in the derivation.

**Case (l\( \oplus \)).** Then \( t^U = b_{1\ell_1} \oplus^g b_{2\ell_2} \). By construction we can suppose that \( g = g_1 \wedge g_2 \), then

\[
\begin{align*}
\phi \cdot \epsilon \mapsto \phi \cdot g_c \leq \phi \cdot g_c \\
\phi \mapsto b_{1\ell_1} \in \text{Bool}_{g_1} &\quad \epsilon_1 \mapsto \text{Bool}_{g_1} \leq \text{Bool}_{g'_1} \\
\phi \mapsto b_{2\ell_2} \in \text{Bool}_{g_2} &\quad \epsilon_2 \mapsto \text{Bool}_{g_2} \leq \text{Bool}_{g'_2}
\end{align*}
\]

\[ (l\oplus) \]

Therefore

\[ \epsilon_1(b_1)_{g_1} \oplus^g \epsilon_2(b_2)_{g_2} \mid \mu \]

\[ \phi \mapsto (\epsilon_1 \wedge \epsilon_2)(b_1 \mathbf{[\oplus]} b_2)_{(g_1 \wedge g_2)} :: \text{Bool}_g \mid \mu \]

Then

\[ (l\oplus) \]

\[ \phi \cdot \epsilon \mapsto \phi \cdot g_c \leq \phi \cdot g_c \\
\phi \mapsto (\epsilon_1 \wedge \epsilon_2)(b_1 \mathbf{[\oplus]} b_2)_{(g_1 \wedge g_2)} :: \text{Bool}_g \in \mathbb{T}[\text{Bool}_g] \]

and the result holds.

**Case (lprot).** Then \( t^U = \phi \mapsto \text{prot}_{\varphi_g}^g \phi'(\epsilon u) \) and

\[
\begin{align*}
\phi \cdot \epsilon \mapsto \phi \cdot g_c \leq \phi \cdot g_c &\quad \epsilon'_r \mapsto \varphi_r \wedge g' \leq g'_c \\
\phi' \mapsto u \in \mathbb{T}[U'] &\quad \epsilon \mapsto U' \leq U \\
\epsilon \mapsto \epsilon' \mapsto g' \leq g
\end{align*}
\]

\[ (lprot) \]

Therefore

\[ \text{prot}_{\varphi_g}^g \phi'(\epsilon u) \mid \mu \mapsto (\epsilon \wedge \epsilon')(u \wedge g') :: U \wedge g \mid \mu \]

But by Lemma E.9, \( \phi \mapsto u \in \mathbb{T}[U'] \). Therefore by definition of join \( \phi \mapsto (u \wedge g') \in \mathbb{T}[U' \wedge g'] \). Then using Lemma 6.13

\[
\begin{align*}
\phi \mapsto (u \wedge g') \in \mathbb{T}[U' \wedge g'] \\
(\epsilon \wedge \epsilon') \mapsto U' \wedge g' \leq U \wedge g
\end{align*}
\]

\[ L:: \]

\[ \phi \mapsto (\epsilon \wedge \epsilon')(u \wedge g') :: U \wedge g \in \mathbb{T}[U \wedge \ell] \]

and the result holds.
Case (lapp). Then $t^U = \epsilon_1(\lambda^{\delta_1^U}x^{U_1}, \iota^{U_1})_{\eta_1} @ U_{12}^{\delta_1^U} U_2 \epsilon_2 u$ and $U = U_2 \triangleright g$. Then

$$\phi \triangleright t^{U_{12}} \in T[U_{12}]$$

$$\phi \triangleright (\lambda^{\delta_1^U}x^{U_1}, \iota^{U_1})_{\eta_1} \in T[U_1]$$

$$\phi \triangleright u \in T[U_2]$$

$$\phi \triangleright g \in T[U_1]$$

If $\epsilon' = (\epsilon_2 \circ \approx \: \text{idom}(\epsilon_1))$ or $\epsilon'_* = (\phi. \epsilon \triangleright \text{ilbl}(\epsilon_1)) \circ \approx \epsilon_\ell \circ \approx \text{ilat}(\epsilon_1)$ are not defined, then $t^U \mid \mu \rightarrow \text{error}$, and then the result hold immediately. Suppose that consistent transitivity does hold, then if $\phi' = (\phi'\epsilon(\phi.g_c \triangleright g_1), \phi.g_c')$

$$\epsilon_1(\lambda^{\delta_1^U}x^{U_1}, \iota^{U_1})_{\eta_1} \epsilon_2 u \mid \mu \rightarrow \text{prot}_{\text{ilbl}((\epsilon_1))} \phi'((\text{ilat}(\epsilon_1)((\epsilon' u :: U_{11})/x^{U_1})) \mid \mu$$

As $\epsilon_2 + U_2' \subseteq U_1$ and by inversion lemma $\text{idom}(\epsilon_1) + U_1 \subseteq U_{11}$, then $\epsilon' + U_2' \subseteq U_{11}$. Therefore

$$\phi \triangleright \epsilon' u :: U_{11} \in T[U_{11}]$$

and by Lemma E.11,

$$\phi \triangleright [(\epsilon' u :: U_{11})/x^{U_1}])_{\epsilon_1}^{U_1} \in T[U_{12}]$$

We know that $\epsilon_\ell \triangleright g_c \triangleright g \leq g'$. By inversion on the label of types, $\text{ilbl}(\epsilon_1) \triangleright g_1 \leq g$. Also by monotonicity of the join, $\phi. \epsilon \triangleright \text{ilbl}(\epsilon_1) + \phi.g_c \triangleright g_1 \leq g_c \triangleright g$. Then, by inversion on the latent effect of function types, $\text{ilat}(\epsilon_1) + g'_\epsilon \leq g''$. Therefore combining evidences, as $\phi.\epsilon' = (\phi.\epsilon \triangleright \text{ilbl}(\epsilon_1)) \circ \approx \epsilon_\ell \circ \approx \text{ilat}(\epsilon_1)$, we may justify the runtime judgment $\phi.\epsilon' \triangleright \phi.g_c \triangleright g_1 \leq g''$. Let us call $t_{U_{12}} = [(\epsilon' u :: U_{11})/x^{U_1})])_{\epsilon_1}^{U_1}$. By Lemma E.8, $\phi' \triangleright t_{U_{12}} \in T[U_{12}]$. Then

$$\phi' \triangleright t_{U_{12}} \in T[U_{12}]$$

$$\text{ilat}(\epsilon_1) + U_{12} \leq U_2 \quad \text{ilbl}(\epsilon_1) + g_1 \leq g$$

and the result holds.

Case (lif-true). Then $t^U = \text{if}_g \epsilon_1 b_{g_1}$ then $\epsilon_2 t_{U_2}$ else $\epsilon_3 t_{U_3} = (U_2 \triangleright \tilde{U}_3) \triangleright g$ and

$$\phi \triangleright b_{g_1} \in T[\text{Bool}_{g}]$$

$$\phi' = (\phi.\epsilon \triangleright \text{ilbl}(\epsilon_1))(\phi.g_c \triangleright g_1), \phi.g_c \triangleright g$$

$$\phi' \triangleright t_{U_2} \in T[U_2]$$

$$\phi' \triangleright t_{U_3} \in T[U_3]$$

$$\phi \triangleright \text{if}_g \epsilon_1 b_{g_1}$$

Therefore

if $\epsilon_1 b_{g_1}$ then $\epsilon_2 t_{U_2}$ else $\epsilon_3 t_{U_3} \mid \mu \rightarrow \text{prot}_{\text{ilbl}((\epsilon_1))} \phi'((\epsilon_2 t_{U_2}) \mid \mu$
But
\[\phi \cdot \varepsilon + \phi \cdot g_c \lesssim \phi \cdot g_c\]
\[\phi \cdot U_2 \in T[U_2]\]
\[\varepsilon_2 + U_2 \subseteq U_2 \triangledown U_3\]
\[\phi \cdot g_1 \lesssim g\]
and the result holds.

Case (lif-true). Analogous to case (if-true).

Case (lif-false). Then \(t U = \text{ref}^U U \varepsilon U\) and
\[\phi \cdot \varepsilon + \phi \cdot g_c \lesssim \phi \cdot g_c\]
\[\phi \cdot U'' \lesssim U'\]
\[\varepsilon \vdash \phi \cdot U'' \lesssim \text{label}(U')\]
\[\phi \cdot \text{ref}^U U \varepsilon U \in T[\text{Ref}_1 U']\]
If \(\epsilon' = \epsilon \triangledown (\phi \cdot \varepsilon \lesssim \varepsilon_\ell)\) is not defined, then \(t U' \mid \mu \phi \rightarrow \text{error}\), and then the result hold immediately.

Suppose that consistent transitivity does hold, then
\[\text{ref}^U U \varepsilon U \mid \mu \phi \rightarrow \phi \cdot U' \mid \mu[\phi \cdot U' \rightarrow \epsilon' (U' \triangledown \phi \cdot g_c) :: U']\]
where \(o U' \notin \text{dom}(\mu)\).

We know that \(\varepsilon_\ell \vdash g_c \lesssim \text{label}(U')\), therefore \(\phi \cdot \varepsilon \lesssim \varepsilon_\ell \vdash \phi \cdot g_c \lesssim \text{label}(U')\). We also know that \(\varepsilon \vdash U'' \lesssim U'\). Therefore combining both evidences we can justify that \(\varepsilon \triangledown (\phi \cdot \varepsilon \lesssim \varepsilon_\ell) + U'_2 \vee \phi \cdot g_c \lesssim U'\).

Let us call \(\mu' = \mu[\phi \cdot U' \rightarrow \epsilon' (U' \triangledown \phi \cdot g_c) :: U']\). It is easy to see that \(\text{freeLocs} o U' = o U'\) and \(\text{dom}(\mu') = \text{dom}(\mu) \cup o U'\), then \(\text{freeLocs} o U' \subseteq \text{dom}(\mu')\). Given that \(t U' + \mu\) then \(\text{freeLocs}(u) \subseteq \text{dom}(\mu')\), and therefore \(\forall v \in \text{cod}(\mu') = \text{cod}(\mu) \cup (\epsilon' (U' \triangledown \phi \cdot g_c) :: U')\). Finally as \(t U' + \mu\) and \(\mu'(\phi \cdot U') = \epsilon' (U' \triangledown \phi \cdot g_c) :: U' \in T[U']\) then we can conclude that \(t U' + \mu'\) and \(\text{dom}(\mu') \subseteq \text{dom}(\mu)\), and the result holds.

Case (lif-true). Then \(t U = \text{ref}^U U \varepsilon U, U = U' \triangledown g\) and
\[\phi \cdot \varepsilon \lesssim \phi \cdot g_c\]
\[\phi \cdot U'' \lesssim \text{Ref}_1 U'\]
\[\phi \cdot \varepsilon \lesssim \phi \cdot g_c\]
\[\phi \cdot \text{ref}^U U \varepsilon U \in T[\text{Ref}_1 U']\]

Then for \(\phi' = (\phi \cdot \varepsilon \triangledown \text{ilbl}(\varepsilon))(\phi \cdot g_c \triangledown g'), (\phi \cdot g_c \triangledown g)\)
\[\text{ref}^U U \varepsilon U \mid \mu \phi \rightarrow \text{prot}^U U \varepsilon U \phi'(\text{iref}(\varepsilon) \nu) \mid \mu\]
where \(\mu(o U') = \nu\). As the store is well typed, therefore \(\phi \cdot \nu \in T[U'']\). By Lemma E.9, \(\phi \cdot \nu \in T[U'']\).

By inversion lemma on references, \(\text{ilbl}(\varepsilon) + \nu \lesssim g\) and \(\text{iref}(\varepsilon) + \nu \lesssim U'\)
\[\phi \cdot \varepsilon \lesssim \phi \cdot g_c\]
\[\phi \cdot \nu \in T[U'']\]
\[\phi \cdot \nu \lesssim g\]
and the result holds.
We know that \( \ell \vdash \text{Ref} \, \ell' \, \ell' \leq \ell \). Then by inversion on reference evidence types and inversion in the label of types, \( \text{ilbl}(\text{iref}(\ell)) \vdash \text{label}(\ell') \). But \( \text{ilbl}(\ell) \vdash \ell' \leq g \), using monotonicity of the join, \( \phi, \ell' \bowtie \text{ilbl}(\ell) \vdash \phi, \ell' \bowtie g \leq \phi, \ell' \bowtie g \). Therefore

\[
((\phi, \ell) \bowtie \text{ilbl}(\ell)) \leq \phi, \ell' \bowtie g \leq \phi, \ell' \bowtie g \leq \text{label}(\ell').
\]

We also know that \( \ell' \vdash \phi, \ell' \bowtie g \leq \text{label}(\ell') \). Combining both evidences, \( \ell' = (\ell_2 \circ \ell) \bowtie \text{iref}(\ell_1) \vdash \text{ilbl}(\ell_1) \bowtie \text{label}(\ell') \). We can then justify that \( \ell' \vdash \ell_2 \bowtie \phi, \ell' \bowtie g \leq \text{label}(\ell') \) and therefore justify the ascription in the heap.

Let us call \( \mu' = \mu \bowtie \ell \) then \( \text{freeLocs}(\mu') \subseteq \text{freeLocs}(\mu) \). As \( \text{freeLocs}(\mu) = \emptyset \) then \( \text{freeLocs}(\mu') \subseteq \mu' \).

As \( \ell \vdash \mu \) then \( \text{freeLocs}(\mu) = \text{dom}(\mu) \), and as \( \text{dom}(\mu) = \text{dom}(\mu') \) then it is trivial to see that \( \forall \, v' \in \text{cod}(\mu'), \text{freeLocs}(\mu') \subseteq \text{dom}(\mu') \), and the result holds.

\( \square \)

**Proposition E.13 (\( \rightarrow \) is well defined).** If \( t^U \vdash \mu \rightarrow r \) and \( t^U \vdash \mu' \), then \( r \in \text{CONFIG}_U \cup \{ \text{error} \} \) and if \( r = t^U \vdash \mu' \in \text{CONFIG}_U \) then also \( t^U \vdash \mu' \) and \( \text{dom}(\mu) \subseteq \text{dom}(\mu') \).

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

**Case** (R→). If \( t^U \vdash \mu \rightarrow r \). By well-definedness of \( \rightarrow \) (Prop E.12), \( r \in \text{CONFIG}_U \cup \{ \text{error} \} \) and if \( r = t^U \vdash \mu' \in \text{CONFIG}_U \) then also \( t^U \vdash \mu' \) and \( \text{dom}(\mu) \subseteq \text{dom}(\mu') \).

**Case** (Rprot). If \( t^U = \text{prot}^{\ell \ell'}^{g_{\ell'}}^{g_{\ell}}\phi'(\ell _{1}^{U''}) \) and

\[
\phi, \ell \bowtie \phi, \ell' \bowtie g_{\ell'} \bowtie g' \leq g_{\ell}
\]

are derivable, then

\[
\phi \vdash \ell' \bowtie U'' \quad \phi \vdash g' \bowtie g
\]

Using induction hypothesis on the premise of (Rprot), then

\[
\text{prot}^{\ell \ell'}^{g_{\ell'}}^{g_{\ell}}\phi'(\ell _{1}^{U''}) \vdash \mu \rightarrow \text{prot}^{\ell \ell'}^{g_{\ell'}}^{g_{\ell}}\phi'(\ell _{2}^{U''}) \vdash \mu'
\]

where \( \phi \vdash t_{1}^{U''} \in \text{T}[U''] \), \( t_{2}^{U''} \vdash \mu' \) and \( \text{dom}(\mu) \subseteq \text{dom}(\mu') \). Therefore
We know that $\varepsilon F$ where $\text{freeLocs}$ and the result holds.

Case (Rf). $t^U = f[t^U_1], \phi \triangleright f[t^U_1] \in T[U_1], t^U_1 \mid \mu \triangleright t^U_1 \mid \mu'$, and consider $F : T[U'] \rightarrow T[U]$, where $F(\phi \triangleright t^U') = \phi \triangleright f[t^U]$. By induction hypothesis, $\phi \triangleright t^U_2 \in T[U']$, so $F(\phi \triangleright t^U_2) = \phi \triangleright f[t^U_2] \in T[U]$. By induction hypothesis we also know that $t^U_2 \triangleright \mu'$.

If $\text{freeLocs}(t^U_2) \subseteq \mu'$, $\text{freeLocs}(f[t^U]) \subseteq \mu$, and $\text{dom}(\mu) \subseteq \text{dom}(\mu')$, then it is easy to see that $\text{freeLocs}(f[t^U_2]) \subseteq \mu'$, and therefore conclude that $f[t^U_2] \triangleright \mu'$.

Case (Rprot()ferr). Similar case to (Rh) case, using $P : \text{EvTerm} \rightarrow T[U]$, $P(\varepsilon) = \phi \triangleright \text{prot}_{\varepsilon^g} \phi'(\varepsilon)$.

\[ \phi \varepsilon \triangleright \phi \varepsilon' \leq \phi \varepsilon' \rightarrow g_r \vee g' \leq g' \]

Proof. By induction on the structure of $\phi \triangleright t^U$. 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 E.14 (TYPE SAFETY). If $\phi \triangleright t^U \in T[U]$ then either $t^U$ is a value $\nu; t^U \mid \mu \triangleright \text{error}$; or if $t^U \mid \mu$ then $t^U \mid \mu \triangleright t^U \mid \mu'$ for some term $\phi \triangleright t^U \in T[U]$ and some $\mu'$ such that $t^U \mid \mu'$ and $\text{dom}(\mu) \subseteq \text{dom}(\mu')$.

Proof. By induction on the structure of $\phi \triangleright t^U$.

Case (Iu,II, Ia, Ia). $t^U$ is a value.

Case (Iprot). $t^U = \text{prot}_{\varepsilon^g} \phi'(\varepsilon t^U)$, and

\[ \phi \varepsilon \triangleright \phi \varepsilon' \leq \phi \varepsilon' \rightarrow g_r \vee g' \leq g' \]

\[ \phi \triangleright t^U \in T[U'] \]

\[ \phi \triangleright \text{prot}_{\varepsilon^g} \phi'(\varepsilon t^U) \in T[U \setminus g] \]

By induction hypothesis on $t^U'$, one of the following holds:

1. $t^U'$ is a simple value, then by (R→→), $t^U \mid \mu \leftrightarrow \nu | \mu$, and by Prop E.13, $\phi \triangleright \nu \in T[U]$ and the result holds.
2. $t^U'$ is an ascribed value $\nu$, then, $\mathcal{t}^U' \rightarrow e$ et' for some $e \in \text{EvTerm} \cup \{ \text{error} \}$. Hence $t^U \mid \mu \leftrightarrow r$ for some $r \in \text{CONFIG}_U \cup \{ \text{error} \}$ by Prop E.13 and either (Rg), or (Rgerr).
(3) \( t^U \downarrow \mu \mapsto^\phi r_1 \) for some \( r_1 \in T[U_1] \cup \{ \text{error} \} \). Hence \( t^U \downarrow \mu \mapsto^\phi r \) for some \( r \in \text{CONFIG}_U \cup \{ \text{error} \} \) by Prop E.13 and either (Rprot) or (Rprotferr).

**Case (I).** \( t^U = \epsilon_1 t^{U_1} :: U_2 \), and
\[
\phi \triangleright t^{U_1} \in T[U_1] \\
\epsilon_1 \uparrow U_1 \leq U_2 \quad \phi.g \triangleright \phi.g_c \downarrow \phi.g_c \\
\phi \triangleright \epsilon_1 t^{U_1} :: U_2 \in T[U_2]
\]
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. \( t^{U_1} \downarrow \mu \mapsto^\phi r_1 \) for some \( r_1 \in T[U_1] \cup \{ \text{error} \} \). Hence \( t^U \downarrow \mu \mapsto r \) for some \( r \in \text{CONFIG}_U \cup \{ \text{error} \} \) by Prop E.13 and either (Rf), or (Rferr).

**Case (Iif).** \( t^U = \text{if}^U \epsilon_1 t^{U_1} \) then \( \epsilon_2 t^{U_2} \) else \( \epsilon_3 t^{U_3} \) and
\[
\phi \triangleright t^{U_1} \in T[U_1] \\
\epsilon_1 \uparrow U_1 \leq \text{Bool} \quad \phi.e \triangleright \phi.g_c \downarrow \phi.g_c \\
\phi' = ((\phi.e \triangleright \text{ilbl}(\epsilon_1))(\phi.g_c \triangleright \text{label}(U_1)), g_c \triangleright g) \\
\phi' \triangleright t^{U_2} \in T[U_2] \\
\epsilon_2 \uparrow U_2 \leq (U_2 \triangleright U_3) \\
\phi' \triangleright t^{U_3} \in T[U_3] \\
\epsilon_3 \uparrow U_3 \leq (U_2 \triangleright U_3) \triangleright g
\]
By induction hypothesis on \( t^{U_1} \), one of the following holds:

1. \( t^{U_1} \) is a value \( u \), then by (R\( \rightarrow \)), \( t^U \downarrow \mu \mapsto^\phi r \) and \( r \in \text{CONFIG}_U \cup \{ \text{error} \} \) by Prop E.13.

2. \( t^{U_1} \) is ascribed value \( v \), then, \( \epsilon_1 t^{U_1} \rightarrow_c e \) for some \( e \in \text{EvTERM} \cup \{ \text{error} \} \). Hence \( t^U \downarrow \mu \mapsto r \) for some \( r \in \text{CONFIG}_U \cup \{ \text{error} \} \) by Prop E.13 and either (Rg), or (Rgerr).

3. \( t^{U_1} \downarrow \mu \mapsto^\phi r_1 \) for some \( r_1 \in T[U_1] \cup \{ \text{error} \} \). Hence \( t^U \downarrow \mu \mapsto r \) for some \( r \in \text{CONFIG}_U \cup \{ \text{error} \} \) by Prop E.13 and either (Rf), or (Rferr).

**Case (Iapp).** \( t^U = \epsilon_1 t^{U_1} @_{\epsilon_2}^{U_1} \rightarrow_{g_c} \epsilon_3 t^{U_2} \)
\[
\phi \triangleright t^{U_1} \in T[U_1] \\
\epsilon_1 \uparrow U_1 \leq U_{11} \rightarrow_g U_{12} \\
\phi \triangleright t^{U_2} \in T[U_2] \\
\epsilon_2 \uparrow U_2 \leq U_{11} \\
\phi \triangleright \epsilon_1 t^{U_1} @_{\epsilon_2}^{U_1} \rightarrow_{g_c} \epsilon_3 t^{U_2} \in T[U_{12} \triangleright g]
\]
By induction hypothesis on \( t^{U_1} \), one of the following holds:

1. \( t^{U_1} \) is a value \( \lambda x^{U_1}.t^{U_1}_x \) (by canonical forms Lemma E.10), posing \( U_1 = U_{11} \rightarrow_g U_{12} \).

   Then by induction hypothesis on \( t^{U_1} \), one of the following holds:
   (a) \( t^{U_1} \) is a value \( u \), then by (R\( \rightarrow \)), \( t^U \downarrow \mu \mapsto^\phi r \) and \( r \in \text{CONFIG}_U \cup \{ \text{error} \} \) by Prop E.13.
   (b) \( t^{U_1} \) is ascribed value \( v \), then, \( \epsilon_2 t^{U_2} \rightarrow_c e \) for some \( e \in \text{EvTERM} \cup \{ \text{error} \} \). Hence \( t^U \downarrow \mu \mapsto r \) for some \( r \in \text{CONFIG}_U \cup \{ \text{error} \} \) by Prop E.13 and either (Rg), or (Rgerr).
   (c) \( t^{U_1} \downarrow \mu \mapsto^\phi r_2 \) for some \( r_2 \in \text{CONFIG}_U \cup \{ \text{error} \} \). Hence \( t^U \downarrow \mu \mapsto r \) for some \( r \in \text{CONFIG}_U \cup \{ \text{error} \} \) by Prop E.13 and either (Rf), or (Rferr). Also by Prop E.13, if \( r = t^{U'} \downarrow \mu' \in T[U] \) then \( \text{dom}(\mu) \subseteq \text{dom}(\mu') \).
(2) \( t_{U_1} \) is an ascribed value \( v \), then, \( \epsilon_1 t_{U_1} \rightarrow_c et' \) for some \( et' \in \text{EVTERM} \cup \{ \text{error} \} \). Hence \( t_{U_1} | \mu \stackrel{\phi}{\rightarrow} r \) for some \( r \in \text{CONFIG} \cup \{ \text{error} \} \) by Prop E.13 and either (Rg), or (Rgerr).

(3) \( t_{U_1} | \mu \rightarrow r_1 \) for some \( r_1 \in \text{CONFIG}_1 \cup \{ \text{error} \} \). Hence \( t_{U_1} | \mu \stackrel{\phi}{\rightarrow} r \) for some \( r \in \text{CONFIG} \cup \{ \text{error} \} \) by Prop E.13 and either (Rf), or (Rferr). Also by Prop E.13, if \( r = t_{U_1} | \mu' \in T[U] \) then \( \text{dom}(\mu) \subseteq \text{dom}(\mu') \).

Case (Iref). Similar case to (Iapp).

Case (Iref). \( t_{U} = \text{ref}_{\ell_f} et_{U''} \) and

\( \phi, \epsilon + \phi . g_c \preceq \phi . g_c \quad \phi \triangleright t_{U''} \in T[U''] \)

\( \text{(Iref)} \)

\( \phi \triangleright \text{ref}_{\ell_f} et_{U''} \in T[\text{Ref}_f U'] \)

By induction hypothesis on \( t_{U''} \), one of the following holds:

(1) \( t_{U''} \) is a value \( v \), then, by (Rf), \( t_{U''} | \mu \stackrel{\phi}{\rightarrow} r \) and \( r \in \text{CONFIG} \) by Prop E.13. Also by Prop E.13, if \( r = t_{U''} | \mu' \in T[U] \) then \( \text{dom}(\mu) \subseteq \text{dom}(\mu') \).

(2) \( t_{U''} \) is a value \( v \), then, \( \epsilon t_{U''} \rightarrow_c et' \) for some \( et' \in \text{EVTERM} \cup \{ \text{error} \} \). Hence \( t_{U''} | \mu \stackrel{\phi}{\rightarrow} r \) for some \( r \in \text{CONFIG} \cup \{ \text{error} \} \) by Prop E.13 and either (Rg), or (Rgerr).

(3) \( t_{U''} | \mu \stackrel{\phi}{\rightarrow} r_1 \) for some \( r_1 \in \text{CONFIG}_1 \cup \{ \text{error} \} \). Hence \( t_{U''} | \mu \stackrel{\phi}{\rightarrow} r \) for some \( r \in \text{CONFIG} \cup \{ \text{error} \} \) by Prop E.13 and either (Rf), or (Rferr). Also by Prop E.13, if \( r = t_{U''} | \mu' \in T[U] \) then \( \text{dom}(\mu) \subseteq \text{dom}(\mu') \).

Case (I''ref). \( t_{U} = t_{\text{Ref}_f U' \ell_f t_{U''}} \)

\( \phi, \epsilon + \phi . g_c \preceq \phi . g_c \quad \phi \triangleright t_{U''} \in T[U''] \)

\( \text{(I''ref)} \)

\( \phi \triangleright t_{\text{Ref}_f U' \ell_f t_{U''}} \in T[U' \lor g] \)

By induction hypothesis on \( t_{U''} \), one of the following holds:

(1) \( t_{U''} \) is a value \( t_{U''} \) (by canonical forms Lemma E.10), where \( U'' = \text{Ref}_f U'' \), then by (Rf), \( \epsilon t_{U''} \rightarrow_c et' \) for some \( et' \in \text{EVTERM} \cup \{ \text{error} \} \). Hence \( t_{U''} | \mu \stackrel{\phi}{\rightarrow} r \) and \( r \in \text{CONFIG} \) by Prop E.13.

(2) \( t_{U''} \) is an ascribed value \( v \), then, \( \epsilon t_{U''} \rightarrow_c et' \) for some \( et' \in \text{EVTERM} \cup \{ \text{error} \} \). Hence \( t_{U''} | \mu \stackrel{\phi}{\rightarrow} r \) for some \( r \in \text{CONFIG} \cup \{ \text{error} \} \) by Prop E.13 and either (Rg), or (Rgerr).

(3) \( t_{U''} | \mu \stackrel{\phi}{\rightarrow} r_1 \) for some \( r_1 \in \text{CONFIG}_1 \cup \{ \text{error} \} \). Hence \( t_{U''} | \mu \stackrel{\phi}{\rightarrow} r \) for some \( r \in \text{CONFIG} \cup \{ \text{error} \} \) by Prop E.13 and either (Rf), or (Rferr). Also by Prop E.13, if \( r = t_{U''} | \mu' \in T[U] \) then \( \text{dom}(\mu) \subseteq \text{dom}(\mu') \).

Case (IUassign). \( t_{U} = \epsilon_1 t_{U_1} g_{U_1} := \epsilon_1 \ell_2 t_{U_2} \)

\( \epsilon_1 + \text{Ref}_g U_1 \leq \text{Ref}_g U_1 \quad \phi \triangleright t_{U_1} \in T[\text{Ref}_g U_1] \)

\( \epsilon_2 \downarrow U_2 \leq U_1 \quad \phi \triangleright t_{U_2} \in T[U_2] \)

\( \phi, \epsilon + \phi . g_c \preceq \phi . g_c \quad \epsilon \downarrow g \preceq \text{label}(U_1) \)

\( \text{(lassign)} \)

\( \phi \triangleright \epsilon_1 t_{U_1} g_{U_1} := \epsilon_1 \ell_2 t_{U_2} \in T[\text{Unit}_1] \)

By induction hypothesis on \( t_{U_2} \), one of the following holds:

(1) \( t_{U_2} \) is a value \( t_{U_2} \) (by canonical forms Lemma E.10), where \( U_2' = \text{Ref}_g U_2'' \). Then by induction hypothesis on \( t_{U_2} \), one of the following holds:
(a) $t^U$ is a value $u$, then by $(R\rightarrow)$, $t^U | \mu \xrightarrow{\phi} r$ and $r \in \text{CONFIG}_U \cup \{\text{error}\}$ by Prop E.13. Also by Prop E.13, if $r = t^U | \mu' \in T[U]$ then $\text{dom}(\mu) \subseteq \text{dom}(\mu')$.

(b) $t^{U_2}$ is an ascribed value $v$, then, $\epsilon_2 t^{U_2} \xrightarrow{c} e'$ for some $e' \in \text{EvTerm} \cup \{\text{error}\}$. Hence $t^U | \mu \xrightarrow{\phi} r$ for some $r \in \text{CONFIG}_U \cup \{\text{error}\}$ by Prop E.13 and either (Rg), or (Rgerr).

(c) $t^{U_2} | \mu \xrightarrow{\phi} r_2$ for some $r_2 \in \text{CONFIG}_U \cup \{\text{error}\}$. Hence $t^U | \mu \xrightarrow{\phi} r$ for some $r \in \text{CONFIG}_U \cup \{\text{error}\}$ by Prop E.13 and either (Rf), or (Rferr). Also by Prop E.13, if $r = t^{U_2} | \mu' \in T[U]$ then $\text{dom}(\mu) \subseteq \text{dom}(\mu')$.

\[\Box\]

**Proposition E.15** (Static terms do not fail). Let us define $\text{StaticTerm}$ the set of evidence augmented terms with full static annotations. Then consider $t_s \in \text{StaticTerm}$, $\phi = (\ell'_{c}, \ell_{c})$, and $\mu_s$, such that $\varepsilon = \delta(\ell'_{c} \lesssim \ell_{c}]$, $\phi \triangleright t_s \in T[S]$, and that $\forall v_s \in \text{cod}(\mu_s), v_s \in \text{StaticTerm}$. Then either $t_s$ is a value, or

\[t_s | \mu_s \xrightarrow{\phi} t'_s | \mu'_s\]

**Proof.** We know that if you follow AGT to derive the dynamic semantics of a gradual language, then by construction the resulting language satisfy the dynamic conservative extension property. As we follow AGT to derive the dynamic semantics, we get this property by construction, save for the assignment elimination reduction rule. In this rule we add an extra check of the form $\phi.\varepsilon \lfloor \leq \rfloor \text{ilbl}(\varepsilon)$. So if we prove that the extra check is always satisfied, then the result holds.

Let us consider a $t'_s$ fully static like so:

\[
\begin{align*}
\epsilon_1 + \text{Ref}_\ell \ S'_1 \leq \text{Ref}_\ell \ S_1 \\
\epsilon_2 + S_2 \leq S_1 \\
\phi \triangleright \phi_{S'_1} \in T[\text{Ref}_\ell \ S'_1] \\
\phi \triangleright u \in T[S_2] \\
\phi \triangleright \epsilon_{\ell'_{c}} \leq \ell_{c} \\
\epsilon_{\ell} \triangleright \ell_{c} \vee \ell \leq \text{label}(S_1) \\
\phi \triangleright \epsilon_{\ell} o_{\ell_{c}}^{S'_1} \ell_{c} \equiv_{\ell_{c}} \epsilon_{\ell} u \in T[\text{Unit}_1]
\end{align*}
\]

By inspection of the reduction rules we have to prove that $\phi.\varepsilon \lfloor \leq \rfloor \text{ilbl}(\varepsilon). \phi.\varepsilon \lfloor \leq \rfloor \text{ilbl}(\varepsilon)$. We know by definition of interior between two static labels that $\varepsilon = \delta(\ell'_{c} \lesssim \ell_{c}] = (\ell'_{c}, \ell_{c}[\ell_{c}, \ell_{c}])$. Also, if $\mu_s(\phi^{S'_1}) = \varepsilon u' :: S'_1$, as everything is static, $\text{ilbl}(\varepsilon)$ have to have the form $([\ell_{u}, \ell_{u}], [\text{label}(S'_1), \text{label}(S_1)])$, for some $\ell_{u}$. Then we have to prove that $\ell_{c} \leq \text{label}(S_1)$, but notice that as everything is static, $\epsilon_{\ell} \triangleright \ell_{c} \vee \ell \leq \text{label}(S_1)$ is equivalent to $\epsilon_{\ell} \triangleright \ell_{c} \vee \ell \leq \text{label}(S_1)$, therefore we know that $\ell_{c} \leq \text{label}(S_1)$ and the result holds.

\[\Box\]

### E.5 Dynamic Gradual Guarantee

In this section we present the proof the Dynamic Gradual Guarantee for GSLRef without the specific check in rule (r7).

**Definition E.16** (Intrinsic term precision). Let $\Omega \in \mathcal{D}(\mathbb{V}[\ast] \times \mathbb{V}[\ast]) \cup \mathcal{D}(\text{Loc}_c \times \text{Loc}_c)$ be defined as $\Omega ::= \{x^{U_1} \equiv x^{U_2}, o^{U_1} \equiv a^{U_2}\}$ We define
\[ \begin{align*}
\Omega \cup \{ x^{U_1} \subseteq x^{U_2} \} \vdash x^{U_1} \subseteq x^{U_2} & & g_1 \subseteq g_2 \quad \Omega \vdash g_2 \quad \Omega \vdash \text{unit}_{g_1} \subseteq \text{unit}_{g_2} \\
\Omega \cup \{ o^{U_1} \subseteq o^{U_2} \} \vdash o^{U_1} \subseteq o^{U_2} & & \Omega \vdash \text{unit}_{g_1} \subseteq \text{unit}_{g_2} \\
n \Omega \vdash \text{prot}_{\epsilon_1} \epsilon_1 \subseteq \text{prot}_{\epsilon_2} \epsilon_2 & & \Omega \vdash \text{prot}_{\epsilon_1} \epsilon_1 \subseteq \text{prot}_{\epsilon_2} \epsilon_2 \\
\Omega \vdash \text{proto}_{\epsilon_1} \text{proto}_{\epsilon_2} \epsilon_1 \subseteq \text{proto}_{\epsilon_1} \text{proto}_{\epsilon_2} \epsilon_2 & & \Omega \vdash \text{proto}_{\epsilon_1} \text{proto}_{\epsilon_2} \epsilon_1 \subseteq \text{proto}_{\epsilon_1} \text{proto}_{\epsilon_2} \epsilon_2 \\
\Omega \vdash \text{re} \text{proto}_{\epsilon_1} \text{proto}_{\epsilon_2} \epsilon_1 \subseteq \text{re} \text{proto}_{\epsilon_1} \text{proto}_{\epsilon_2} \epsilon_2 & & \Omega \vdash \text{re} \text{proto}_{\epsilon_1} \text{proto}_{\epsilon_2} \epsilon_1 \subseteq \text{re} \text{proto}_{\epsilon_1} \text{proto}_{\epsilon_2} \epsilon_2 \\
\Omega \vdash \text{ref}_{\epsilon_1} \text{ref}_{\epsilon_2} \epsilon_1 \text{ref}_{\epsilon_1} \epsilon_2 \text{ref}_{\epsilon_2} \epsilon_2 & & \Omega \vdash \text{ref}_{\epsilon_1} \text{ref}_{\epsilon_2} \epsilon_1 \text{ref}_{\epsilon_1} \epsilon_2 \text{ref}_{\epsilon_2} \epsilon_2 \\
\end{align*} \]

\[ \Omega \vdash \text{ref}_{\epsilon_1} \text{ref}_{\epsilon_2} \epsilon_1 \text{ref}_{\epsilon_1} \epsilon_2 \text{ref}_{\epsilon_2} \epsilon_2 \]

where \( \phi_1 \subseteq \phi_2 \iff \phi_1.\text{ref}_{\epsilon_1} \subseteq \phi_2.\text{ref}_{\epsilon_1} \)

Fig. 39. Intrinsic term precision

an ordering relation \( \cdot \vdash \cdot \subseteq \cdot \) \( \subseteq \) \( \text{ref} \text{ref}_{\epsilon_1} \text{ref}_{\epsilon_2} \epsilon_1 \text{ref}_{\epsilon_1} \epsilon_2 \text{ref}_{\epsilon_2} \epsilon_2 \)

\[ \forall \epsilon_1 \in \text{dom}(\mu_1), \exists \epsilon_2 \in \text{dom}(\mu_2) \text{ s.t.} \]

\[ \Omega \vdash \text{ref}_{\epsilon_1} \text{ref}_{\epsilon_2} \epsilon_1 \text{ref}_{\epsilon_1} \epsilon_2 \text{ref}_{\epsilon_2} \epsilon_2 \]

\[ \Omega \vdash \mu_1 \subseteq \mu_2 \]

**Definition E.17 (Well Formedness of \( \Omega \)).** We say that \( \Omega \) is well formed iff \( \forall \{ t^{U_1} \subseteq t^{U_2} \} \in \Omega, U_1 \subseteq U_2 \)

\[ \text{Definition E.17 (Well Formedness of \( \Omega \)). } \quad \text{We say that } \Omega \text{ is well formed iff } \forall \{ t^{U_1} \subseteq t^{U_2} \} \in \Omega, U_1 \subseteq U_2 \]
Before proving the gradual guarantee, we first establish some auxiliary properties of precision. For the following propositions, we assume Well Formedness of $Ω$ (Definition E.17).

**Proposition E.18.** If $Ω ⊳ t^{U_1} ⊆ t^{U_2}$ for some $Ω ∈ \mathcal{P}(V[\ast] × V[\ast]) ∪ \mathcal{P}(\text{Loc}_x × \text{Loc}_y)$, then $U_1 ⊆ U_2$.

**Proof.** Straightforward induction on $Ω ⊳ t^{U_1} ⊆ t^{U_2}$, since the corresponding precision on types is systematically a premise (either directly or transitively). □

**Proposition E.19.** Let $g_1, g_2 ∈ \text{EvFrame}$ such that $ϕ_1 ⊳ g_1[\epsilon_1 t^{U_1}] ∈ T[U'_1], ϕ_2 ⊳ g_2[\epsilon_2 t^{U_2}] ∈ T[U'_2]$, with $U'_1 ⊆ U'_2$. Then if $g_1[\epsilon_1 t^{U_1}] ∈ g_2[\epsilon_2 t^{U_2}]$, $γ_{12} ∈ \epsilon_2$ and $t^{U_1} ⊆ t^{U_2}$, then $g_1[\epsilon_1 t^{U_1}] ∈ g_2[\epsilon_2 t^{U_2}]$.

**Proof.** We proceed by case analysis on $g_1$.

Case ($□ @^U f$ et). Then for $i ∈ \{1, 2\}$ $g_i$ must have the form $□ @^U f^i$ for some $U''_i, ε'_i$ and $t^{U_i}$. If $g_1[\epsilon_1 t^{U_1}] ∈ g_2[\epsilon_2 t^{U_2}]$ then by $\subseteq_{\text{APP}} ε_1 ⊆ ε_2, ε'_1 ⊆ ε'_2, U''_1 ⊆ U''_2$ and $t^{U_1} ⊆ t^{U_2}$.

As $ε_{12} ⊆ ε_2$ and $t^{U_1} ⊆ t^{U_2}$, then by $\subseteq_{\text{APP}} ε_{12} t^{U_1} ⊆ ε_{12} t^{U_2}$ and $\subseteq_{\text{APP}} ε_{12} t^{U_1} ⊆ ε_{12} t^{U_2}$, and the result holds.

Case ($□ ⊢^0 ev, ev ≈, ev @^U f$, $□ :: U, □ ⊢^0, □ :: U, □ :: = \epsilon_f)$ et, $ev := \epsilon_f □, if^g □ then et else et)$. Straightforward using similar argument to the previous case. □

**Proposition E.20.** Let $g_1, g_2 ∈ \text{EvFrame}$ such that $ϕ_1 ⊳ g_1[\epsilon_1 t^{U_1}] ∈ T[U'_1], ϕ_2 ⊳ g_2[\epsilon_2 t^{U_2}] ∈ T[U'_2]$, with $U'_1 ⊆ U'_2$. Then if $g_1[\epsilon_1 t^{U_1}] ⊆ g_2[\epsilon_2 t^{U_2}]$ then $t^{U_1} ⊆ t^{U_2}$ and $ε_1 ⊆ ε_2$.

**Proof.** We proceed by case analysis on $g_1$.

Case ($□ @^U f$ et). Then there must exist some $ε_1, U_1, ε'_1$ and $t^{U_1}$ such that $g[\epsilon_1 t^{U_1}] = ε_1 t^{U_1} @^U ε'_1 t^{U_1}$ and $g[\epsilon_2 t^{U_2}] = ε_2 t^{U_2} @^U ε'_2 t^{U_2}$. Then by the hypothesis and the premises of ($\subseteq_{\text{APP}}$), $t^{U_1} ⊆ t^{U_2}$ and $ε_1 ⊆ ε_2$, and the result holds immediately.

Case ($□ ⊢^0 ev, ev ≈, ev @^U f$, $□ :: U, !U, □ :: = \epsilon_f$ et, $ev := \epsilon_f □, if^g □ then et else et)$. Straightforward using similar argument to the previous case. □

**Proposition E.21.** Let $f_1, f_2 ∈ \text{EvFrame}$ such that $ϕ_1 ⊳ f_1[\ell^{U_1}] ∈ T[U'_1], ϕ_2 ⊳ f_2[\ell^{U_2}] ∈ T[U'_2]$, with $U'_1 ⊆ U'_2$. Then if $f_1[\ell^{U_1}] ⊆ f_2[\ell^{U_2}]$ and $t^{U_1} ⊆ t^{U_2}$, then $f_1[\ell^{U_1}] ⊆ f_2[\ell^{U_2}]$.

**Proof.** Suppose $f_1[\ell^{U_1}] = g_1[\ell^{U_1}]$. We know that $ϕ_1 ⊳ g_1[\ell^{U_1}] ∈ T[U'_1], ϕ_1 ⊳ g_1[\ell^{U_2}] ∈ T[U'_2]$ and $U'_1 ⊆ U'_2$. Therefore if $g_1[\ell^{U_1}] ⊆ g_1[\ell^{U_2}]$, by Prop E.20, $ε_1 ⊆ ε_2$. Finally by Prop E.19 we conclude that $g_1[\epsilon_1 t^{U_1}] ⊆ g_1[\epsilon_2 t^{U_2}]$. □

**Proposition E.22.** Let $f_1, f_2 ∈ \text{EvFrame}$ such that $ϕ_1 ⊳ f_1[\ell^{U_1}] ∈ T[U'_1], ϕ_2 ⊳ f_2[\ell^{U_2}] ∈ T[U'_2]$, with $U'_1 ⊆ U'_2$. Then if $f_1[\ell^{U_1}] ⊆ f_2[\ell^{U_2}]$ then $t^{U_1} ⊆ t^{U_2}$.

**Proof.** Suppose $f_1[\ell^{U_1}] = g_1[\ell^{U_1}]$. We know that $ϕ_1 ⊳ g_1[\ell^{U_1}] ∈ T[U'_1], ϕ_1 ⊳ g_2[\ell^{U_2}] ∈ T[U'_2]$ and $U'_1 ⊆ U'_2$. Therefore if $g_1[\ell^{U_1}] ⊆ g[\ell^{U_2}]$, then using Prop E.20 we conclude that $t^{U_1} ⊆ t^{U_2}$.
Proposition E.23 (Substitution preserves precision). If \( \Omega \cup \{ x^U \subseteq x^U \} \vdash t^{U_1} \subseteq t^{U_2} \) and \( \Omega \vdash t^{U_3} \subseteq t^{U_4} \), then \( \Omega \vdash [t^{U_1}/x^U] t^{U_1} \subseteq [t^{U_4}/x^U] t^{U_2} \).

Proof. By induction on the derivation of \( t^{U_1} \subseteq t^{U_2} \), and case analysis of the last rule used in the derivation. All cases follow either trivially (no premises) or by the induction hypotheses. \( \square \)

Proposition E.24 (Monotone precision for \( \circ \leq \)). If \( \varepsilon_1 \leq \varepsilon_2 \) and \( \varepsilon_3 \leq \varepsilon_4 \) then \( \varepsilon_1 \circ \leq \varepsilon_3 \leq \varepsilon_2 \circ \leq \varepsilon_4 \).

Proof. By definition of consistent transitivity for \( \leq \) and the definition of precision. \( \square \)

Proposition E.25 (Monotone precision for \( \circ \)). If \( \varepsilon_1 \leq \varepsilon_2 \) and \( \varepsilon_3 \leq \varepsilon_4 \) then \( \varepsilon_1 \circ \varepsilon_3 \leq \varepsilon_2 \circ \varepsilon_4 \).

Proof. By definition of consistent transitivity for \( \leq \) and the definition of precision. \( \square \)

Proposition E.26 (Monotone precision for Join). If \( \varepsilon_1 \leq \varepsilon_2 \) and \( \varepsilon_3 \leq \varepsilon_4 \) then \( \varepsilon_1 \como \varepsilon_3 \leq \varepsilon_2 \como \varepsilon_4 \).

Proof. By definition of join and the definition of precision. \( \square \)

Proposition E.27. If \( \text{Ref} \ U_1 \subseteq \text{Ref} \ U_2 \) then \( U_1 \subseteq U_2 \).

Proof. By definition of precision we know that \( \{ \text{Ref} \ T \mid T \in \gamma(U_1) \} \subseteq \{ \text{Ref} \ T \mid T \in \gamma(U_2) \} \). This relation is true only if \( \gamma(U_1) \subseteq \gamma(U_2) \) which is equivalent to \( U_1 \subseteq U_2 \). \( \square \)

Proposition E.28. If \( U_{11} \subseteq U_{12} \) and \( U_{21} \subseteq U_{22} \) then \( U_{11} \como U_{21} \subseteq U_{12} \como U_{22} \).

Proof. By induction on the type derivation of the types and consistent join. \( \square \)

Lemma E.29. If \( \varepsilon_1 \vdash \text{Ref}_{g_{11}} U_{11} \leq \text{Ref}_{g_{12}} U_{12} \) and \( \varepsilon_2 \vdash \text{Ref}_{g_{21}} U_{21} \leq \text{Ref}_{g_{22}} U_{22} \), and \( \varepsilon_1 \leq \varepsilon_2 \), then \( \operatorname{iref}(\varepsilon_1) \subseteq \operatorname{iref}(\varepsilon_2) \).

Proof. By definition of precision and \( \operatorname{iref} \). \( \square \)

Proposition E.30 (Dynamic guarantee for \( \longrightarrow \)). Suppose \( \Omega \vdash t_1^{U_1} \subseteq t_1^{U_2} \), \( \phi_1 \leq \phi_2 \), and \( \Omega \vdash \mu_1 \subseteq \mu_2 \). If \( \mu_1 \vdash \phi_1 (t_2^{U_1}) \mid \mu_2 \vdash \phi_2 (t_2^{U_2}) \) where \( \Omega' \vdash t_2^{U_1} \subseteq t_2^{U_2} \) and \( \Omega' \vdash \mu_1' \leq \mu_2' \), for some \( \Omega' \subseteq \Omega \).

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

Case (\( \longrightarrow \ \oplus \)). We know that \( t_1^{U_1} = (\varepsilon_{11} (b_1)_{g_{11}} \oplus \varepsilon_{12} (b_2)_{g_{12}}) \) then by (\( \equiv \phi \)) \( t_1^{U_1} = (\varepsilon_{21} (b_1)_{g_{21}} \oplus \varepsilon_{22} (b_2)_{g_{22}}) \) for some \( \varepsilon_{21}, \varepsilon_{22}, g_{21}, g_{22} \) such that \( \varepsilon_{11} \leq \varepsilon_{21}, \varepsilon_{12} \leq \varepsilon_{22}, g_{11} \leq g_{21} \) and \( g_{12} \leq g_{22} \).

If \( \mu_1 \vdash \phi_1 (b_3) \mid \mu_2 \vdash \phi_2 (b'_3) \) where \( b_3 = (\varepsilon_{11} \como \varepsilon_{12}) (b_1 \ [\oplus] b_2)_{(g_{11} \como g_{12})} : \text{Bool}_{g_{11}} \), then

\[
(\varepsilon_{21} \como \varepsilon_{22}) (b_1 \ [\oplus] b_2)_{(g_{21} \como g_{22})} : \text{Bool}_{g_{22}}.
\]

By Lemma E.26, \( (\varepsilon_{11} \como \varepsilon_{12}) \subseteq (\varepsilon_{21} \como \varepsilon_{22}) \). Also \( (g_{11} \como g_{12}) \subseteq (g_{21} \como g_{22}) \).

Therefore \( t_2^{U_1} \subseteq t_2^{U_2} \). As \( \Omega' = \Omega, \mu_1 = \mu_1' \) and \( \mu_2 = \mu_2' \) then \( \Omega' \vdash \mu_1' \subseteq \mu_2' \).
Case ($\leftarrow\rightarrow$prot). We know that $t_{11}^{U_1} = \text{prot}_{\mathcal{E}_{\text{prot}}(U_1)}^{g_1(U_1)}\phi'_1(e_1 u_1)$, then by $(\subseteq_{\text{prot}}) t_{12}^{U_2} = \text{prot}_{\mathcal{E}_{\text{prot}}(U_2)}^{g_2(U_2)}\phi'_2(e_2 u_2)$, and therefore

$$
g_1' \subseteq g_2' \quad \phi'_1 \subseteq \phi'_2 \quad U_1 \subseteq U_2 \quad \Omega \uplus u_1 \subseteq u_2 \quad \epsilon_1 \subseteq \epsilon_2$$

$$\Omega \uplus \text{prot}_{\mathcal{E}_{\text{prot}}(U_1)}^{g_1(U_1)}\phi'_1(e_1 u_1) \subseteq \text{prot}_{\mathcal{E}_{\text{prot}}(U_2)}^{g_2(U_2)}\phi'_2(e_2 u_2)$$

for some $\epsilon_2, u_2, U_2$ and $\epsilon_{\text{Ell}}$, where $u_1 \in \mathbb{T}[U_1']$ and $u_2 \in \mathbb{T}[U_2']$. If $t_{11}^{U_1} | \mu_1 \xrightarrow{\phi_1} (e_1 \notin \epsilon_1) (u_1 \not\in \epsilon_1)$ then by Lemma E.26, $(\epsilon_2 \notin \epsilon_{\text{Ell}}) \subseteq (e_2 \notin \epsilon_{\text{Ell}})$, and so $t_{12}^{U_2} | \mu_2 \xrightarrow{\phi_2} (e_2 \notin \epsilon_{\text{Ell}}) (u_2 \not\in \epsilon_{\text{Ell}})$. Therefore by $\subseteq_{\text{i-lbl}}$, $(e_1 \notin \epsilon_{\text{Ell}})(u_1 \not\in \epsilon_{\text{Ell}})$, $U_1 \subseteq U_2 \subseteq (e_2 \notin \epsilon_{\text{Ell}}) (u_2 \not\in \epsilon_{\text{Ell}})$. As $\Omega' = \Omega$, $\mu'_1 = \mu_1$ and $\mu'_2 = \mu_2$ then $\Omega' \uplus \mu'_1 \subseteq \mu'_2$.

Case ($\rightarrow$app). We know that $t_{11}^{U_1} = e_{11}(\lambda x^{U_{11}}. t_{12}^{U_{12}})_{U_1}^{g_1(U_1)}\phi'_1(e_1 u_1)$ then by $(\subseteq_{\text{app}}) t_{11}^{U_1}$ must have the form $t_{12}^{U_2} = e_{21}(\lambda x^{U_{12}}. t_{22}^{U_{22}})_{U_2}^{g_2(U_2)}\phi'_2(e_2 u_2)$ for some $e_{21}, x^{U_{12}}, t_{22}^{U_{22}}, U_3, U_4, e_{22}, g_{22}, g_2$ and $u_2$. Let us pose $e_\epsilon = e_{12} \subseteq \epsilon \subseteq \text{idom}(e_{11})$ and $\phi'_1 = (e_1 \notin \epsilon) \iota_{\text{lbl}}(e_{11})) \subseteq \epsilon \subseteq \epsilon_{\text{Ell}}(e_{11})$, $\phi'_2 = (e_2 \notin \epsilon) \iota_{\text{lbl}}(e_{21})) \subseteq \epsilon \subseteq \epsilon_{\text{Ell}}(e_{21})$. Then $t_{11}^{U_1} | \mu_1 \xrightarrow{\phi_1} \text{prot}_{\mathcal{E}_{\text{prot}}(U_1)}^{g_1(U_1)}\phi'_1(e_1 u_1) | \mu_1$ with $t'_{11} = [(e_1 u_1 : U_1)]/x^{U_{11}}] t_{22}^{U_{22}}$.

Also, let us pose $e_\epsilon = e_{22} \subseteq \epsilon \subseteq \text{idom}(e_{21})$ and $\phi'_2 = (e_2 \notin \epsilon) \iota_{\text{lbl}}(e_{21})) \subseteq \epsilon \subseteq \epsilon_{\text{Ell}}(e_{21})$, $\phi'_2 = (e_2 \notin \epsilon) \iota_{\text{lbl}}(e_{22})) \subseteq \epsilon \subseteq \epsilon_{\text{Ell}}(e_{22})$. Then $t_{11}^{U_1} | \mu_2 \xrightarrow{\phi_2} \text{prot}_{\mathcal{E}_{\text{prot}}(U_2)}^{g_2(U_2)}\phi'_2(e_2 u_2) | \mu_2$ with $t'_{12} = [(e_2 u_2 : U_2)]/x^{U_{12}}] t_{22}^{U_{22}}$.

As $\Omega \uplus t_{11}^{U_1} \subseteq t_{12}^{U_1}$, then $u_1 \subseteq u_2, \epsilon_{12} \subseteq \epsilon_{22}$ and idom($e_{11}$) $\subseteq$ idom($e_{21}$) as well, then by Prop. E.24 $\epsilon_{12} \subseteq \epsilon_{22}$. Then $e_{11} u_1 : U_1 \subseteq e_{22} u_2 : U_2$ by $(\subseteq_{\text{i-lbl}})$.

We also know by $(\subseteq_{\text{app}})$ and $(\subseteq_{\text{i-lbl}})$ that $\Omega \uplus \{x^{U_{12}} \subseteq x^{U_{11}}\} \vdash t_{12}^{U_{22}} \subseteq t_{22}^{U_{22}}$. By Substitution preserves precision (Prop E.23) $t'_{11} \subseteq t'_{12}$, therefore $\text{idom}(e_{11}) t'_{11} : U_2 \subseteq \text{idom}(e_{22}) t'_{12} : U_4$ by $(\subseteq_{\text{i-lbl}})$. Also $g_1 \subseteq g_2$, $\text{ilbl}(e_{11}) \subseteq \text{ilbl}(e_{21})$, $g'_1 \subseteq g'_2$ and by Lemma E.24 and E.26, $\epsilon'_{12} \subseteq \epsilon'_{22}$. Also, as $\phi_1, g_1 \subseteq \phi_2, g_2$ by monotonicity of the join $g_1 \vee \phi_1, g_1 \subseteq g_2 \vee \phi_2, g_2$, and as $\phi_1, g_1 \subseteq \phi_2, g_2$ also by monotonicity of the join $g'_1 \vee \phi_1, g'_1 \subseteq g'_2 \vee \phi_2, g'_2$. Then by $(\subseteq_{\text{prot}}) t_{12}^{U_1} \subseteq t_{12}^{U_2}$. As $\Omega' = \Omega$, $\mu'_1 = \mu_1$ and $\mu'_2 = \mu_2$ then $\Omega' \uplus \mu'_1 \subseteq \mu'_2$.

Case ($\leftarrow$if-true). $t_{11}^{U_1}$ is $\text{if}_{\mathcal{E}_{\text{if}}(U_1)}^{g_{\mathcal{E}_{\text{if}}(U_1)}} \text{true}_{\mathcal{E}_{\text{if}}(U_1)}$ then else $e_{12} t_{12}^{U_{12}} e_{13} t_{13}^{U_{13}}$ then by $(\subseteq_{\text{i-lbl}})$ $t_{11}^{U_1}$ has the form $t_{12}^{U_1} = e_{21} t_{22}^{U_{12}} t_{23}^{U_{22}} t_{22}^{U_{22}}$ for some $e_{21}, e_{22}, e_{23}, t_{22}^{U_{22}}$. Then $t_{11}^{U_1} | \mu_1 \xrightarrow{\phi_1} \text{prot}_{\mathcal{E}_{\text{prot}}(U_1)}^{g_1(U_1)}\phi'_1(e_1 u_1) | \mu_1$, and $t_{12}^{U_1} | \mu_2 \xrightarrow{\phi_2} \text{prot}_{\mathcal{E}_{\text{prot}}(U_2)}^{g_2(U_2)}\phi'_2(e_2 u_2) | \mu_2$.

Where $\phi'_1 = ((\phi_1, g_1, \text{ilbl}(e_{21})) \subseteq (g'_1 \vee \phi_1, g_1))$. Using the fact that $t_{11}^{U_1} \subseteq t_{12}^{U_1}$ we know that $e_{12} \subseteq e_{22}$, $t_{12}^{U_2} \subseteq t_{22}^{U_{22}}$, $g'_1 \subseteq g'_2$, as $\phi_1, g_1 \subseteq \phi_2, g_2$ and $g_1 \subseteq g_2$, and as join is monotone, $\phi_1, g_1 \subseteq \phi_2, g_2$. Also as $\phi_1, g_1 \subseteq \phi_2, g_2$ and $g'_1 \subseteq g'_2$, and as join is monotone, $\phi_1, g_1 \subseteq \phi_2, g_2$. By Prop E.18, we know that $U_{12} \subseteq U_{22}$ and $U_{13} \subseteq U_{23}$. Therefore by Prop E.28 ($U_{12} \vee U_{13} \subseteq (U_{22} \vee U_{23})$). Also as $\phi_1, g \subseteq \phi_2, g$ and $\text{ilbl}(e_{21}) \subseteq \text{ilbl}(e_{22})$ then by Lemma E.26 ($\phi_1, g \vee \text{ilbl}(e_{21}) \subseteq (\phi_2, g \vee \text{ilbl}(e_{22})$). Then using $(\subseteq_{\text{prot}})$, $t_{12}^{U_1} \subseteq t_{12}^{U_2}$. As $\Omega' = \Omega$, $\mu'_1 = \mu_1$ and $\mu'_2 = \mu_2$ then $\Omega' \uplus \mu'_1 \subseteq \mu'_2$.

Case ($\rightarrow$if-false). Same as case $\leftarrow$if-true, using the fact that $e_{13} \subseteq e_{23}$ and $t_{13}^{U_2} \subseteq t_{23}^{U_2}$.
Case (→ref). We know that $t_1^{U_1} = \text{ref}_{\alpha_1}^{U_1} e_1 u_1$, then by ($\in_{\text{ref}}$) $t_1^{U_1} = \text{ref}_{\alpha_2}^{U_2} e_2 u_2$, and therefore

$$U_1'' \subseteq U_2'' \quad \epsilon_1 \subseteq \epsilon_2 \quad g_{e_1} \subseteq g_{e_2}$$

$$\epsilon_1 \subseteq \epsilon_2 \quad \Omega \sqcap u_1 \subseteq u_2$$

$$\Omega \vdash \text{ref}_{\alpha_1}^{U_1} e_1 u_1 \subseteq \text{ref}_{\alpha_2}^{U_2} e_2 u_2$$

for some $\epsilon_2, u_2, U_2'$ and $\epsilon_2$, where $u_1 \in T[U_1]$ and $u_2 \in T[U_2]$. If

$$t_1^{U_1} \mid \mu_1 \xrightarrow{\phi_1} \phi_1^{U_1} \mid \mu_1^{[U_1'' \rightarrow v_1']}$$

for some $v_1'$ and where $v_1' = e'(u_1 \rightarrow g_{r_1}) : U_1''$, $\epsilon_1' = \epsilon_1 \rightarrow (\phi_{1, \epsilon} \circ \epsilon_1)$. Therefore, $t_1^{U_2} \mid \mu_2 \xrightarrow{\phi_2} \phi_2^{U_2} \mid \mu_2^{[U_2'' \rightarrow v_2]}$, for some $v_2'$ and where $v_2' = e'(u_2 \rightarrow g_{r_2}) : U_2''$, $\epsilon_2' = \epsilon_2 \rightarrow (\phi_{2, \epsilon} \circ \epsilon_2)$. By Lemma E.26 and E.24, $\epsilon_1' \subseteq \epsilon_2'$. Also as $\phi_{1, \epsilon} \subseteq \phi_{2, \epsilon}$ and $U_1 \subseteq U_2$, then by definition of $\rho$, $\epsilon_1'' \subseteq \epsilon_2''$. Then using $\Omega' = \Omega \cup \{U_1'' \subseteq U_2''\}$ and that $\bot \subseteq \bot$, by ($\in_{\equiv}$) we can see that $\Omega' \vdash 1_1'' \subseteq 1_2''$. As $g_{r_1} \subseteq g_{r_2}$, by monotonicity of the join, $u_1 \rightarrow g_{r_1} \subseteq u_2 \rightarrow g_{r_2}$. Therefore using $\equiv$; $\Omega' \vdash v_1' \subseteq v_2'$. Also because $\Omega \subseteq \Omega'$, then by the fact that $\Omega \vdash \mu_1 \subseteq \mu_2$, it is easy to see that $\Omega \cup \{U_1'' \subseteq U_2''\} \vdash 1_1'' \subseteq 1_2''$, i.e. $\Omega' \vdash \mu_1' \subseteq \mu_2'$.

Case (→deref). We know that $t_1^{U_1} = !\text{Ref}_{\alpha_1}^{U_1} e_1 g_{g_1} u_1 \mid t_1^{U_2} = !\text{Ref}_{\alpha_2}^{U_2} e_2 g_{g_2} u_2$ and so

$$\Omega \vdash !\text{Ref}_{\alpha_1}^{U_1} e_1 g_{g_1} u_1 \subseteq !\text{Ref}_{\alpha_2}^{U_2} e_2 g_{g_2} u_2$$

As $\Omega \vdash \mu_1 \subseteq \mu_2$, using ($\equiv_{\mu}$) then $\Omega \vdash \mu_1([U_1'') \subseteq \mu_2([U_2''])$. Then

$$\equiv_{\mu} \text{Ref}_{\alpha_1}^{U_1} e_1 g_{g_1} u_1 \mid \mu_1 \xrightarrow{\phi_1} \text{prot}_{\alpha_1}^{U_1} \phi_1'(\text{iref}(\epsilon_1) \mu_1([U_1'']))$$

$$\equiv_{\mu} \text{Ref}_{\alpha_2}^{U_2} e_2 g_{g_2} u_2 \mid \mu_2 \xrightarrow{\phi_2} \text{prot}_{\alpha_2}^{U_2} \phi_2'(\text{iref}(\epsilon_2) \mu_2([U_2'']))$$

Where $\phi' = (\phi_{1, \epsilon} \rightarrow (\phi_{1, \epsilon} \\ \phi_{2, \epsilon} \rightarrow \phi_{2, \epsilon} g_{g_1} g_{g_2})$. By monotonicity of the join $\phi_{1, \epsilon} \rightarrow (\phi_{1, \epsilon} \rightarrow \phi_{2, \epsilon} \rightarrow \phi_{2, \epsilon} g_{g_1} g_{g_2})$ and $\phi_{1, \epsilon} \rightarrow (\phi_{1, \epsilon} \rightarrow \phi_{2, \epsilon} g_{g_1} g_{g_2})$. As $\epsilon_1 \subseteq \epsilon_2$, then by Lemma E.29, $\text{iref}(\epsilon_1) \subseteq \text{iref}(\epsilon_2)$. Then Using ($\equiv_{\mu}$) we can conclude that $\Omega \vdash t_1^{U_1} \subseteq t_1^{U_2}$. As $\Omega' = \Omega, \mu_1 = \mu_1'$ and $\mu_2 = \mu_2'$ then also $\Omega' \vdash \mu_1' \subseteq \mu_2'$.

Case (→assign). We know that $t_1^{U_1} = e_11^{g_{g_1}} u_1 \mid t_1^{U_2} = e_21^{g_{g_2}} u_2$ and so

$$\Omega \vdash e_11^{g_{g_1}} u_1 \subseteq e_21^{g_{g_2}} u_2$$

Then

$$t_1^{U_1} \mid \mu_1 \xrightarrow{\phi_1} \text{unit}_1 \mid \mu_1^{[U_1' \rightarrow v_1]}, \text{where} \ v_1 = e'(u_1 \rightarrow (g_{r_1} \rightarrow g_{r_1})) : U_1', \text{and} \ \epsilon_1' = (\epsilon_1 \circ \epsilon_1) \rightarrow (\phi_{1, \epsilon} \rightarrow \text{ilbl}(\epsilon_1))$$

Similarly, then

$$t_1^{U_2} \mid \mu_2 \xrightarrow{\phi_2} \text{unit}_2 \mid \mu_2^{[U_2' \rightarrow v_2]}, \text{where} \ v_2 = e'(u_2 \rightarrow (g_{r_2} \rightarrow g_{r_2})) : U_2', \text{and} \ \epsilon_2' = (\epsilon_2 \circ \epsilon_2) \rightarrow (\phi_{2, \epsilon} \rightarrow \text{ilbl}(\epsilon_2))$$

We need to prove that $\mu_1' = \mu_1^{[U_1' \rightarrow v_1]} \subseteq \mu_2' = \mu_2^{[U_2' \rightarrow v_2]}$. Because $\Omega \vdash \mu_1 \subseteq \mu_2$ then $\Omega \vdash t_1^{U_1} \subseteq t_2^{U_2}$ by ($\equiv_{\mu}$). By well formedness of $\Omega$ we also know that $U_1 \subseteq U_2$. Therefore, by Lemmas E.24, E.25 and E.26 $\epsilon_1' \subseteq \epsilon_2'$. Then using ($\equiv$), $v_1 \subseteq v_2$, following that $\Omega' = \Omega \vdash \mu_1' \subseteq \mu_2'$.

\[\square\]

**Proposition E.31 (Dynamic Guarantee).** Suppose $t_1^{U_1} \subseteq t_1^{U_2}$, $\phi_1 \subseteq \phi_2$, and $\mu_1 \subseteq \mu_2$. If $t_1^{U_1} \mid \mu_1 \xrightarrow{\phi_1} t_1^{U_2} \mid \mu_1'$ then $t_1^{U_2} \mid \mu_2 \xrightarrow{\phi_2} t_2^{U_2} \mid \mu_2'$ where $t_1^{U_2} \subseteq t_2^{U_2}$ and $\mu_1' \subseteq \mu_2'$.

**Proof.** We prove the following property instead: Suppose $\Omega \vdash t_1^{U_1} \subseteq t_1^{U_2}$, $\phi_1 \subseteq \phi_2$, and $\Omega \vdash \mu_1 \subseteq \mu_2$. If $t_1^{U_1} \mid \mu_1 \xrightarrow{\phi_1} t_2^{U_1} \mid \mu_1'$ then $t_1^{U_2} \mid \mu_2 \xrightarrow{\phi_2} t_2^{U_2} \mid \mu_2'$ where $\Omega' \vdash t_1^{U_1} \subseteq t_2^{U_2}$ and $\Omega' \vdash \mu_1' \subseteq \mu_2'$, for some $\Omega' \supseteq \Omega$.

By induction on the structure of a derivation of $t_1^{U_1} \subseteq t_1^{U_2}$. For simplicity we omit the $\equiv$ notation on precision relations when it is not relevant for the argument.
Case (R→). Ω ⊢ t^{U_1}_1 ⊑ t^{U_2}_1, Ω ⊢ μ_1 ⊑ μ_2 and
t^{U_1}_1 | μ_1 \xrightarrow{\phi_1} t^{U_2}_1 | μ'_1. By dynamic guarantee of \(\rightarrow\) (Prop E.30), t^{U_2}_1 | μ_2 \xrightarrow{\phi_2} t^{U_2}_1 | μ'_2 where Ω' + t^{U_1}_2 ⊑ t^{U_2}_2, Ω' + μ'_1 ⊑ μ'_2 for some Ω' ⊇ Ω. And the result holds immediately.

Case (Rf). t^{U_1}_1 = f_1[t^{U_1}_1]. t^{U_2}_1 = f_2[t^{U_2}_1]. We know that Ω ⊢ f_1[t^{U_1}_1] ⊑ f_2[t^{U_2}_1]. By using Prop E.18, U'_1 ⊑ U'_2. By Prop E.22, we also know that Ω + t^{U_1}_1 ⊑ t^{U_2}_1. By induction hypothesis, t^{U_1}_1 | μ_1 \xrightarrow{\phi_1} t^{U_2}_1 | μ'_1, t^{U_2}_1 | μ_2 \xrightarrow{\phi_2} t^{U_2}_1 | μ'_2, Ω' + t^{U_1}_1 ⊑ t^{U_2}_1, and Ω' + μ'_1 ⊑ μ'_2 for some Ω' ⊇ Ω.

Then by Prop E.21 then Ω' + f_1[t^{U_1}_1] ⊑ f_2[t^{U_2}_1] and the result holds.

Case (Rprot). Then t^{U_1}_1 = prot_{\epsilon_1, g_1, \phi'_1(\epsilon_1 t^{U_1}_1)}^{g_1, U_1} and t^{U_2}_1 = prot_{\epsilon_2, g_2, \phi'_2(\epsilon_2 t^{U_1}_1)}^{g_2, U_2}.

As t^{U_1}_1 ⊑ t^{U_2}_1 then by (\subseteqprot), t^{U_1}_1 ⊑ t^{U_2}_1, \phi_1 ⊑ \phi_2, \epsilon_1 ⊑ \epsilon_2, g_1 ⊑ g_2, g'_1 ⊑ g'_2, and \epsilon_1 \subseteq \epsilon_2. By (Rprot), t^{U_1}_1 | μ \xrightarrow{\phi'_1} t^{U_2}_1 | μ' and by induction hypothesis, t^{U_1}_2 ⊑ t^{U_2}_2 and Ω' + μ'_1 ⊑ μ'_2 for some Ω' ⊇ Ω.

But then by (\subseteqprot),
Ω' + prot_{\epsilon_1, g_1, \phi'_1(\epsilon_1 t^{U_1}_1)}^{g_1, U_1} ⊑ prot_{\epsilon_2, g_2, \phi'_2(\epsilon_2 t^{U_1}_1)}^{g_2, U_2} and the result holds.

Case (Rg). t^{U_1}_1 = g_1[et_1], t^{U_2}_1 = g_2[et_2], where Ω ⊢ g_1[et_1] ⊑ g_2[et_2]. Also et_1 → c et'_1 and et_2 → c et'_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 E.20, \epsilon_{11} \subseteq \epsilon_{12} \subseteq \epsilon_{21}, and by (\subseteq) \epsilon_{12} \subseteq \epsilon_{22}, v_1 \subseteq v_2 and U_1 \subseteq U_2. Then as et_1 → c (\epsilon_{12} \circ c \epsilon_{11}) v_1 and et_2 → c (\epsilon_{22} \circ c \epsilon_{21}) v_2 then, by Prop E.24 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 E.19, it follows that Ω + g_1[et'_1] ⊑ g_1[et'_2]. As Ω' = Ω, μ'_1 = μ_1 and μ_2 = μ'_2 then Ω' + μ'_1 ⊑ μ'_2.

Case (Rprotg). Analogous to (Rprot) case but using → c instead.

\[\square\]
E.6 Noninterference

In this section we present the proof of noninterference for GSLRef. We use a logical relation that is more general than the one presented in the paper. The main difference (beside using intrinsic terms), is that the logical relation is no longer indexed by a static security effect. As \( \phi \) embeds the static security effect information, we generalize the logical relation to also relate two different static security effects as well. Section E.6.1 present some auxiliary definitions. Section E.6.2 presents the proof of Noninterference (Prop E.65), which implies Security Type Soundness (Prop 5.5) presented in the paper.

E.6.1 Definitions. We introduce a function \( uval \), which strips away ascriptions from a simple value:

\[
uval : \text{GType} \rightarrow \text{SimpleValue}\\
uval(u) = u\\uval(\varepsilon u :: U) = u.
\]

In order to compare the observable results of program, we introduce the \( rval(\nu) \) operator, which strips away any checking-related information like labels or evidence-carrying ascriptions:

\[
rval : \text{Value} \rightarrow \text{RawValue}\\rval(b_g) = b\\rval(\varepsilon b_g :: U) = b\\rval(\varepsilon \text{unit}_g) = \text{unit}\\rval(\varepsilon \text{unit}_g :: U) = \text{unit}\\rval(\varepsilon \text{unit}_g :: U) = o\\rval(\varepsilon \text{unit}_g :: U) = o\\rval(\varepsilon (\lambda' x^{U_1}.t^{U_2})_g) = (\lambda' x^{U_1}.t^{U_2})\\rval(\varepsilon (\lambda' x^{U_1}.t^{U_2})_g :: U) = (\lambda' x^{U_1}.t^{U_2})
\]

**Definition E.32 (Gradual security logical relations).** For an arbitrary element \( \ell_o \) of the security lattice, the \( \ell_o \)-level gradual security relations are step-indexed and type-indexed binary relations on tuples of security effect, closed terms and stores defined inductively as presented in Figure 40. The notation \( \langle \phi_1, v_1, \mu_1 \rangle \approx_{\ell_o}^k \langle \phi_2, v_2, \mu_2 \rangle : U \) indicates that the tuple of security effect \( \phi_1 \), value \( v_1 \) and store \( \mu_1 \) is related to the tuple of security effect \( \phi_2 \), value \( v_2 \) and store \( \mu_2 \) at type \( U \) for \( k \) steps when observed at the security level \( \ell_o \). Similarly, the notation \( \langle \phi_{t=t_0}, t_{t=t_0}, \mu_{\ell=t_0} \rangle^k \langle \phi_1, \mu_1 \rangle C(U) \) indicates that the tuple of security effect \( \phi_1 \), term \( t_1 \) and store \( \mu_1 \), and the tuple of security effect \( \phi_2 \), term \( t_2 \) and store \( \mu_2 \) are related computations for \( k \) steps, that produce related values and related stores at type \( U \) when observed at the security level \( \ell_o \). Notation \( \mu_1 \approx_{\ell_o}^k \mu_2 \) relates stores \( \mu_1 \) and \( \mu_2 \) for \( k \) steps when observed at security level \( \ell_o \). Finally, notation \( \phi_1 \approx_{\ell_o} \phi_2 \), relates security effect \( \phi_1 \) and \( \phi_2 \) for any number of steps at security level \( \ell_o \).

We say that a value is observable at level \( \ell_o \) if, given a security effect \( \phi \), the value is typeable, the security effect is observable, and the label of the value is sublabel of \( \ell_o \). Also, as value \( v \) can be a casted value, we need to analyze if its underlying evidence justifies that the security level of the bare value is also subsumed by the observer security level. We do this by demanding that the underlying evidence and label is also observable. We say that a security effect is observable if its underlying evidence and static label is also observable. We say that an evidence and label
\[
\langle \phi_1, v_1, \mu_1 \rangle \approx^{k_{\ell_o}}_{\ell_o} \langle \phi_2, v_2, \mu_2 \rangle : U \iff \phi_1 \approx_{\ell_o} \phi_2 \land \mu_1 \approx^{k_{\ell_o}}_{\ell_o} \mu_2 \land \phi_1 \triangleright v_1 \in T[U] \land \text{obsEq}_{\ell_o}(\phi_1 \triangleright v_1, \phi_2 \triangleright v_2) \land (\text{obs}_{\ell_o}(\phi_1 \triangleright v_1) \implies \text{obsRel}^{U}_{\ell_o, \ell_o}(\phi_1, v_1, \mu_1, \phi_2, v_2, \mu_2))
\]

\[
\text{obsRel}^{U}_{\ell_o, \ell_o}(\phi_1, v_1, \mu_1, \phi_2, v_2, \mu_2) \iff (\text{rval}(v_1) = \text{rval}(v_2)) \quad \text{if } U \in \{\text{Bool}_g, \text{Unit}_g, \text{Ref}_g\}
\]

\[
\text{obsRel}^{U_1}_{\ell_o, \ell_o}(\phi_1, v_1, \mu_1, \phi_2, v_2, \mu_2) \iff \forall j \leq k. \forall U' = U_1' \triangleright g_1' \triangleright g_2' U_2', \forall \phi'_1, \phi'_2 \approx_{\ell_o} \phi'_1 \land \phi'_2 \land \phi'_1 \triangleright v'_1 \land \phi'_2 \triangleright v'_2 \land \ell_o \phi'_1, \ell_o \phi'_2 \land \ell_o \phi'_1 \lor \ell_o \phi'_2 \iff \forall \phi'_1, \phi'_2 \approx_{\ell_o} \phi'_1 \land \phi'_2 \land \phi'_1 \triangleright v'_1 \land \phi'_2 \triangleright v'_2 \land \ell_o \phi'_1, \ell_o \phi'_2 \land \ell_o \phi'_1 \lor \ell_o \phi'_2, \text{we have:}
\]

\[
\langle \phi_1, \epsilon'_1 v_1 \triangleright_{U'_1} \epsilon'_2 v'_1, \mu'_1 \rangle \approx^{j}_{\ell_o} \langle \phi_2, \epsilon'_2 v_2 \triangleright_{U'_2} \epsilon'_2 v'_2, \mu'_2 \rangle : C(U_{1''} \triangleright g_2')
\]

Fig. 40. Gradual security logical relations

are observable, if any value with that underlying evidence and static label, can be used used as argument of a function that expects a value with security level \(\ell_o\). If the consistent transitivity check of the reduction of the application does not hold, then it is not plausible that the security level of the value is subsumed by \(\ell_o\), and therefore is not observable. For instance, consider \(\ell_o = L\), evidence
\( \varepsilon = \langle [H, \top], [\bot, \top] \rangle \) and static label \( g = \? \). We can construct any value such as \( v = \varepsilon \text{true} \) :: Bool\(_g\).

The level of the value and the bare value are sublabel of \( \ell_o \). But the evidence describes that at some point during reduction, the security level of the bare value was required to be at least as high as \( H \). Therefore, \( v \) is not observable at level \( L \) (considering \( L \leq H \)), because as \( g \sim (\ell_o) = \langle [\bot, L], [L, L] \rangle \), the consistent transitivity operation \( \langle [H, \top], [\bot, \top] \rangle \circ <^c \langle [\bot, L], [L, L] \rangle \) does not hold.

Two stores are related at \( k \) steps if each value in the heap of the locations they have in common, are related at \( j < k \) steps for any related security effects. We say that store \( \mu_2 \) is the evolution of store \( \mu_1 \), annotated \( \mu_1 \rightarrow_{\ell_o} \mu_2 \) if the domain of \( \mu_1 \) is a subset of \( \mu_2 \).

Two tuples of security effects, values and stores are related for \( k \) steps at type \( \text{Bool}_g \) if the security effects are related, the stores are related for \( k \) steps, the values can be typed as \( \text{Bool}_g \) using the security effects as context (any security effect will do, given that the typing of values do not depend on the security effect). Additionally, both security effect and values must both be either observable or not observable. If the security effect and values are observable then the raw values are the same. Two tuples are observables at type \( \text{Unit}_g \) and \( \text{Ref}_g \) \( U \) analogous to booleans.

Pairs are related at function types similarly to booleans. The difference is that functions can not be compared as booleans. Two functions are related if, given two related values and stores for \( j \leq k \) steps at the argument type, the application of those function to the related values are also related for \( j \) steps at the return type.

Two tuples of terms and stores are related computations for \( k \) steps at type \( U \), first, if the security effects are related, and the stores are related for \( k \) steps. Second the terms must be typed as \( U \) using an observationally higher security effect. Third, if for any \( j < k \) both terms can be reduced for at least \( j \) steps, then the resulting stores are related for the remaining \( k - j \) steps. Finally, if after at least \( j \) steps the resulting terms are irreducible, then the resulting terms are also related values for the remaining \( k - j \) steps at type \( U \). Notice that the logical relation also relates programs that do not terminate as long as after \( k \) steps the new stores are also related.

To define the fundamental property of the step-indexed logical relations we first define how to relate substitutions:

**Definition E.33.** Let \( \rho \) be a substitution and \( \Gamma \) a type substitution. We say that substitution \( \rho \) satisfy environment \( \Gamma \), written \( \rho \models \Gamma \), if and only if \( \text{dom}(\rho) = \Gamma \).

**Definition E.34 (Related substitutions).** Tuples \( \langle \phi_1, \rho_1, \mu_1 \rangle \) and \( \langle \phi_2, \rho_2, \mu_2 \rangle \) are related on \( k \) steps under \( \Gamma \), notation \( \Gamma \vdash \langle \phi_1, \rho_1, \mu_1 \rangle \approx \langle \phi_2, \rho_2, \mu_2 \rangle \), if \( \rho_1 \models \Gamma \), \( \mu_1 \approx \ell_o, \mu_2 \) and

\[
\forall x^U \in \Gamma. \langle \phi_1, \rho_1(x^U), \mu_1 \rangle \approx \langle \phi_2, \rho_2(x^U), \mu_2 \rangle : U
\]

**E.6.2 Proof of noninterference.**

**Lemma E.35 (Noninterference for booleans).** Suppose \( k > 0 \), and

- an open term \( \phi \bimap t^U \in T[\text{Bool}_{\ell_o}] \) where \( \text{FV}(t) = \{ x^{U_1} \} \) with \( \text{label}(U_1) \not\sim \ell_o \)
- two compatible valid stores \( t^U \bimap \mu_1, \mu_1 \approx \ell_o, \mu_2 \)

Then for any \( j < k \), \( v_1, v_2 \in T[\text{Unit}_1] \), if both

- \( t^U[v_1/x^{U_1}] \bimap \mu_1 \xrightarrow{\phi} j v_1' \bimap \mu_1' \)
- \( t^U[v_2/x^{U_1}] \bimap \mu_2 \xrightarrow{\phi} j v_2' \bimap \mu_2' \)

we have that \( \text{rval}(v_1') = \text{rval}(v_2') \), and \( \mu_1' \approx \ell_o, \mu_2' \).

**Proof.** The result follows as a special case of Proposition E.65 below. \( \square \)
In this theorem, we treat $t^U$ as a program that takes $x^U_i$ as its input. Furthermore, the security level $g' = \text{label}(U_i)$ of the input is not subsumed by the security level $\ell_o$ of the observer. As such, noninterference dictates that changing non-observable input must not change the observable value of the output (i.e., change true to false or vice-versa). However, this theorem is technically termination-insensitive in that it is vacuously true if a change of inputs changes a program that terminates with a value into one that either terminates with an error, or does not terminate at all. If a program does not terminate after any number of steps, then at least the stores are related at observation level $\ell_o$.

Note that we compare equality of raw values at first-order type. Restricting attention to first-order types (i.e., Bool) is common when investigating observational equivalence of typed languages. We strip away security information because a person or client who uses the program ultimately observes only the raw value that the program produces.

Also, gradual security dynamically traps some information leaks, so a change in equivalent inputs may cause a program that previously yielded a value or diverged to now produce an error. This change in behavior falls under the notion of termination-insensitive, since yielding an error is simply a third form of termination behavior (in addition to producing a value and diverging).

Finally, we use notation $t^S \mid \mu \xrightarrow{k} t^{S'} \mid \mu'$ to describe that configuration $t^S \mid \mu$ reduces, in at most $k$ steps, to configuration $t^{S'} \mid \mu'$.

**Lemma E.36.** Consider $\epsilon_1 \vdash g \triangleleft g'$. If $\forall \epsilon_2$ such that $\epsilon_2 \vdash g' \triangleleft \ell_o$, $\epsilon_1 \circ_k \epsilon_2 \vdash g \triangleleft \ell_o$ is not defined. Then if $\epsilon_3 \vdash g' \triangleleft g''$, then $\forall \epsilon_4$ such that $\epsilon_4 \vdash g'' \triangleleft \ell_o$, then $(\epsilon_1 \circ_k \epsilon_3) \circ_k \epsilon_4 \vdash g \triangleleft \ell_0$ is not defined.

**Proof.** Applying associativity: $(\epsilon_1 \circ_k \epsilon_3) \circ_k \epsilon_4 = \epsilon_1 \circ_k (\epsilon_3 \circ_k \epsilon_4)$, but $(\epsilon_3 \circ_k \epsilon_4) \vdash g'' \triangleleft \ell_o$, and we know that $\epsilon_1 \circ_k \epsilon_2$ is not defined $\forall \epsilon_2$ such that $\epsilon_2 \vdash g' \triangleleft \ell_o$. Therefore $(\epsilon_1 \circ_k \epsilon_3) \circ_k \epsilon_4 \vdash g \triangleleft \ell_0$ is not defined and the result holds. \[\Box\]

**Lemma E.37.** Consider $\epsilon_1 \vdash g \triangleleft g'$. If $\forall \epsilon_2$ such that $\epsilon_2 \vdash g' \triangleleft \ell_o$, $\epsilon_1 \circ_k \epsilon_2 \vdash g \triangleleft \ell_o$ is not defined. Also $\epsilon_0 \vdash g_1 \triangleleft g_2$. If $\epsilon_3 \vdash g_2 \vdash g' \triangleleft \ell_o$, then $(\epsilon_0 \circ_k \epsilon_1) \circ_k \epsilon_3 \vdash g_1 \land g \triangleleft \ell_o$ is not defined.

**Proof.** Let us prove that if $(\epsilon_0 \circ_k \epsilon_1) \circ_k \epsilon_3 \vdash g_1 \land g \triangleleft \ell_o$ is defined, then $\epsilon_1 \circ_k \epsilon_2$ is defined.

As join is monotone $\exists \epsilon'_0$ such that $\epsilon'_0 \vdash g' \leq g_2 \land g'$. Suppose $\epsilon_0 = ([\ell_{11}, \ell_{12}], [\ell_{21}, \ell_{22}])$, $\epsilon_0 = ([\ell_{31}, \ell_{32}], [\ell_{41}, \ell_{42}])$, $\epsilon'_0 = ([\ell_{51}, \ell_{52}], [\ell_{61}, \ell_{62}])$, and $\epsilon_3 = ([\ell_{71}, \ell_{72}], [\ell_{81}, \ell_{82}])$.

As $\epsilon_0 \circ_k \epsilon_1 = ([\ell_{11} \land \ell_{31}, \ell_{12} \land \ell_{32}], [\ell_{21} \lor \ell_{41}, \ell_{22} \lor \ell_{42}])$ is defined, then $\ell_{11} \land \ell_{31} \leq \ell_{12} \land \ell_{32}$ and $\ell_{21} \lor \ell_{41} \leq \ell_{22} \lor \ell_{42}$. Also as

$$(\epsilon_0 \circ_k \epsilon_1) \circ_k \epsilon_3 = ([\ell_{11} \land \ell_{31}, \ell_{12} \land \ell_{32}] \land ((\ell_{22} \lor \ell_{42}) \land \ell_{72}) \land \ell_{82}],$$

is defined then $\ell_{41} \lor \ell_{41} \land \ell_{71} \leq ((\ell_{22} \lor \ell_{42}) \land \ell_{72})$, $\ell_{11} \land \ell_{31} \leq ((\ell_{22} \lor \ell_{42}) \land \ell_{72})$, $\ell_{11} \land \ell_{31} \leq \ell_{82}$, and $\ell_{21} \lor \ell_{41} \land \ell_{71} \leq \ell_{82}$.

If we choose $\epsilon'_0$ as the interior of the judgment, then we do not get new information, therefore $[\ell_{21}, \ell_{22}] \subseteq [\ell_{51}, \ell_{52}]$, i.e. $\ell_{51} \leq \ell_{21}$ and $\ell_{22} \leq \ell_{52}$. Using the same argument $\ell_{61} \leq \ell_{71}$ and $\ell_{72} \leq \ell_{62}$. Then

$$\epsilon'_0 \circ_k \epsilon_3 = \Delta^k([\ell_{51}, \ell_{52}], [\ell_{61}, \ell_{62}] \cap [\ell_{71}, \ell_{72}], [\ell_{81}, \ell_{82}])$$

$$= \Delta^k([\ell_{51}, \ell_{52}], [\ell_{61} \lor \ell_{71}, \ell_{62} \land \ell_{72}], [\ell_{81}, \ell_{82}])$$

$$= \Delta^k([\ell_{51}, \ell_{52}], [\ell_{71}, \ell_{72}], [\ell_{81}, \ell_{82}])$$
which is defined if \( \ell_{51} \leq \ell_{72}, \ell_{71} \leq \ell_{82} \) and \( \ell_{51} \leq \ell_{82} \). But \( \ell_{51} \leq \ell_{21} \leq \ell_{21} \lor \epsilon_{41} \lor \ell_{71} \leq (\ell_{22} \lor \epsilon_{42}) \lor \ell_{72} \leq \ell_{72}, \ell_{51} \leq \ell_{21} \leq \ell_{21} \lor \epsilon_{41} \lor \ell_{71} \leq \ell_{82} \) and \( \ell_{71} \leq \ell_{21} \lor \epsilon_{41} \lor \ell_{71} \leq \ell_{82} \).

Therefore

\[
\epsilon'_0 \circ \epsilon_3 = \{[\ell_{51}, \ell_{52} \land \ell_{72} \land \ell_{82}], [\ell_{51} \lor \epsilon_{71} \lor \ell_{81}, \ell_{82}])
\]

Using the same method, \( \epsilon_1 \circ \epsilon_3 \) is defined if \( \ell_{21} \lor \epsilon_{51} \leq \ell_{22} \land (\ell_{52} \land \ell_{72} \land \ell_{82}), \ell_{11} \leq \ell_{22} \land (\ell_{52} \land \ell_{72} \land \ell_{82}) \), and \( \ell_{11} \leq \ell_{82} \).

But by definition of \( \ell_{21} \leq \ell_{22} \), also \( \ell_{21} \leq \ell_{22} \leq \ell_{52}, \ell_{21} \leq \ell_{21} \lor \epsilon_{41} \lor \ell_{71} \leq (\ell_{22} \lor \epsilon_{42}) \land \ell_{72} \leq \ell_{72}, \ell_{21} \leq \ell_{21} \lor \epsilon_{41} \lor \ell_{71} \leq \ell_{82} \), and \( \ell_{51} \leq \ell_{71} \leq \ell_{72} \), therefore \( \ell_{21} \lor \epsilon_{51} \leq \ell_{22} \land (\ell_{52} \land \ell_{72} \land \ell_{82}) \).

Also \( \ell_{11} \leq \ell_{22} \leq \ell_{52}, \ell_{11} \leq \epsilon_{31} \leq (\ell_{22} \lor \epsilon_{42}) \land \ell_{72} \leq \ell_{72}, \ell_{11} \leq \ell_{11} \lor \epsilon_{31} \leq \ell_{82} \), therefore \( \ell_{11} \leq \ell_{22} \land (\ell_{52} \land \ell_{72} \land \ell_{82}) \), and \( \ell_{11} \leq \ell_{82} \).

Then as \( \epsilon_1 \circ (\epsilon'_0 \circ \epsilon_3) \) is defined then if we choose \( \epsilon_2 = (\epsilon'_0 \circ \epsilon_3) \lor g' \leq \ell_0 \), the result holds.

\[\square\]

**Lemma E.38 (Associativity).** Consider \( \epsilon_1, \epsilon_2 \) and \( \epsilon_3 \), such that \( \epsilon_1 \lor g_1 \leq g_2, \epsilon_2 \lor g_2 \leq g_3 \) and \( \epsilon_3 \lor g_3 \leq g_4 \). \( (\epsilon_1 \circ \epsilon_2) \circ \epsilon_3 = \epsilon_1 \circ (\epsilon_2 \circ \epsilon_3) \)

**Proof.** Suppose \( \epsilon_1 = \langle [\ell_{11}, [\ell_{12}, [\ell_{21}, [\ell_{22}]]) \rangle, \epsilon_2 = \langle [\ell_{31}, [\ell_{32}, [\ell_{41}, [\ell_{42}]]) \rangle \rangle, \) and \( \epsilon_3 = \langle [\ell_{51}, [\ell_{52}, [\ell_{61}, [\ell_{62}]]) \rangle \rangle \)

Then

\[
\begin{align*}
(\epsilon_1 \circ \epsilon_2) \circ \epsilon_3 &= \Delta^\epsilon([\ell_{11}, [\ell_{12}, [\ell_{21}, [\ell_{22}]]) \land [\ell_{31}, [\ell_{32}, [\ell_{41}, [\ell_{42}]]) \leq [\ell_{51}, [\ell_{52}, [\ell_{61}, [\ell_{62}]])
\end{align*}
\]

where \( \ell'_{21} = \ell_{12} \land (\ell_{22} \land \ell_{32}) \land \ell_{42} \land \ell_{52} \land \ell_{62} \) and \( \ell'_{61} = \ell_{11} \lor (\ell_{21} \land \ell_{31}) \lor \ell_{41} \lor \ell_{51} \lor \ell_{61} \). But

\[
\begin{align*}
\epsilon_1 \circ \epsilon_2 &= \epsilon_1 \circ \Delta^\epsilon([\ell_{31}, [\ell_{32}, [\ell_{41}, [\ell_{42}]]) \land [\ell_{51}, [\ell_{52}, [\ell_{61}, [\ell_{62}]])
\end{align*}
\]

where \( \ell'_{21} = \ell_{12} \land (\ell_{22} \land \ell_{32}) \land \ell_{42} \land \ell_{52} \land \ell_{62} \) and \( \ell'_{61} = \ell_{11} \lor (\ell_{21} \land \ell_{31}) \lor \ell_{41} \lor \ell_{51} \lor \ell_{61} \), and the result holds.

\[\square\]

**Lemma E.39.** Consider \( \epsilon_1, \epsilon_2 \) and \( \epsilon_3 \) such that \( \epsilon_1 \lor g_1 \leq g_2, \epsilon_2 \lor g_2 \leq g_3 \) and \( \epsilon_3 \lor g_3 \leq g_4 \). If \( \epsilon_1 \lor (\epsilon_2 \circ \epsilon_3) \) is defined, then \( \epsilon_1 \lor (\epsilon_2 \circ \epsilon_3) \) is defined

**Proof.** By definition of join and consistent transitivity, using the property that the join operator is monotone.

\[\square\]
LEMMA E.40. If $\not\exists F_1$, such that $\varepsilon_1 \vdash g_1 \leq g_2$, then $\not\exists F_2$, such that $\varepsilon_2 \vdash g_1 \lor g_3 \leq g_2$.

Proof. By definition of join and consistent transitivity, using the property that the join operator is monotone. □

LEMMA E.41. Consider stores $\mu_1, \mu_2, \mu'_1, \mu'_2$ such that $\mu_1 \rightarrow \mu'_1$, and substitutions $\rho_1$ and $\rho_2$, such that $\Gamma \vdash \langle \phi_1, \rho_1, \mu_1 \rangle \approx_{\ell_0}^k \langle \phi_2, \rho_2, \mu_2 \rangle$, then if for all $j \leq k$, if $\mu'_1 \approx_{\ell_0}^j \mu'_2$ then $\Gamma \vdash \langle \phi_1, \rho_1, \mu'_1 \rangle \approx_{\ell_0}^j \langle \phi_2, \rho_2, \mu'_2 \rangle$.

Proof. By definition of related computations and related stores. The key argument is that given that $\mu_1 \rightarrow \mu'_1$ then $\mu'_1$ have at least the same locations of $\mu_1$ and the values still are related as well given that they still have the same type. □

LEMMA E.42 (Substitution preserves typing). If $\phi \triangleright t^U \in \mathbb{T}[U]$ and $\rho \models \text{FV}(t^U)$ then $\phi \triangleright \rho(t^U) \in \mathbb{T}[U]$.

Proof. By induction on the derivation of $\phi \triangleright t^U \in \mathbb{T}[U]$ □

LEMMA E.43 (Reduction preserves relations). Consider $\phi_i \leq_{\ell_o} \phi'_i, \phi'_i \triangleright t_i \in \mathbb{T}[U], \mu_i \in \text{Store}, t_i \vdash \mu_i$, and $\mu_1 \approx_{\ell_o}^k \mu_2$. Consider $j < k$, posing $t_i | \mu_i \xrightarrow{\phi'_i} t'_i | \mu'_i$, we have $\langle \phi_1, t_1, \mu_1 \rangle \approx_{\ell_o}^k \langle \phi_2, t_2, \mu_2 \rangle : C(U)$ if and only if $\langle \phi_1, t'_1, \mu'_1 \rangle \approx_{\ell_o}^{k-j} \langle \phi_2, t'_2, \mu'_2 \rangle : C(U)$.

Proof. Direct by definition of $\langle \phi_1, t_1, \mu_1 \rangle \approx_{\ell_o}^k \langle \phi_2, t_2, \mu_2 \rangle : C(U)$ and transitivity of $\xrightarrow{\phi'_j}$. □

LEMMA E.44 (Ascription preserves relation). Suppose $\varepsilon \vdash U' \leq U$.

1. If $\langle \varepsilon_1, u, \mu \rangle \approx_{\ell_o}^k \langle \varepsilon_2, u, \mu \rangle : U'$ then $\langle \varepsilon_1, \varepsilon v_1 :: U, \mu_1 \rangle \approx_{\ell_o}^{k+1} \langle \varepsilon_2, \varepsilon v_2 :: U, \mu_2 \rangle : C(U)$.

2. If $\langle \varepsilon_1, t, \mu \rangle \approx_{\ell_o}^k \langle \varepsilon_2, t, \mu \rangle : C(U')$ then $\langle \varepsilon_1, \varepsilon t_1 :: U, \mu_1 \rangle \approx_{\ell_o}^k \langle \varepsilon_2, \varepsilon t_2 :: U, \mu_2 \rangle : C(U)$.

Proof. Following Zdancewic [2002], the proof proceeds by induction on the judgment $\varepsilon \vdash U' \leq U$. The difference here is that consistent subtyping is justified by evidence, and that the terms have to be ascribed to exploit subtyping. In particular, case 1 above establishes a computation-level relation because each ascribed term $(\varepsilon v_1 :: U)$ may not be a value: each value $v_i$ is either a bare value $u_i$ or a casted value $\varepsilon_i u_i :: U_i$, with $\varepsilon_i + S_i \leq U$. In the latter case, $(\varepsilon(\varepsilon_i u_i :: U_i) :: U)$ either steps to error (in which case the relation is vacuously established), or steps to $\varepsilon' u_i :: U$, which is a value. Next if both values were originally observables, then whatever the label of $U$ both values are going to be related. If both values were originally not observables, then by Lemma E.44 both values are going to be still non observables. □

LEMMA E.45. Consider $\varepsilon_{11} \vdash U_1 \leq U_2, \varepsilon_{21} \vdash U_2 \leq U_3,$ and $\varepsilon_{31} = \varepsilon_{11} \circ \varepsilon_{21}$ such that $\varepsilon_{31} \vdash U_1 \leq U_3$. Then if $\varepsilon_{11} \approx_{\ell_o} \varepsilon_{12}$ and $\varepsilon_{21} \approx_{\ell_o} \varepsilon_{22}$, then $\varepsilon_{31} \approx_{\ell_o} \varepsilon_{32}$.

Proof. By induction on $\varepsilon_{11} \approx_{\ell_o} \varepsilon_{12}$. □

LEMMA E.46. If $\langle \phi_1, v_1, \mu_1 \rangle \approx_{\ell_o}^k \langle \phi_2, v_2, \mu_2 \rangle : U$ and, $\phi_1 \triangleright \text{uval}(v_1) \in \mathbb{T}[U_i]$ where $U_i \leq U$, then $\forall U', \varepsilon_1 \approx_{\ell_o} \varepsilon_2, \varepsilon_1 \triangleright U \leq U', \varepsilon_1 = \varepsilon'_i u_i :: U, \varepsilon_2 = \varepsilon'_i \circ \varepsilon_i, we know that \langle \phi_1, \varepsilon'_i \text{uval}(v_1) :: U', \mu_1 \rangle \approx_{\ell_o}^k \langle \phi_2, \varepsilon'_i \text{uval}(v_2) :: U', \mu_1 \rangle : U'$.
Proof. The result follows by induction on relation $\langle \phi_1, v_1, \mu_1 \rangle \approx^{k}_{e_o} \langle \phi_2, v_2, \mu_2 \rangle : U$ using Lemmas E.43, E.45, and observational monotonicity of the transitivity (Lemma E.52).

Lemma E.47 (Downward Closed / Monotonicity). If

1. $\langle \phi_1, v_1, \mu_1 \rangle \approx^{k}_{e_o} \langle \phi_2, v_2, \mu_2 \rangle : U$ then
   $\forall j \leq k, \langle \phi_1, v_1, \mu_1 \rangle \approx^{j}_{e_o} \langle \phi_2, v_2, \mu_2 \rangle : U$

2. $\langle \phi_1, t^U_1, \mu_1 \rangle \approx^{k}_{e_o} \langle \phi_2, t^U_2, \mu_2 \rangle : C(U)$ then
   $\forall j \leq k, \langle \phi_1, t^U_1, \mu_1 \rangle \approx^{j}_{e_o} \langle \phi_2, t^U_2, \mu_2 \rangle : C(U)$

3. $\mu_1 \approx^{k}_{e_o} \mu_2$ then $\forall j \leq k, \mu_1 \approx^{j}_{e_o} \mu_2$

Proof. By induction on type $U$ and the definition of related stores.

Lemma E.48. Consider $e_1 \vdash g_1' \preceq g_1$ and $e_2 \vdash g_2' \preceq g_2$. Then $(\neg obs_{e_o}(e_1 g_1) \land e_1 \leq[e_o] e_2) \Rightarrow \neg obs_{e_o}(e_2 g_2)$.

Proof. Suppose $e_1 = \langle [\ell_{11}, \ell_{12}], [\ell_{13}, \ell_{14}] \rangle$ and $e_2 = \langle [\ell_{21}, \ell_{22}], [\ell_{23}, \ell_{24}] \rangle$.

Also consider $e_1' = g_{e_o}(g_1, \epsilon_o) = \langle [\ell_{11}', \ell_{12}], [\ell_{14}', \epsilon_o] \rangle$ and $e_2' = g_{e_o}(g_2, \epsilon_o) = \langle [\ell_{21}', \ell_{22}], [\ell_{24}, \epsilon_o] \rangle$.

If $e_1 \preceq e_1' = \Delta^\epsilon(\langle [\ell_{11}, \ell_{12}], [\ell_{13}, \ell_{14}], [\ell_{14}, \epsilon_o] \rangle)$ is not defined then

1. $\ell_{13} \lor \ell_{14}' \preceq \ell_{14} \land \ell_{12}'$,
2. $\ell_{14} \preceq \ell_{14} \land \ell_{12}'$, or
3. $\ell_{13} \lor \ell_{14}' \preceq \ell_0$ or
4. $\ell_{14}' \preceq \ell_0$.

By construction we know that $\ell_{11} \preceq \ell_{14}$. By $e_1 \leq[e_o] e_2$ we know that $\ell_{13} \preceq \ell_{23}$.

If $g_1 = \ell$, then $[\ell_{11}', \ell_{12}'] = [\ell_{13}, \ell_{14}] = [\ell, \ell]$, therefore $\ell \preceq \ell_0$. If $\ell_0 \preceq \ell_0$, then $\ell_{23} \lor \ell_{21} \preceq \ell_0$ and the result holds immediately.

If $\ell \preceq \ell_0$, by construction of evidence we know that it must be the case that $\ell_{11} \preceq \ell_{13}$, then either

1. $\ell_0 \lor \ell \preceq \ell$ (which is impossible),
2. $\ell_{13} \preceq \ell \lor \ell$ (which is a contradiction by construction of evidence), or
3. $\ell_0 \lor \ell \preceq \ell_0$ (which contradicts $\ell \preceq \ell_0$) or
4. $\ell_{13} \preceq \ell_0$.

so the only possibility is that $\ell_{13} \preceq \ell_0$, but we know that $\ell_{11} \preceq \ell_{13}$, i.e. $\ell_{11} \preceq \ell$ and that $\ell \preceq \ell_0$, then by transitivity $\ell_{11} \preceq \ell_0$ which is a contradiction so $\ell \preceq \ell_0$ case cannot happen.

If $g_1 = ?$, then $[\ell_{11}', \ell_{12}'] = [\bot, \ell_0]$.

If (1) holds, i.e. $\ell_{13} \preceq \ell_{14}$, by construction we know that $\ell_{13} \preceq \ell_{14}$, therefore it must be the case that $\ell_{13} \preceq \ell_0$, but $\ell_{13} \preceq \ell_{23}$ and the result holds because (3) does not hold for $e_2$.

If (2) holds, i.e. $\ell_{13} \preceq \ell_{14}$, by construction we know that $\ell_{13} \preceq \ell_{14}$, therefore it must be the case that $\ell_{13} \preceq \ell_0$. We also know by construction that $\ell_{11} \preceq \ell_{13}$, then $\ell_{13} \preceq \ell_0$. As $\ell_{13} \preceq \ell_{23}$, then $\ell_{23} \preceq \ell_0$, and therefore (3) does not hold for $e_2$, i.e. $\ell_{23} \lor \ell_{21} \preceq \ell_0$. If (3) holds, i.e. $\ell_{13} \lor \bot \preceq \ell_0$, then $\ell_{13} \preceq \ell_0$, but $\ell_{13} \preceq \ell_{23}$ and the result holds because (3) does not hold for $e_2$.

If (4) holds, i.e. $\ell_{13} \preceq \ell_0$, as $\ell_{11} \preceq \ell_{13} \preceq \ell_{23}$ then $\ell_{23} \preceq \ell_0$, and therefore (3) does not hold for $e_2$, i.e. $\ell_{23} \lor \ell_{21} \preceq \ell_0$.

Lemma E.49. Consider $e_1 \vdash g_1' \preceq g_1$, $e_2 \vdash g_2' \preceq g_2$, and $e_3 = e_1 \lor e_2$ such that $e_3 \vdash g_1 \lor g_2 \preceq g_1 \lor g_2$. Then $(\neg obs_{e_o}(e_1 g_1) \land \neg obs_{e_o}(e_2 g_2)) \Rightarrow obs_{e_o}(e_3 g_1 \lor g_2)$.
Proof. Suppose ε₁ = ⟨[ℓ₁₁, ℓ₁₂], [ℓ₁₃, ℓ₁₄]⟩ and ε₂ = ⟨[ℓ₂₁, ℓ₂₂], [ℓ₂₃, ℓ₂₄]⟩.

Then ε₁ ∨ ε₂ = ε₁ = ⟨[ℓ₁₁ ∨ ℓ₂₁, ℓ₁₂ ∨ ℓ₂₂], [ℓ₁₃ ∨ ℓ₂₃, ℓ₁₄ ∨ ℓ₂₄]⟩. Also consider ε’₁ = gₛ(ℓ₁, ℓ₀) = ⟨[ℓ’₁₁, ℓ’₁₂], [ℓ₀, ℓ₀]⟩, ε’₂ = gₛ(ℓ₂, ℓ₀) = ⟨[ℓ’₂₁, ℓ’₂₂], [ℓ₀, ℓ₀]⟩, and ε’ = gₛ(ℓ₂, ℓ₃, ℓ₀) = ⟨[ℓ’₃₁, ℓ’₃₂], [ℓ₀, ℓ₀]⟩.

If g₁ = ε₁ and g₂ = ε₂, then ℓ’₁₂ = ℓ₁ ∧ ℓ₂, ℓ’₂₂ = ℓ₂ and ℓ’₁₂ = ℓ₁. Also ℓ’₃₁ = ℓ₁ ∧ ℓ₂, ℓ’₂₁ = ℓ₂ and ℓ’₁₁ = ℓ₁.

If g₁ = ε₁ or g₂ = ε₂ (the other case is analogous) then ℓ’₁₂ = ℓ₀ and, ℓ’₁₂ = ℓ₀ and ℓ’₂₂ = ℓ₂ such that ℓ₁ ≤ ℓ₂. Also ℓ’₁₁ = ⊥, ℓ’₂₁ = ℓ₂, but ℓ’₃₁ = ⊥. Therefore ℓ’₁₂ ∨ ℓ’₂₂ and ℓ’₃₁ ≤ ℓ’₁₁ ∨ ℓ’₂₁.

We know that

(1) ℓ₁₁ ∨ ℓ’₁₁ ≤ ℓ₁₁ ∧ ℓ’₁₁,
(2) ℓ₁₁ ≤ ℓ₁₁ ∧ ℓ’₁₁, or
(3) ℓ₁₁ ∨ ℓ’₁₁ ≤ ℓ₀ or
(4) ℓ₁₁ ≤ ℓ₀.

(5) ℓ₂₃ ∨ ℓ’₂₁ ≤ ℓ₂₄ ∧ ℓ’₂₂,
(6) ℓ₂₁ ≤ ℓ₂₄ ∧ ℓ’₂₂, or
(7) ℓ₂₃ ∨ ℓ’₂₁ ≤ ℓ₀ or
(8) ℓ₂₁ ≤ ℓ₀.

We have to prove

(9) (ℓ₁₁ ∨ ℓ₂₃) ∨ ℓ’₃₁ ≤ (ℓ₁₁ ∧ ℓ₂₃) ∧ ℓ’₃₁,
(10) (ℓ₁₁ ∨ ℓ₂₃) ∨ ℓ’₃₁ ≤ (ℓ₁₁ ∧ ℓ₂₃) ∧ ℓ’₃₁.
(11) (ℓ₁₁ ∨ ℓ₂₃) ≤ (ℓ₁₁ ∧ ℓ₂₃) ∧ ℓ’₃₁, or
(12) (ℓ₁₁ ∨ ℓ₂₃) ∨ ℓ’₃₁ ≤ ℓ₀ or
(13) (ℓ₁₁ ∨ ℓ₂₃) ≤ ℓ₀.

(13) follows directly by (4) and (8).

(12) follows from (3) and monotonicity of the join.

By definition of evidence and interior, ℓ’₁₂ ≤ ℓ₀ and ℓ’₃₁ ≤ ℓ’₃₁. Therefore, from (1) ℓ₁₁ ≤ ℓ₁₁ ∧ ℓ’₁₁, from (5) ℓ₂₃ ≤ ℓ₂₄ and therefore ℓ₁₁ ∨ ℓ₂₃ ≤ ℓ₁₁ ∧ ℓ₂₃. Also as ℓ₁₁ ≤ ℓ’₁₁ and ℓ₂₃ ≤ ℓ’₂₃, then ℓ₁₁ ∨ ℓ₂₃ ≤ ℓ’₁₁ ∨ ℓ’₂₃ = ℓ’₁₂. By similar argument ℓ’₃₁ ≤ (ℓ₁₁ ∧ ℓ₂₃) and also ℓ’₁₁ ∨ ℓ’₂₁ ≤ ℓ’₃₁. But then ℓ’₁₁ ∧ ℓ’₂₁ ≤ ℓ’₃₁ and (10) holds.

Lemma E.50. Consider ε₁ ⊢ g₁ ≻ g₂, ε₂ ⊢ g₂ ≻ g₃, and ε₃ = ε₁ ⇨ ε₂ such that ε₁ ⊢ g₁ ≻ g₃. Then obsₐ(ε₁(g₁)) ⇒ (obsₐ(ε₂(g₂)) ∧ obsₐ(ε₂(g₃))).

Proof. Suppose ε₁ = ⟨[ℓ₁, ℓ₂], [ℓ₃, ℓ₄]⟩, ε₂ = ⟨[ℓ₅, ℓ₆], [ℓ₇, ℓ₈]⟩.

ε₁ ⇨ ε₂ = △ⁿ([ℓ₁, ℓ₂], [ℓ₃ ∨ ℓ₅, ℓ₄ ∧ ℓ₆], [ℓ₇, ℓ₈]) = ⟨[ℓ₁, ℓ₂ ∧ ℓ₄ ∧ ℓ₆ ∧ ℓ₈], [ℓ₁ ∨ ℓ₃ ∨ ℓ₅ ∨ ℓ₇, ℓ₈]⟩

Notice that as ℓ₃ ≤ ℓ₁ ∧ ℓ₃ ∧ ℓ₅ ∧ ℓ₇ when ε₁ [≤] ε₃, and as ℓ₇ ≤ ℓ₁ ∧ ℓ₃ ∧ ℓ₅ ∧ ℓ₇ then ε₂ [≤] ε₃. What we have to prove is equivalent to prove that

(¬obsₐ(ε₁(g₁)) ∨ ¬obsₐ(ε₂(g₂))) ⇒ ¬obsₐ(ε₃(g₃))

If ¬obsₐ(ε₁(g₂)) and as ε₁ [≤] ε₃, then by Lemma E.48 ¬obsₐ(ε₃(g₃)) and the result holds. Similarly, if ¬obsₐ(ε₂(g₂)) and as ε₂ [≤] ε₃, then by Lemma E.48 ¬obsₐ(ε₃(g₃)) and the result holds.

Lemma E.51. Consider ε₁ ⊢ g₁ ≻ g₂, ε₂ ⊢ g₂ ≻ g₃, and ε₃ = ε₁ ⇨ ε₂ such that ε₁ ⊢ g₁ ≻ g₃. Then obsₐ(ε₁(g₂)) ⇒ obsₐ(ε₃(g₃)).

Proof. Suppose ε₁ = ⟨[ℓ₁, ℓ₂], [ℓ₃, ℓ₄]⟩, ε₂ = ⟨[ℓ₅, ℓ₆], [ℓ₇, ℓ₈]⟩.

ε₁ ⇨ ε₂ = △ⁿ([ℓ₁, ℓ₂], [ℓ₃ ∨ ℓ₅, ℓ₄ ∧ ℓ₆], [ℓ₇, ℓ₈]) = ⟨[ℓ₁, ℓ₂ ∧ ℓ₄ ∧ ℓ₆ ∧ ℓ₈], [ℓ₁ ∨ ℓ₃ ∨ ℓ₅ ∨ ℓ₇, ℓ₈]⟩

We have to prove that
By definition of the transitivity operator, $\ell_1 \preceq \ell_7$, $\ell_1 \preceq \ell_4 \wedge \ell_6$, and $\ell_3 \vee \ell_5 \preceq \ell_8$.

Let us consider $\epsilon'_1 = \langle \epsilon_3(g_2, \ell_o) = \langle [\ell'_1, \ell'_2], [\ell_o, \ell_o] \rangle, \epsilon'_2 = \epsilon'_3 = \langle \ell'_3, \ell'_4 \rangle, [\ell_o, \ell_o] \rangle$ We know that

1. $\ell_3 \vee \ell'_1 \preceq \ell_4 \wedge \ell'_2$,
2. $\ell_1 \preceq \ell_4 \wedge \ell'_2$, or
3. $\ell_3 \vee \ell'_1 \preceq \ell_o$ or
4. $\ell_1 \preceq \ell_o$.
5. $\ell_7 \preceq \ell'_2 \preceq \ell_8 \wedge \ell'_6$,
6. $\ell_5 \triangleleft \ell_8 \wedge \ell'_6$, or
7. $\ell_7 \preceq \ell'_5 \preceq \ell_o$ or
8. $\ell_5 \preceq \ell_o$.

We have to prove

10. $(\ell_1 \vee \ell_3 \vee \ell_5 \vee \ell_7) \vee \ell'_5 \preceq \ell_8 \wedge \ell'_6$, 
11. $\ell_1 \preceq \ell_8 \wedge \ell'_6$, or
12. $(\ell_1 \vee \ell_3 \vee \ell_5 \vee \ell_7) \vee \ell'_5 \preceq \ell_o$ or
13. $\ell_1 \preceq \ell_o$.

Notice that if $g_3 = ?$ then $\ell'_6 = \ell_o$ and therefore by (4) $\ell_1 \preceq \ell'_6$, and by (3), $\ell_3 \preceq \ell'_6$. Also $\ell'_5 = \perp$ and therefore $\ell'_5 \triangleleft \ell_7 \preceq \ell_8$. If $g_3 = \ell$, then $\ell'_5 = \ell'_6 = \ell$ and $\ell_7 = \ell_3 = \ell$, but we know that $\ell_1 \preceq \ell_8$, and therefore $\ell_1 \preceq \ell'_6$ and $\ell'_5 \preceq \ell_8$. Also as $\ell_3 \preceq \ell_8$ then $\ell_3 \preceq \ell'_6$.

We also know that $\ell_3 \vee \ell_5 \preceq \ell_8$ and by definition of intervals $\ell_7 \preceq \ell_8$. We know that $\ell_1 \preceq \ell'_6$. By (5) $\ell_7 \preceq \ell'_5 \preceq \ell'_6$. By (6) $\ell_5 \preceq \ell'_6$. Also $\ell_3 \preceq \ell'_6$ and (10) follows.

We know that $\ell_1 \preceq \ell_8$ and that $\ell_1 \preceq \ell'_6$ therefore (11) holds. By (4), (3), (7), (8) and because $\ell'_5 \preceq \ell_o$ by definition of interior, (12) holds. Finally (13) holds by (4).

\[ \square \]

**Lemma E.52.** Consider $\epsilon_1 \vdash g_1 \nleq g_2$, $\epsilon_2 \vdash g_2 \nleq g_3$, and $\epsilon_3 = \epsilon_1 \circ \prec \epsilon_2$ such that $\epsilon_3 \vdash g_1 \nleq g_3$. Then $(\neg \text{obs}_{\epsilon_1}(\epsilon_1 g_2) \lor \neg \text{obs}_{\epsilon_2}(\epsilon_2 g_3)) \iff \neg \text{obs}_{\epsilon_3}(\epsilon_3 g_3)$.

**Proof.** By Lemmas E.50 and E.51.

\[ \square \]

**Lemma E.53.** Consider $\epsilon_1$ and $\epsilon'_1 = \epsilon_2 \dashv (\epsilon_1 \circ \prec \epsilon_3)$, for some $\epsilon_2$ and $\epsilon_3$. Then $\epsilon_1 \lceil [\leq] \epsilon'_1$.

**Proof.** Suppose $\epsilon_2 = \langle [\ell_1, \ell_2], [\ell_3, \ell_4] \rangle$, $\epsilon_3 = \langle [\ell_5, \ell_6], [\ell_7, \ell_8] \rangle$, and $\epsilon_3 = \langle [\ell_9, \ell_10], [\ell_11, \ell_12] \rangle$.

$\epsilon_1 \circ \prec \epsilon_3 = (\ell_5, \ell_6) \wedge (\ell_7, \ell_8) \wedge (\ell_9, \ell_10) \wedge (\ell_11, \ell_12)$.

$\epsilon_2 \dashv (\epsilon_1 \circ \prec \epsilon_3) = \langle [\ell_1 \wedge \ell_3 \wedge \ell_2 \wedge (\ell_5 \wedge \ell_7 \wedge \ell_9 \wedge \ell_11 \wedge \ell_12)], [\ell_3 \wedge \ell_5 \wedge \ell_7 \wedge \ell_9 \wedge (\ell_11 \wedge \ell_12)] \rangle$.

But $\ell_7 \preceq \ell_3 \vee \ell_5 \vee \ell_7 \vee \ell_9 \vee \ell_11$ and therefore, $\epsilon_1 \lceil [\leq] \epsilon'_1$.

\[ \square \]

**Lemma E.54.** Consider $\epsilon_1 \vdash g_1 \nleq g_1$ and $\epsilon'_1 = \epsilon_2 \dashv (\epsilon_1 \circ \prec \epsilon_3)$ such that $\epsilon'_1 \vdash g_2 \nleq g_2$. Then $\neg \text{obs}_{\epsilon_1}(\epsilon_1 g_1) \Rightarrow \neg \text{obs}_{\epsilon_2}(\epsilon'_1 g_2)$.

**Proof.** By Lemma E.53 and Lemma E.48 the result holds immediately.

\[ \square \]

**Lemma E.55.** Consider $\epsilon_1 \vdash g_1 \nleq g_1$, $\epsilon_2 \vdash g_2 \nleq g_2$, and $\epsilon_3 = \epsilon_1 \vee \epsilon_2$ such that $\epsilon_3 \vdash g_1 \nleq g_2 \nleq g_1 \vee g_2$. Then $\epsilon_1 \lceil [\leq] \epsilon_3$.
Proof. Suppose \( \varepsilon_1 = \langle \ell_1, \ell_2 \rangle, \varepsilon_2 = \langle \ell_3, \ell_4 \rangle \), \( \varepsilon_3 = \langle \ell_5, \ell_6 \rangle \), \( \varepsilon_4 = \langle \ell_7, \ell_8 \rangle \), then \( \varepsilon_3 = \langle \ell_5 \vee \ell_6, \ell_4 \rangle \). As \( \ell_3 \preceq \ell_5 \vee \ell_6 \), therefore \( \varepsilon_1 \preceq \varepsilon_3 \) and the result holds. \[\square\]

Lemma E.56. Consider \( \varepsilon_1 \vdash g_1' \leq g_1, \varepsilon_2 \vdash g_2' \leq g_2 \), and \( \varepsilon_3 = \varepsilon_1 \wedge \varepsilon_2 \) such that \( \varepsilon_3 \vdash g_1' \wedge g_2' \leq g_1 \wedge g_2 \). Then \( \neg \text{obs}_{\varepsilon_1}(\varepsilon_3 g_1) \wedge \neg \text{obs}_{\varepsilon_2}(\varepsilon_3 g_2) \iff \neg \text{obs}_{\varepsilon_3}(\varepsilon_3 g_1 \wedge g_2) \).

Proof. First we prove the \( \Rightarrow \) direction. By Lemma E.55, \( \varepsilon_1 \leq \varepsilon_3 \). Suppose \( \text{obs}_{\varepsilon_1}(\varepsilon_1 g_1) \) does not hold (the other case is analogous). Then by Lemma E.48 the result holds immediately. Then for the \( \Leftarrow \) we use Lemma E.49 and the result holds immediately. \[\square\]

Lemma E.57. Consider \( \phi' \triangleright t^U \in \mathbb{T}[U] \), and \( \mu \), such that \( t^U \vdash \mu \) and \( \neg \text{obs}_{\varepsilon}(\phi') \), and \( \forall k > 0 \), such that \( t^U \vdash k t^U \vdash \mu' \), then \( \forall \phi \),

1. \( \forall \phi' \in \mathbb{D}(\mu') \setminus \mathbb{D}(\mu), \neg \text{obs}_{\varepsilon}(\phi \triangleright \mu') \).
2. \( \forall \phi' \in \mathbb{D}(\mu') \wedge \mathbb{D}(\mu) \wedge \mu'(o^U) \neq \mu(o^U) \),
   (a) \( \neg \text{obs}_{\varepsilon}(\phi \triangleright \mu'(o^U)) \), and
   (b) \( \neg \text{obs}_{\varepsilon}(\phi \triangleright \mu'(o^U)) \).

Proof. We use induction on the derivation of \( t^U \). The interest cases are the last step of reduction rules for references and assignments.

Case \( t = \varepsilon_1 a^U \vdash_{\varepsilon_1} \varepsilon_2 u \). We are only updating the heap so we only have to prove (a) and (b). Then

\[
\varepsilon_1 a^U \vdash_{\varepsilon_1} \varepsilon_2 u \xrightarrow{\phi'} \text{unit} \mid \mu[a^U \rightarrow \varepsilon'(u \triangleright (\phi' \triangleright g \triangleright g')) :: U']
\]

where \( \varepsilon' = (\varepsilon_2 \circ \varepsilon_1) \triangleright (\phi' \triangleright \text{irref}(\varepsilon_1)) \triangleright \text{ilbl}(\varepsilon_1) \). For simplicity let us call \( \varepsilon'_2 = (\varepsilon_2 \circ \varepsilon_1)(\text{irref}(\varepsilon_1)) \) and \( \varepsilon'_3 = \varepsilon_3 \circ \varepsilon_1(\text{ilbl}(\varepsilon_1)) \). We have to prove that (b) \( \neg \text{obs}_{\varepsilon_3}(\phi' \triangleright \text{ilbl}(U')) \). As \( \neg \text{obs}_{\varepsilon_3}(\phi' \triangleright \text{ilbl}(U')) \), by Lemma E.56, \( \neg \text{obs}_{\varepsilon_3}(\phi' \triangleright \text{ilbl}(U')) \). Then by Lemma E.54, \( \neg \text{obs}_{\varepsilon_3}(\phi' \triangleright \text{ilbl}(U')) \). Next we have to prove that (a) \( \text{obs}_{\varepsilon_3}(\phi \triangleright \mu(o^U)) \) is not defined. Consider that \( \mu(o^U) = \varepsilon u :: U' \). We know that \( \text{obs}_{\varepsilon_3}(\phi \triangleright \mu(o^U)) \) is not defined, and that \( \phi' \leq \varepsilon \), therefore by Lemma E.48, \( \text{obs}_{\varepsilon_3}(\phi(U')) \) is not defined as well and the result holds.

Case \( t = \text{ref}^U_{\varepsilon_2} \varepsilon_3 u \). We are extending the heap, so we need to only prove (1). Then

\[
\text{ref}^U_{\varepsilon_2} \varepsilon_3 u \mid \mu \xrightarrow{\phi'} \text{ref}^U_{\varepsilon_2} \varepsilon_3 u \mid \mu[o^U \rightarrow \varepsilon'(u \triangleright \phi' \triangleright g) :: U']
\]

where \( o^U \notin \mathbb{D}(\mu) \), \( \varepsilon' = \varepsilon_2 \triangleright (\phi' \triangleright g) \). We need to prove that \( \text{obs}_{\varepsilon_2}(\phi \triangleright \varepsilon'(u \triangleright \phi' \triangleright g) :: U') \) does not hold. In order to do so, we will show that \( \text{obs}_{\varepsilon_2}(\phi \triangleright \text{ilbl}(U')) \) does not holds, which follows directly by Lemma E.54.

\[\square\]

Lemma E.58. Consider \( \phi' \), such that \( \text{obs}_{\varepsilon}(\phi' \triangleright g' \triangleright g) \) does not hold, then then \( \forall k > 0 \), such that \( t^U \vdash \mu_1 \xrightarrow{\phi'} k t^U \vdash \mu'_1 \), then if \( \mu_1 \preceq_{\varepsilon} \mu_2 \), then \( \mu'_1 \preceq_{\varepsilon} \mu'_2 \).

Proof. By Lemma E.57 we know three things:

1. \( \forall o^U \in \mathbb{D}(\mu'_1) \setminus \mathbb{D}(\mu_1), \text{obs}_{\varepsilon}(\phi \triangleright \mu'_1(o^U)) \) does not hold, i.e. new locations are not observable.
(2) \( \forall o'^{U} \in \text{dom}(\mu'_1) \cap \text{dom}(\mu_1) \land \mu_1'(o'^{U}) \neq \mu(o'^{U}) \),

(a) \( \text{obs}_{\ell_o}(\phi \triangleright \mu_1(o'^{U})) \) does not hold, and

(b) \( \text{obs}_{\ell_o}(\phi \triangleright \mu'_1(o'^{U})) \) does not hold.

i.e. for all updated references they have to be previously not observable, and by definition therefore related, and second they are still non observable after the update, and by definition those locations are still related under \( \phi \).

Therefore \( \mu'_1 \approx^k_{\ell_o} \mu'_2 \) and the result holds. \( \square \)

**Lemma E.59.** Consider simple values \( u_i \in T[U_1] \) and

\( \langle \phi_1, \epsilon_1 u_1 :: U, \mu_1 \rangle \approx^k_{\ell_o} \langle \phi_2, \epsilon_2 u_2 :: U, \mu_2 \rangle : U \).

If \( \ell_1 \approx \epsilon_1 \epsilon_2 : g' \) where \( \ell_1 \sim g \leq g' \), then

\( \langle \phi_1, (\epsilon'_1 \sim \epsilon_1)(u_1 \sim g) :: U \sim g', \mu_1 \rangle \approx^k_{\ell_0} \langle \phi_2, (\epsilon'_2 \sim \epsilon_2)(u_2 \sim g) :: U \sim g', \mu_2 \rangle : U \sim g' \)

**Proof.** By induction on relation \( \langle \phi_1, \epsilon_1' u_1 :: U, \mu_1 \rangle \approx^k_{\ell_0} \langle \phi_2, \epsilon_2' u_2 :: U, \mu_2 \rangle : U \) and Lemma E.56 (observational-monotonicity of the join), considering that the label stamping can make the new values non observable and that join of evidences does not introduce imprecision. \( \square \)

**Lemma E.60.** Suppose that \( \phi_1 \leq_{\ell_o} \phi'_1, \phi'_1 \triangleright \text{prot}_{g_i_U}^{g_i'} \phi''_1(\epsilon_i t_{U_i}) \in T[U \sim g], \) for \( i \in \{1, 2\} \), where \( \neg \text{obs}_{\ell_o}(\phi_1, e_i \phi'_i, g_i) \), and either \( \neg \text{obs}_{\ell_o}(\phi_1, e_i \phi'_i, g_i) \) or \( \neg \text{obs}_{\ell_o}(\phi_1, g_i) \). Also consider two stores \( \mu_1 \) such that \( \mu_1 \approx^k_{\ell_o} \mu_2 \).

Then \( \langle \phi_1, \text{prot}_{e_i'' U}^{e_i' U} \phi''_1(\epsilon_i t_{U_i}), \mu_1 \rangle \approx^k_{\ell_o} \langle \phi_2, \text{prot}_{e_i'' U}^{e_i' U} \phi''_2(\epsilon_i t_{U_i}), \mu_2 \rangle \)

**Proof.** Suppose that after at least \( j \) more steps, where \( j < k \), both subterms reduce to a value (let us assume no cast errors are produced, otherwise the lemma vacuously holds):

\[
t_{U_i} \mid \mu_i \xrightarrow{\phi'_i} \epsilon'_i u_i \mid \mu'_i
\]

Therefore:

\[
\text{prot}_{e_i'' U}^{e_i' U} \phi''_1(\epsilon_i t_{U_i}) \mid \mu'_1 \n\xrightarrow{\phi'_1} \epsilon'_i u_i \mid \mu'_1
\]

\[
\text{prot}_{e_i'' U}^{e_i' U} \phi''_2(\epsilon_i t_{U_i}) \mid \mu'_2
\]

As the values can be radically different we have to make sure that both values are not observables. If \( \text{obs}_{\ell_o}(\phi_1, e_i \phi'_i, g_i) \) does not hold then the values are not observables because the security context is not observable. Let us assume that \( \text{obs}_{\ell_o}(\phi_1, e_i \phi'_i, g_i) \) holds, but \( \text{obs}_{\ell_o}(\phi'_i, g_i) \) not. Then by Lemma E.56, \( \text{obs}_{\ell_o}(\langle e'_i \sim \epsilon_i \rangle(\text{Label}(U) \sim g)) \) does not hold, and therefore \( \text{obs}_{\ell_o}(\phi_1 \triangleright (e'_i \sim \epsilon_i)(u_1 \sim g)) :: U \sim g \) does not hold, and by definition of related evidences \( (e'_i \sim \epsilon_i) \approx_{\ell_o} (e'_2 \sim \epsilon_2) \).

Now we have to prove that the resulting stores are related. But by Lemma E.58 the result immediately.

\( \square \)

**Lemma E.61.** Suppose that \( \phi_1 \leq_{\ell_o} \phi'_1, \phi'_1 \leq_{\ell_o} \phi''_1, \langle \phi_1, t_1, \mu_1 \rangle \approx^k_{\ell_o} \langle \phi_2, t_2, \mu_2 \rangle : C(U'), \) and that \( \phi'_1 \triangleright \text{prot}_{e_i'' U}^{e_i' U} \phi''_1(\epsilon_i t_{U_i}) \in T[U \sim g], \) for \( i \in \{1, 2\} \). If \( \ell_1 \approx \epsilon_1 \epsilon_2 : U, \phi_1 \approx^k_{\ell_o} \phi_2, \phi'_1 \approx^k_{\ell_o} \phi'_2, \phi''_1 \approx^k_{\ell_o} \phi''_2, \) and \( \epsilon'_1 \approx_{\ell_o} \epsilon'_2 : g \).

then \( \langle \phi_1, \text{prot}_{e_i'' U}^{e_i' U} \phi''_1(\epsilon_i t_{U_i}), \mu_1 \rangle \approx^k_{\ell_o} \langle \phi_2, \text{prot}_{e_i'' U}^{e_i' U} \phi''_2(\epsilon_i t_{U_i}), \mu_2 \rangle : C(U \sim g) \)
Proof. In case that combining evidence may fail, then the Lemma vacuously holds. Let us assume that combining evidence always succeeds. Consider $j < k$, we know by definition of related computations that

\[ \mu_i \xrightarrow{\phi^j} \mu'_i \]

then $\mu'_i \approx^j_{\ell_o} \mu'_2$, and by Lemma E.62 $\mu_i \rightarrow \mu'_i$. If $t^U_i$ are reducible after $k - 1$ steps, then the result holds immediately by (Rprot). The interest case if $t^U_i$ are irreducible after $j < k$ steps:

Suppose that after $j$ steps $t^U_i = v_i$, then $\left\langle \phi_1, v_1, \mu'_1 \right\rangle \approx^{k-j}_{\ell_o} \left\langle \phi_2, v_2, \mu'_2 \right\rangle : U'$.

Therefore:

\[ \left\langle \phi'_i, t^{U'}_i \right\rangle \quad \mu'_i \]

\[ \left\langle \phi''_i, t^{U'}_i \right\rangle \quad \mu'_i \]

\[ \left\langle \phi'_i, 1 \right\rangle \]

We know by Lemma E.46 that $\left\langle \phi_1, e'_i u_1 :: U, \mu'_i \right\rangle \approx^{k-j}_{\ell_o} \left\langle \phi_2, e'_2 u_2 :: U, \mu'_2 \right\rangle : U$.

If $\neg \text{obs}_\ell_o(\phi_i \triangleright v_i)$ or $\neg \text{obs}_\ell_o(e_i \triangleright \text{label}(U))$, then by Lemma E.64, $\text{obs}_\ell_o(\phi_i \triangleright e'_i u_1 :: U)$ also does not hold. Finally by Lemma E.56 $\text{obs}_\ell_o(\phi_i \triangleright (e''_i \triangleright v_i)(\text{label}(U) \triangleright g))$ does not hold and therefore the final values are related.

Let us consider that $\text{obs}_\ell(o)(\phi_i \triangleright v_i)$, $\text{obs}_\ell(o)(e_i \triangleright \text{label}(U))$, and that $\text{obs}_\ell(o)(\phi_i \triangleright e''_i u_1 :: U)$ holds (otherwise we follow by the previous argument).

Let us assume that $\neg \text{obs}_\ell(o)(e'_i g)$. Then by Lemma E.56, $\neg \text{obs}_\ell(o)(\phi_i \triangleright (e''_i \triangleright v_i)(\text{label}(U) \triangleright g))$, and therefore $\neg \text{obs}_\ell(o)(\phi_i \triangleright (e''_i \triangleright v_i)(u_i \triangleright g'_i) :: U \triangleright g)$.

If $\text{obs}_\ell(o)((e''_i \triangleright v_i)(\text{label}(U) \triangleright g))$ hold, then the result follows by Lemma E.59, and by backward preservation of the relations (Lemma E.43).

\[ \square \]

**Lemma E.62.** Consider term $\phi \triangleright t^U \in T[U]$, store $\mu$ and $j > 0$, such that $t^U \mid \mu \xrightarrow{\phi} t^{U'} \mid \mu'$. Then $\mu \rightarrow \mu'$.

**Proof.** Trivial by induction on the derivation of $t^U$. The only rules that change the store are the ones for reference and assignment, neither of which remove locations. \[ \square \]

**Lemma E.63.** If $\phi \leq_{\ell_o} \phi'$ and $\phi' \leq_{\ell_o} \phi''$, then $\phi \leq_{\ell_o} \phi''$.

**Proof.** Trivial because if $\phi$ is not observable, then $\phi'$ is not observable as well by definition of $\leq_{\ell_o}$, and therefore $\phi''$ must also be not observable. \[ \square \]

**Lemma E.64.** Consider $\phi_i \triangleright v \in T[U]$, and $e \triangleright U \leq U'$. Suppose $e v :: U' \xrightarrow{L} e' u :: U'$. If $\neg \text{obs}_\ell(o)(\phi_i \triangleright v) \lor \neg \text{obs}_\ell(o)(eU') \iff \neg \text{obs}_\ell(o)(\phi_i \triangleright e' u :: U')$.

**Proof.** Direct by Lemma E.52. \[ \square \]

Next, we present the Noninterference proposition, which naturally implies the Security Type Soundness proposition (Prop 5.5) presented in the paper.

**Proposition E.65 (Noninterference).** If $\phi'_i \triangleright i \in T[U]$, $\mu_i \in \text{STORE}$, $i \triangleright \mu_i$, $\Gamma = FV(i)$, and $\forall k \geq 0, \phi_i \leq_{\ell_o} \phi'_i, $ then $\langle \phi_1, \rho_1, \mu_1 \rangle \approx^{k}_{\ell_o} \langle \phi_2, \rho_2, \mu_2 \rangle$.

If $\langle \phi_1, \rho_1, \mu_1 \rangle \approx^{k}_{\ell_o} \langle \phi_2, \rho_2, \mu_2 \rangle$, then $\langle \phi_1, \rho_1(\overline{i}), \mu_1 \rangle \approx^{k}_{\ell_o} \langle \phi_2, \rho_2(\overline{i}), \mu_2 \rangle$.
Proof. By induction on the derivation of term $\bar{t} \in T[U]$. Let us take an arbitrary index $k \geq 0$.

Case (x). $\bar{t} = x^U$ so $\Gamma = \{x^U\}$. $\Gamma \vdash \langle \phi_1, \rho_1, \mu_1 \rangle \approx_{\ell_o}^k \langle \phi_2, \rho_2, \mu_2 \rangle$ implies by definition that $\langle \phi_1, \rho_1(x^U), \mu_1 \rangle \approx_{\ell_o}^k \langle \phi_2, \rho_2(x^U), \mu_2 \rangle : U$, and the result holds immediately.

Case (b). $\bar{t} = b_g$. By definition of substitution, $\rho_1(b_g) = \rho_2(b_g) = b_g$. By definition, $\langle \phi_1, b_g, \mu_1 \rangle \approx_{\ell_o}^k \langle \phi_2, b_g, \mu_2 \rangle : \text{Bool}_g$ as required.

Case (o). $\bar{t} = o^{U_1}_{\rho_1}$ where $U = \text{Ref}_g\ U_1$. By definition of substitution, $\rho_1(o^{U_1}_{\rho_1}) = \rho_2(o^{U_1}_{\rho_1}) = o^{U_1}_{\rho_1}$. We know that $\phi_1 \triangleright o^{U_1}_{\rho_1} \in T[\text{Ref}_g, U_1]$. By definition of related stores, $\langle \phi_1, o^{U_1}_{\rho_1}, \mu_1 \rangle \approx_{\ell_o}^k \langle \phi_2, o^{U_1}_{\rho_1}, \mu_2 \rangle : \text{Ref}_g\ U_1$ as required, and the result holds.

Case (λ). $t^U = (\lambda^U x^{U_1}. t^{U_2})_g$. Then $U = U_1 g^{\gamma} U_2$. By definition of substitution, assuming $x^{U_1} \notin \text{dom}(\rho_1)$, and Lemma E.42:

$$\phi'_1 \triangleright \rho_1(t^{U_1}) = \phi'_2 \triangleright (\lambda^U x^{U_1}. \rho_1(t^{U_2}))_g \in T[U]$$

Consider $j \leq k, \mu'_1, \mu'_2$ such that $\mu_1 \Rightarrow \mu'_1$ and $\mu'_1 \approx_{\ell_o} \mu'_2$, and assume two values $v_1$ and $v_2$ such that $\langle \phi_1, v_1, \mu'_1 \rangle \approx_{\ell_o} \langle \phi_2, v_2, \mu'_2 \rangle : U'_1$. Consider $U' = U_1 g^{\gamma} U_2$, $\epsilon_{l_1} \approx_{\ell_o} \epsilon_{l_2}$, $\epsilon_{l_1} \approx_{\ell_o} \epsilon_{l_2}$, $\epsilon_{l_1} \approx_{\ell_o} \epsilon_{l_2}$, $\epsilon_{l_1} \approx_{\ell_o} \epsilon_{l_2}$, such that $\epsilon_{l_1} \triangleright U_1 g^{\gamma} U_2 \leq U'$, that $\epsilon_{l_2} \triangleright U'_1 \leq U''$, and that $\epsilon_{l_2} \triangleright \phi'_2 g^{\epsilon} \leq g'' \leq g'''$. For simplicity, let us annotate $U'' = U'' g^{\gamma} g'''$. We need to show that:

$$\langle \phi_1, \epsilon_{l_1}(\lambda^U x^{U_1}. \rho_1(t^{U_2}))_g \circ_{U'_1}^{U_2} \epsilon_{l_2} v_1, \mu'_1 \rangle \approx_{\ell_o} \langle \phi_2, \epsilon_{l_2}(\lambda^U x^{U_1}. \rho_1(t^{U_2}))_g \circ_{U'_1}^{U_2} \epsilon_{l_2} v_2, \mu'_2 \rangle : C(U'_2)$$

Each $v_1$ is either a bare value $u_1$ or a casted value $\epsilon_{l_1} u_1 :: U'_1$. In the latter case, the application expression combines evidence, which may fail with error. If it succeeds, we call the combined evidence $\epsilon_{l_2}$. The application rule then applies: it may fail with error if the evidence $\epsilon_{l_2}$ cannot be combined with the evidence for the function parameter. Every time a failure is produced product of evidence combination, then the relation vacuously holds. We therefore consider the only interesting case, where reductions always succeed. Then:

$$\epsilon_{l_1}(\lambda^U x^{U_1}. \rho_1(t^{U_2}))_g \circ_{U'_1}^{U_2} \epsilon_{l_2} v_1, \mu'_1$$

$$\phi'_1$$

$$\text{prot}_{\epsilon_{l_1} g}^{U'_1} \phi'_1(\epsilon_{l_1}(\epsilon_{l_1} u_1 :: U'_1/x^{U_1}) \circ_{U'_1}^{U_2} \epsilon_{l_2} v_1, \mu'_1)$$

$$\phi'_1$$

$$\text{prot}_{\epsilon_{l_2} g}^{U''}_g \phi'_2(\epsilon_{l_2}(\epsilon_{l_2} u_1 :: U'_1/x^{U_1}) \circ_{U'_1}^{U_2} \epsilon_{l_2} v_1, \mu'_2)$$

where $\phi''_1 = \langle \epsilon_{l_1}, \phi'_2 g^{\epsilon} \circ_{\ell_o} g''', \phi'''_1 \rangle$, $\epsilon''_1 = (\phi_1 \circ_{\ell_o} \text{ilat}(\epsilon_{l_1})) \circ_{\ell_o} \phi^{\epsilon} \circ_{\ell_o} \text{ilat}(\epsilon_{l_1})$.

Notice that $\text{ilat}(\epsilon_{l_1}) g^{\epsilon} \approx_{\ell_o} \epsilon_{l_1} g^{\epsilon} \approx_{\ell_o} \epsilon_{l_2} g^{\epsilon''}$ also $\epsilon_{l_1} g^{\epsilon''} \approx_{\ell_o} \epsilon_{l_2} g^{\epsilon''}$. If $\text{obs}_{\epsilon_{l_1}}(\phi'_1)$ do not hold, then by Lemma E.56, $\text{obs}_{\epsilon_{l_2}}(\phi''_1)$ do not hold. Then $\phi'_1 \leq_{\ell_o} \phi'_1$, and by Lemma E.63, $\phi'_1 \leq_{\ell_o} \phi''_1$. Also by Lemmas E.52 and E.56, $\phi''_1 \approx_{\ell_o} \phi''_1$.

$\epsilon_{l_1}, \epsilon_{l_2}$ and $\epsilon_{l_1}$ are the new evidences for the label, return value and argument, respectively. We then extend the substitutions to map $x^{U_1}$ to the casted arguments:

$$\rho'_1 = \rho_1 \{x^{U_1} \mapsto \epsilon_{l_1} u_1 :: U_1\}$$

We know that $\langle \phi_1, v_1, \mu'_1 \rangle \approx_{\ell_o} \langle \phi_2, v_2, \mu'_2 \rangle$ and consider $\phi \triangleright u_1 \in T[U_{u_1}]$ then $\epsilon_{l_1} \triangleright U_{u_1} \leq U_1$ and $\epsilon_{l_1} = (\epsilon_{l_1} \circ_{\ell_o} \epsilon_{l_2}) \circ_{\ell_o} \text{idom}(\epsilon_{l_1})$. As $\epsilon_{l_2} \approx_{\ell_o} \epsilon_{l_2}$ and $\text{idom}(\epsilon_{l_1}) \approx_{\ell_o} \text{idom}(\epsilon_{l_2})$, therefore using
Lemma E.46 \( \langle \phi_1, (\varepsilon_{a_1} u_1 :: U_1), \mu'_1 \rangle \approx_{\ell_0} \langle \phi_2, (\varepsilon_{a_2} u_2 :: U_1), \mu'_2 \rangle : U_1 \)

So as \( \mu_i \rightarrow \mu'_i \) then by Lemma E.41, \( \Gamma, x:U_i \vdash \langle \phi_1, \rho'_1, \mu'_1 \rangle \approx_{\ell_0} \langle \phi_2, \rho'_2, \mu'_2 \rangle. \)

We also know that \( \phi'_i \triangleright \rho_i(t^{U_i}) \in T[U_2]. \) Then by induction hypothesis:

\[
\langle \phi_1, \rho'_1(t^{U_i}), \mu'_1 \rangle \approx_{\ell_0} \langle \phi_2, \rho'_2(t^{U_i}), \mu'_2 \rangle : C(U_2)
\]

Finally, as \( \varepsilon_{p_1} \equiv icod(\varepsilon_{l_1}) \), we know that \( icod(\varepsilon_{l_1}) \equiv \ell_0 \equiv icod(\varepsilon_{l_2}) \), also \( \varepsilon_{l_1} \equiv ilbl(\varepsilon_{l_1}) \), we know that \( ilbl(\varepsilon_{l_1}) \equiv \ell_0 \equiv ilbl(\varepsilon_{l_2}) \) then by Lemma E.61:

\[
\langle \phi_1, \text{prot}_{\ell_0}^{\phi_1, U_2^i} \phi'_1(\varepsilon_{p_1}(t^{U_i})), \mu'_1 \rangle \\
\approx_{\ell_0} \langle \phi_2, \text{prot}_{\ell_0}^{\phi_1, U_2^i} \phi'_2(\varepsilon_{p_2}(t^{U_i})), \mu'_2 \rangle : C(U'_2)
\]

and finally the result holds by backward preservation of the relations (Lemma E.43).

---

Case (!). \( t^U = !\text{Ref}_{U_1} \varepsilon_{l_1} t^U_i. \) Then \( U = U_1 \rightarrow g. \)

By definition of substitution:

\[
\rho_i(t^U) = !\text{Ref}_{U_1} \varepsilon_{l_1} \rho_i(t^U_i)
\]

We have to show that

\[
\langle \phi_1, !\text{Ref}_{U_1} \varepsilon_{l_1} \rho_i(t^U_i), \mu_1 \rangle \\
\approx_{\ell_0}^k \langle \phi_2, !\text{Ref}_{U_1} \varepsilon_{l_1} \rho_i(t^U_i), \mu_2 \rangle : C(U_1 \rightarrow g)
\]

By Lemma E.42:

\[
\phi'_i \triangleright !\text{Ref}_{U_1} \varepsilon_{l_1} \rho_i(t^U_i) \in T[U_1 \rightarrow g]
\]

By induction hypotheses on the subterm:

\[
\langle \phi_1, \rho_i(t^U_i), \mu_1 \rangle \approx_{\ell_0}^k \langle \phi_2, \rho_i(t^U_i), \mu_2 \rangle : C(U'_1)
\]

Consider \( j < k \), then by definition of related computations

\[
\rho_i(t^U_i) \mid \mu_i \xrightarrow{\phi'_i} j^U_i \mid \mu'_i \implies \mu'_i \approx_{\ell_0}^{k-j} \mu'_2 \wedge (\text{irred}(t^U_i) \implies \langle \phi_1, t^U_i, \mu'_1 \rangle \approx_{\ell_0}^{k-j} \langle \phi_2, t^U_i, \mu'_2 \rangle : U'_1)
\]

Where \( U'_1 = \text{Ref}_{U_1} \ v^U_i. \) If terms \( t^U_i \) are reducible after \( j = k - 1 \) steps, then

\[
!\text{Ref}_{U_1} \varepsilon_{l_1} \rho_i(t^U_i) \mid \mu_i \xrightarrow{\phi'_i} j^U_i \mid \mu'_i \implies \text{error}
\]

If after at most \( j \) steps \( t^U_i \) is irreducible it means that for some \( j' \leq j \), \( !\text{Ref}_{U_1} \varepsilon_{l_1} \rho_i(t^U_i) \mid \mu_i \xrightarrow{\phi'_i} \phi'_i \mid \mu'_i \). If \( j' = j \) then we use the same same argument for reducible terms and the result holds.

Let us consider now \( j' < j. \) Then \( \langle \phi_1, v_1, \mu'_1 \rangle \approx_{\ell_0}^{k-j} \langle \phi_2, v_2, \mu'_2 \rangle : U'_1. \) By Lemma E.10, each \( v_i \) is either a location \( o_{U'_1/\varepsilon_{l_1}^i} \) or a casted location \( \varepsilon_{l_1}(o_{U'_1/\varepsilon_{l_1}^i}) :: U'_1. \) Let us assume they both are a casted location (the other cases are analogous). In case a value \( v_{1j} \) is a casted value, then the whole term \( \rho_i(t^U_i) \) can take a step by \( (Rg) \), combining \( g \) with \( \varepsilon_i \). Such a step either fails, or succeeds with a new combined evidence. Therefore, either:

\[
\rho_i(t^U_i) \mid \mu_i \xrightarrow{\phi'_i} \text{error}
\]

in which case we do not care since we only consider termination-insensitive noninterference; or:

\[
\rho_i(t^U_i) \mid \mu_i \xrightarrow{\phi'_i} J^U_i \mid \mu'_i \xrightarrow{\phi'_i} !\text{Ref}_{U_1} \varepsilon_{l_1} \rho_i(t^U_i) \mid \mu'_i \xrightarrow{\phi'_i} \text{prot}_{\ell_0}^{\phi_1, U_1} \phi'_i(\text{iref}(\varepsilon_i) v_{1j}) \mid \mu'_i
\]
with \( v'_1 = \mu'_1(U_i^\mu)^r = \epsilon_1 u'_1 :: U_i''', \phi''_1 = \langle (\phi'_1 \varepsilon \sim \text{ilbl}(\epsilon'_1)) (\phi'_1 \text{g} \sim \text{gbl}(\epsilon'_1)) \rangle \). Notice that as
\[
\langle \phi'_1, v_1, \mu'_1 \rangle \approx_{\epsilon'_1} \langle \phi'_2, v_2, \mu'_2 \rangle : U_i' \quad \text{and as } \epsilon \approx_{\epsilon_o} \epsilon, \text{ by then Lemma E.46,}
\]
\[
\langle \phi'_1, \epsilon'_1 a'_i U_i''', \mu'_1 \rangle \approx_{\epsilon'_1} \langle \phi'_2, \epsilon'_2 a'_i U_i'''', \mu'_2 \rangle : \text{Ref}_g U_i, \text{ therefore } \epsilon'_1 \approx_{\epsilon_o} \epsilon'_2, \text{ i.e. } \text{ilbl}(\epsilon'_1) \approx_{\epsilon_o} \text{ilbl}(\epsilon'_2) \text{ and } \text{iref}(\epsilon'_1) \approx_{\epsilon_o} \text{iref}(\epsilon'_2).
\]

By Lemma E.56, if \( \sim \text{obs}_{\epsilon_o}(\phi'_1) \) then \( \sim \text{obs}_{\epsilon_o}(\phi''_1) \). Then by Lemma E.63, \( \phi_1 \leq_{\epsilon_o} \phi''_1 \). Also by Lemma E.56, either \( \text{obs}_{\epsilon_o}(\phi''_1) \) or \( \sim \text{obs}_{\epsilon_o}(\phi''_1) \), therefore \( \phi''_1 \approx_{\epsilon_o} \phi''_1 \).

If both locations are related but not observable because \( \sim \text{obs}_{\epsilon_o}(\phi'_1) \), then the resulting values also are not related and the result hold immediately. If both locations are related but not observable because \( \sim \text{obs}_{\epsilon_o}(\text{ilbl}(\phi'_1)) \), then by Lemma E.56 \( \sim \text{obs}_{\epsilon_o}(\phi''_1) \), and the result holds by Lemma E.60.

If both locations are observables, then as \( \langle \phi'_1, v'_1, \mu'_1 \rangle \approx_{\epsilon'_1} \langle \phi'_2, v'_2, \mu'_2 \rangle : U_i' \), by Lemma E.61,
\[
\langle \phi_1, \text{prot}_{\epsilon'_1} U_i^{\mu'_1}, \phi''_1 \rangle \approx \langle \phi_2, \text{prot}_{\epsilon'_2} U_i^{\mu'_2}, \phi''_2 \rangle : C(U_i^2)
\]
and finally the result holds by backward preservation of the relations (Lemma E.43).

---

Case \( (\implies) \). \( t^U = \epsilon_1 t_{U_i}^{U_i^1} \epsilon_2 t_{U_i}^{U_i^2} \). Then \( U = \text{Unit}_{\perp} \).

By definition of substitution:
\[
\rho_i(t^U) = \epsilon_1 \rho_1(t_{U_i}^{U_i^1}) \epsilon_2 \rho_2(t_{U_i}^{U_i^2})
\]
and Lemma E.42:
\[
\phi'_1 \approx \epsilon_1 \rho_1(t_{U_i}^{U_i^1}) \epsilon_2 \rho_2(t_{U_i}^{U_i^2}) \in T[\text{Unit}_{\perp}]
\]

We have to show that
\[
\langle \phi_1, \epsilon_1 \rho_1(t_{U_i}^{U_i^1}) \epsilon_2 \rho_2(t_{U_i}^{U_i^2}), \mu_1 \rangle \\ \approx_{\epsilon_o} \langle \phi_2, \epsilon_2 \rho_2(t_{U_i}^{U_i^2}), \mu_2 \rangle : C(U)
\]

By induction hypotheses
\[
\langle \phi_1, \rho_1(t_{U_i}^{U_i^1}), \mu_1 \rangle \approx_{\epsilon_o} \langle \phi_2, \rho_2(t_{U_i}^{U_i^1}), \mu_2 \rangle : C(U_i)
\]

Suppose \( j_1 < k \), and that \( \rho_1(t_{U_i}^{U_i^1}) \) irreducible after \( j_1 \) steps (otherwise, similar to case !, the result holds immediately). Then by definition of related computations:
\[
\rho_1(t_{U_i}^{U_i^1}) | \mu_1 \xrightarrow{\phi'_1} h v_1 | \mu'_1 \implies \mu'_1 \approx_{\epsilon_o} (\phi_1, v_1, \mu'_1) \approx_{\epsilon_o} (\phi_2, v_2, \mu'_2) : U_i
\]

By Lemma E.62 \( \mu_1 \not\approx \mu'_1 \), and \( \mu'_1 \approx_{\epsilon_o} (\phi_2, v_2, \mu'_2) \) then by Lemma E.41, \( \langle \phi_1, \rho_1(t_{U_i}^{U_i^1}), \mu'_1 \rangle \approx_{\epsilon_o} \langle \phi_2, \rho_2(t_{U_i}^{U_i^1}), \mu'_2 \rangle : C(U_i) \).

By induction hypotheses
\[
\langle \phi_1, \rho_1(t_{U_i}^{U_i^1}), \mu'_1 \rangle \approx_{\epsilon_o} \langle \phi_2, \rho_2(t_{U_i}^{U_i^1}), \mu'_2 \rangle : C(U_i)
\]

Again, consider \( j_2 = k - j_1 \), if after \( j_2 \) steps \( \rho_1(t_{U_i}^{U_i^2}) \) is reducible or is a value, the result holds immediately. The interest case if after \( j_2 \) steps \( \rho_1(t_{U_i}^{U_i^2}) \) reduces to values \( v'_1 \):
\[
\rho_1(t_{U_i}^{U_i^2}) | \mu'_1 \xrightarrow{\phi'_1} h v'_1 | \mu''_1 \implies \mu''_1 \approx_{\epsilon_o} (\phi_1, v'_1, \mu''_1) \approx_{\epsilon_o} (\phi_2, v'_2, \mu''_2) : U_2
\]

Then
\[
\rho_1(t_{U_i}^{U_i^2}) | \mu_1 \xrightarrow{\phi'_1} h v_1 | \mu''_1 \implies \mu''_1 \approx_{\epsilon_o} (\phi_1, v_1, \mu''_1) \approx_{\epsilon_o} (\phi_2, v_2, \mu''_2) : U_2
\]

Now \( v_1 \) and \( v'_1 \) can be bare values or casted values. In the case of casted values we can combine evidence, which may fail with \textbf{error}. We assume that all evidence combinations succeed, otherwise
the relation vacuously holds. As both values \( v_i \) are related at some reference type, then by canonical forms (Lemma E.10) they both must be locations \( o_{\ell_1}^{U_1} \) for some \( U_1 \leq U_i \).

\[
\begin{align*}
\epsilon_1 v_i &:= \epsilon_2 v_i', \quad \mu'' \\
\phi_1' &\rightarrow 2, \quad \epsilon_1 o_{\ell_1}^{U_1} \\
\phi_1' &\rightarrow 1 \quad \text{unit} \cdot \mu''
\end{align*}
\]

Where \( \mu'' = \mu'' [o_{\ell_1}^{U_1} \mapsto \epsilon_1'(u_i \triangleright (\phi'_{11} g \triangleright \ell)) = U_1' \). Notice that \( \epsilon_1 \approx \ell_1 \epsilon_1 \) and \( \epsilon_2 \approx \epsilon_2 \). As \( \langle \phi_1, \epsilon_1', \mu'_1 \rangle \approx_{\ell_1}^{k_1-j_1} \langle \phi_2, \epsilon_2, \mu''_2 \rangle : U_2 \) then by Lemma E.46,

\[
\langle \phi_1, \epsilon_{11} o_{\ell_1}^{U_1} \rangle \approx_{\ell_1}^{k_1-j_1} \langle \phi_2, \epsilon_{22} U_2' \rangle : U_1'.
\]

Similarly as \( \langle \phi_1, \epsilon_1', \mu'_1 \rangle \approx_{\ell_1}^{k_1-j_1} \langle \phi_2, \epsilon_2, \mu''_2 \rangle : U_1 \), then by Lemma E.46

\[
\langle \phi_1, \epsilon_{11} o_{\ell_1}^{U_1} \rangle \approx_{\ell_1}^{k_1-j_1} \langle \phi_2, \epsilon_{22} U_2' \rangle : U_1'.
\]

We consider first when the values are observable and the locations are identical: As \( \text{iref}(\epsilon_{11}) \approx_{\ell_1} \text{iref}(\epsilon_{12}) \) then either \( \text{obs}_{\ell_1}(\text{iref}(\epsilon_{11})) \) or \( \neg \text{obs}_{\ell_1}(\text{iref}(\epsilon_{12})) \). Also as \( \phi_1' \approx_{\ell_1} \phi_2' \), then either \( \text{obs}_{\ell_1}(\phi_1') \) or \( \neg \text{obs}_{\ell_1}(\phi_1') \).

Notice that \( \epsilon_{11}' = (\epsilon_{11} \circ <: \text{iref}(\epsilon_{11})) \circ \epsilon_t' \), where \( \epsilon_t' = ((\phi_1' g \triangleright \ell) \circ <: \phi_1' g \triangleright \ell) \).

\[
\text{Lemma E.46, } \langle \phi_1, (\epsilon_{12} \circ <: \text{iref}(\epsilon_{11}))(u_{12}', \mu'_{12}) \approx_{\ell_0}^{k_1-j_1} \langle \phi_2, (\epsilon_{22} \circ <: \text{iref}(\epsilon_{11}))(u_{12}', \mu'_{12}) : U_1'.
\]

- Suppose \( \text{obs}_{\ell_0}(\phi_1' g \triangleright \ell) \land \text{obs}_{\ell_0}(\epsilon_{11}' g) \land \epsilon_{11}' = \phi_1' g \triangleright \ell \), then by Lemma E.56, \( \text{obs}_{\ell_0}(\epsilon_{11}' g) \).
  - If \( \text{obs}_{\ell_0}(\epsilon_{11}' g) \), then by Lemma E.52, \( \text{obs}_{\ell_0}(\epsilon_{11}' g) \).
  - If \( \neg \text{obs}_{\ell_0}(\epsilon_{11}' g) \), then by Lemma E.52, \( \neg \text{obs}_{\ell_0}(\epsilon_{11}' g) \).

Therefore \( \epsilon_{11}' \approx_{\ell_0} \epsilon_{12}' \), then by Lemma E.59,

\[
\langle \phi_1, \epsilon_{11}' (u_{12}' \triangleright (\phi'_{11} g \triangleright \ell)) \rangle = U_1', \mu''
\]

Also if \( \neg \text{obs}_{\ell_0}(\phi_1) \Rightarrow \neg \text{obs}_{\ell_0}(\phi_1) \) and therefore by monotonicity of the join \( \neg \text{obs}_{\ell_0}(\epsilon_{11}' g) \). Therefore if the values where different but context not observables, now the new values are going to be not observable as well, independently of the context. Then \( \forall, \phi_2, \epsilon_{12}' \), we only have to prove that \( \mu'' \approx_{\ell_0}^{k_1-j_1-j_2-3} \mu'' \), but using monotonicity (Lemma E.47), it is trivial to prove that because either both both stores update the same location \( o_{\ell_1}^{U_1} \) to values that are related, therefore the result holds.

We consider now when the values are not observable and the locations may be different:

Suppose that \( \mu'' (o_{\ell_1}^{U_1}) = \epsilon_{01} u_{11}' = U_1' \) such that \( \langle \phi_1, \epsilon_{01} u_{11}' = U_1', \mu'' \rangle \approx_{\ell_0}^{k_1-j_1-j_2-3} \langle \phi_2, \epsilon_{02} U_2' = U_1', \mu'' \rangle : U_1' \), then we know that \( \phi_1' g \triangleright \ell \circ \text{ibl}(\phi_{11}) \) \( \leq \) \( \text{ibl}(\epsilon_{01}) \).

As \( \neg \text{obs}_{\ell_0}(\phi_1' v_i) \), by Lemma E.64, \( \neg \text{obs}_{\ell_0}(\phi_1' v_i) \).
We have to show that

\[ e_1^{U_i'} \vdash U_i' \, : \, \text{Ref}_r U_i' \]. Then by definition of \( \text{obs}_{r_i} \), either \( \neg \text{obs}_{r_i}(\phi_i' e_i' g_i) \) or \( \neg \text{obs}_{r_i}(\text{ilbl}(e_i')) \) therefore, by Lemma E.56, \( \neg \text{obs}_{r_i}(\langle \phi_i' e_i' g_i \rangle) \), then by Lemma E.48, \( \neg \text{obs}_{r_i}(\text{ilbl}(r_i U_i')) \), and finally by definition of related values \( \neg \text{obs}_{r_i}(\phi_i' e_{i1} u_{i1}' : U_i') \). Analogously, suppose that \( \mu_i''(o_i^{U_i'}) = e_{i11} u_{i2}'' : U_i'' \), then \( \neg \text{obs}_{r_i}(\phi_i' e_{i12} u_{i2}'' : U_i'') \).

Notice that \( e_i' = (e_i' \vdash r_i \text{ilbl}(e_i'))) \), which \( e_i' = ((\phi_i' e_i' \text{ilbl}(e_i'))) \). As \( \neg \text{obs}_{r_i}(\phi_i' e_i' g_i) \) and finally by definition of related values \( \neg \text{obs}_{r_i}(\phi_i' e_{i1} u_{i1}' : U_i') \). Analogously, such a step either fails, or succeeds with a new combined evidence. Therefore, by Lemma E.52. We know that if \( e_i' \vdash U_i' \), by definition of related computations

\[ \langle \phi_1, \mu_1'(U_1), \mu_1'' \rangle \approx_{\theta_o} \langle \phi_2, \mu_2'(U_2), \mu_2'' \rangle : U_1' \]

Consider \( j < k \), by definition of related computations

\[ \rho_i(t_i U_i') \vdash U_i' \]

By induction hypotheses:

\[ \langle \phi_1, \rho_1(t_i U_i'), \mu \rangle \approx_{\theta_o} \langle \phi_2, \rho_2(t_i U_i'), \mu \rangle : C(U_i') \]

If terms \( t_i U_i' \) are reducible after \( j = k - 1 \) steps, then

\[ \rho_i(t_i U_i') \vdash U_i' \]

If after \( j = k \) steps \( t_i U_i' \) is irreducible, it means that for some \( j' < j \) \( \rho_i(t_i U_i') \vdash U_i' \). In case a value \( v_i j \) is a casted value, then the whole term \( \rho_i(t_i U_i') \) can take a step by \( (Rg) \), combining \( e_i \) with \( e_i \). Such a step either fails, or succeeds with a new combined evidence. Therefore, either:

\[ \rho_i(t_i U_i') \vdash U_i' \]

in which case we do not care since we only consider termination-insensitive noninterference, or:

\[ \rho_i(t_i U_i') \vdash U_i' \]

with, \( \mu_i'' = \mu_i''[o_i U_i' \vdash e_i'(u_i \triangleright e_i' g_i) : U_i] \). Where \( \phi_i' = e_i'(u_i \triangleright e_i' g_i) : U_i \). Notice that \( \phi_i' e_i \approx_{\theta_o} \phi_i' e \), and \( e_i' \approx_{\theta_o} e_i' \theta_{e_i} \theta_{e_i} \) therefore by Lemma E.52. We know that if \( u_i \in T[u_i] \), then \( e_i + U_i \leq U_i \). Also, as
\[ \langle \phi_1, v_1, \mu'_1 \rangle \approx_{t_o}^{k-j'} \langle \phi_2, v_2, \mu'_2 \rangle : U'_1 \text{ then by Lemma E.46,} \\
\langle \phi_1, e_u u_1 :: U_1, \mu'_1 \rangle \approx_{t_o}^{k-j'} \langle \phi_2, e'_2 u_2 :: U_1, \mu'_2 \rangle : U'_1 \text{ and as } (\phi', e' \circ e) \vdash \phi, g.c \approx \text{ label}(U_1), \text{ then by Lemma E.59, Lemma E.54, and Lemma E.47,} \\
\langle \phi_1, e'_u(u_1 \triangleright \phi'_1 g.c.) :: U_1, \mu'_1 \rangle \approx_{t_o}^{k-j''-2} \langle \phi_2, e''_2(u_2 \triangleright \phi'_2 g.c.) :: U_1, \mu'_2 \rangle : U'_1. \]

Also if \( \neg \text{obs}_{t_o}(\phi_1) \Rightarrow \neg \text{obs}_{t_o}(\phi'_1) \) and therefore by monotonicity of the join \( \neg \text{obs}_{t_o}(\phi''_1) \text{ label}(U_1) \). Therefore if the values where different but context not observables, now the new values are going to be not observable as well, independently of the context. Then

\[\forall, \phi''_1 \approx_{t_o}^{k} \phi''_2, \langle \phi''_1, e'_u(u_1 \triangleright \phi''_1 g.c.) :: U_1, \mu''_1 \rangle \approx_{t_o}^{k-j''-2} \langle \phi''_2, e''_2(u_2 \triangleright \phi''_2 g.c.) :: U_1, \mu''_2 \rangle : U'_1.\]

By definition of related stores \( \mu''_1 \approx_{t_o}^{k-j''-2} \mu''_2 \) then by Monotonicity of the relation (Lemma E.47) \( \mu''_1 \approx_{t_o}^{k-j''-2} \mu''_2 \) and the result holds.

\[
\text{Case } (\odot). \quad t^U = e_1 t^U_1 \oplus^g e_2 t^U_2
\]

By definition of substitution:

\[\rho_i(t^U) = e_1 \rho_i(t^U_1) \oplus^g e_2 \rho_i(t^U_2)\]

and Lemma E.42:

\[\phi'_i \ast e_i \rho_i(t^U) \oplus^g e_2 \rho_i(t^U_2) \in T[U]\]

We use a similar argument to case := for reducible terms. The interest case is when we suppose some \( j_1 \) and \( j_2 \) such that \( j_1 + j_2 < k - 3 \) where:

\[\rho_i(t^U_1) \mid \mu_i \xrightarrow{\phi'_i} j_i v_{11} \mid \mu'_i \implies \mu'_i \approx_{t_o}^{k-j_i} \mu'_2 \wedge \langle \phi_1, v_{11}, \mu'_1 \rangle \approx_{t_o}^{k-j_i} \langle \phi_2, v_{21}, \mu'_2 \rangle : U_1\]

\[\rho_i(t^U_2) \mid \mu'_i \xrightarrow{\phi'_i} j_2 v_{12} \mid \mu''_i \implies \mu''_i \approx_{t_o}^{k-j_i-j_2} \mu''_2 \wedge \langle \phi_1, v_{12}, \mu''_1 \rangle \approx_{t_o}^{k-j_i-j_2} \langle \phi_2, v_{22}, \mu''_2 \rangle : U_2\]

By Lemma E.10, each \( v_{ij} \) is either a boolean \( b_{ij}, g_{ij} \) or a casted boolean \( e_i(b_{ij}) g_{ij} :: U_j \). In case a value \( v_{ij} \) is a casted value, then the whole term \( \rho_i(t^U) \) can take a step by (Rg), combining \( \epsilon_i \) with \( e_{ij} \). Such a step either fails, or succeeds with a new combined evidence. Therefore, either:

\[\rho_i(t^U) \mid \mu_i \xrightarrow{\phi'_i} j_i+j_2 \text{error}\]

in which case we do not care since we only consider termination-insensitive noninterference, or:

\[\xrightarrow{\epsilon_i(b_{ij}) g_{ij} :: \text{Bool}_g} \rho_i(t^U) \mid \mu''_i \]

\[\xrightarrow{\epsilon_i'(b_{ij}) g_{ij}' :: \text{Bool}_g} \mu''_i \]

with \( b_i = b_{11} \otimes b_{12} \), \( \epsilon_i' = \epsilon_i' \wedge \epsilon_i' \), and \( g'_i = g_{ij} \wedge g_{ij}' \). It remains to show that:

\[\langle \phi_1, e_i'(b_{ij}) g'_i :: \text{Bool}_g, \mu''_i \rangle \approx_{t_o}^{k-j_i-j_i-3} \langle \phi_2, e_i'(b_{ij}) g'_i :: \text{Bool}_g, \mu''_i \rangle : \text{Bool}_g\]

If \( \neg \text{obs}_{t_o}(\phi_1) \), then the result is trivial because the resulting booleans are also related as they are not observable.

If \( \text{obs}_{t_o}(\phi_1) \), then by Lemma E.46, \( \langle \phi_1, e_{11}(b_{11}) g_{11} :: \text{ Bool}_g, \mu''_i \rangle \approx_{t_o}^{k} \langle \phi_2, e_{12}(b_{21}) g_{12} :: \text{ Bool}_g, \mu''_i \rangle \). If \( \neg \text{obs}_{t_o}(\text{label}(\epsilon_{11}')) \) or \( \neg \text{obs}_{t_o}(\text{label}(\epsilon_{12}')) \), then by Lemma E.56, \( \neg \text{obs}_{t_o}(\epsilon_{11}' g) \) and the result holds. If both \( \text{obs}_{t_o}(\text{label}(\epsilon_{11}')) \) then \( b_{11} = b_{21} \) and \( b_{12} = b_{22} \), so \( b_1 = b_2 \), and the result holds.
We omit the $\varepsilon_1$ with $\varepsilon_2 \vdash U_2 \leq U_{11}$, and $U = U_{12} \sim \gamma g$.

We use a similar argument to case $\vdash$ for reducible terms. The interest case is when we suppose some $j_1$ and $j_2$ such that $j_1 + j_2 < k$ where by induction hypotheses and the definition of related computations:

$$\rho_1(t^U) | \mu_i \xrightarrow{\phi_i'} j_1 \nu_1 \mid \mu_i' \quad \Rightarrow \quad \mu_i' \approx_{\ell_o}^k \mu_2' \land \langle \phi_1, \nu_{11}, \mu_1' \rangle \approx_{\ell_o}^k \langle \phi_2, \nu_{21}, \mu_2' \rangle : U_1$$

$$\rho_1(t^U) | \mu_i' \xrightarrow{\phi_i'} j_2 \nu_2 \mid \mu_i'' \quad \Rightarrow \quad \mu_i'' \approx_{\ell_o}^{k-j_2} \mu_2'' \land \langle \phi_1, \nu_{12}, \mu_1'' \rangle \approx_{\ell_o}^{k-j_2} \langle \phi_2, \nu_{22}, \mu_2'' \rangle : U_2$$

Then

$$\rho_1(t^U) | \mu_i \xrightarrow{\phi_i'} j_1+j_2 \varepsilon_1 \nu_{11} \varepsilon_2 \nu_{12} \mid \mu_i''$$

If $\text{obs}_{\ell_o}(\phi_i \vdash \nu_{11})$ then, by definition of $\approx_{\ell_o}$ at values of function type, using $\varepsilon_1$ and $\varepsilon_2$ to justify the subtyping relations, we have:

$$\langle \phi_1, \varepsilon_1 \nu_{11} \varepsilon_2 \nu_{12}, \mu_i'' \rangle \approx_{\ell_o}^{k-j_2} \langle \phi_2, \varepsilon_1 \nu_{21} \varepsilon_2 \nu_{22}, \mu_i'' \rangle : C(U_{12} \sim \gamma g)$$

Finally, by backward preservation of the relations (Lemma E.43) the result holds.

As $\neg \text{obs}_{\ell_o}(\phi_i \vdash \nu_{11})$, and we assume by canonical forms that $\nu_{11} = \varepsilon_1(\lambda^{g'_{11}} t_{11})_{g_{11}} :: U_1$ and that $\nu_{12} = \varepsilon_{12} \nu_{12} :: U_2$ (and that evidence combination always succeed or the result holds immediately), then,

$$\frac{\langle \phi_i', \varepsilon_1 \nu_{11} \varepsilon_2 \nu_{12}, \mu_i'' \rangle \approx_{\ell_o} \langle \phi_i', \nu_{11} \circ \nu_{12}, \mu_i'' \rangle}{\phi_i' \vdash 1 \nu_{11} \circ \nu_{12} \mid \mu_i''}$$

$$\frac{\langle \phi_i', \nu_{11} \circ \nu_{12}, \mu_i'' \rangle \approx_{\ell_o} \langle \phi_i', \nu_1 \circ \nu_{12} \circ \nu_2 \mid \mu_i'' \rangle}{\text{prot}_{\varepsilon_1(\nu_{11} \circ \nu_{12}), \nu_1 \circ \nu_{12}, \mu_i''}}$$

Where $\varepsilon_1' = \varepsilon_1 \circ \varepsilon_1, \varepsilon_2' = \varepsilon_2 \circ \varepsilon_2$, and $\phi_i'' = \langle \phi_i', \nu_1 \circ \nu_{12} \circ \nu_2, \mu_i'' \rangle$. Also by Lemma E.52, $\neg \text{obs}_{\ell_o}(\lambda^{g'_{11}} t_{11})_{g_{11}} :: U_1)$.

Finally by Lemma E.60,

$$\langle \phi_1, \text{prot}_{\varepsilon_1(\nu_{11} \circ \nu_{12}), \nu_1 \circ \nu_{12}, \mu_i''}(\text{icod}(\varepsilon_1' \nu_1)), \mu_i'' \rangle \approx_{\ell_o}^{k-j_2} \langle \phi_2, \text{prot}_{\varepsilon_2(\nu_2 \circ \nu_{12}), \nu_2 \circ \nu_{12}, \mu_i''}(\text{icod}(\varepsilon_2' \nu_2)), \mu_i'' \rangle : C(U_{12} \sim \gamma g)$$

Finally, by backward preservation of the relations (Lemma E.43) the result holds.
Case (if). \( t^U = \text{if}^\nu \, \varepsilon_1 t_{\varepsilon_1} \) then \( \varepsilon_2 t_{\varepsilon_2} \) else \( \varepsilon_3 t_{\varepsilon_3} \), with \( \phi'' \triangleright t_{\varepsilon_2} \in T[U_1] \), \( \nu = \text{label}(U_1) \), \( \varepsilon_1' = (\phi_1, \tilde{\nu} \text{ilbl}(\varepsilon_1)) \), \( \phi''' = (\phi'_1, g_c, \tilde{\nu} g) \), \( \phi'' \triangleright t_{\varepsilon_3} \in T[U_2] \), \( \phi'' \triangleright t_{\varepsilon_3} \in T[U_3] \), \( \varepsilon_1 \cup U_1 \preceq \text{Bool}_g \), and \( U = (U_2 \tilde{\nu} U_3) \triangleright g \)

By definition of substitution:

\[
\rho_1(t^U) = \text{if}^\nu \, \varepsilon_1 \rho_1(t_{\varepsilon_1}) \text{ then } \varepsilon_2 \rho_1(t_{\varepsilon_2}) \text{ else } \varepsilon_3 \rho_1(t_{\varepsilon_3})
\]

We use a similar argument to case \( \triangleright \) for reducible terms. The interest case is when we suppose some \( j_1 \) and \( j_2 \) such that \( j_1 + j_2 < k \) where by induction hypotheses and related computations we have that:

\[
\rho_1(t_{\varepsilon_i}) \mid \mu_i \xrightarrow{\phi'_i} \langle \varphi \triangleright v_{11} \mid \mu_i \rangle \implies \mu'_i \approx^{k-j_i} \mu'_2 \land \langle \phi \triangleright v_{13}, \mu'_1 \rangle \approx^{k-j_i} \langle \phi \triangleright v_{21}, \mu'_2 \rangle : U_1
\]

By Lemma E.10, each \( v_{11} \) is either a boolean \((b_{11})_{\varepsilon_1} \) or a casted boolean \((b_{11})_{\varepsilon_1} \triangleright U_1 \). In either case, \( U_1 \preceq \text{Bool}_g \) implies \( U_1 \preceq \text{Bool}_g \). In case a value \( v_{11} \) is a casted value, then the whole term \( \rho_1(t^U) \) can take a step by \((Rg)\), combining \( \varepsilon_1 \) with \( \varepsilon_1' \). Such a step either fails, or succeeds with a new combined evidence. Therefore, either:

\[
\rho_1(t^U) \mid \mu_i \xrightarrow{\phi'_i} \langle j_{i+1} \text{error} \rangle
\]

in which case we do not care since we only consider termination-insensitive noninterference, or:

\[
\rho_1(t^U) \mid \mu_i \xleftarrow{\phi'_i} \langle j_{i+1} \rangle \text{if}^\nu \, \varepsilon_1' (b_{11})_{\varepsilon_1'} \text{ then } \varepsilon_2 \rho_1(t_{\varepsilon_2}) \text{ else } \varepsilon_3 \rho_1(t_{\varepsilon_3}) \mid \mu_i'
\]

If \( \neg \text{obs}_{\varepsilon_0}(\phi \triangleright v_{11}) \), then by Lemma E.64 \( \neg \text{obs}_{\varepsilon_0}(\phi \triangleright e_{11} b_{11} \triangleright \text{Bool}_g) \). Without loosening generality, let us assume the worst case scenario and that both execution reduce via different branches of the conditional.

Consider \( \phi''' = ((\phi'_1, \tilde{\nu} \text{ilbl}(\varepsilon_1'))((\phi'_1 g_c, \tilde{\nu} g_{11}'), (\phi'_1 g_c, \tilde{\nu} g)) \). It is easy to see that if \( \phi_1 \) is not observable, then as \( \phi_1 \leq_{\varepsilon_0} \phi_1' \) \( \neg \text{obs}_{\varepsilon_0}(\phi'_{11}) \), and therefore by Lemma E.56, \( \neg \text{obs}_{\varepsilon_0}(\phi''_{11} \phi''_{11} g_c) \). Therefore \( \phi_1 \leq_{\varepsilon_0} \phi''_{11} \).

If \( \neg \text{obs}_{\varepsilon_0}(\phi \triangleright e_{11} \text{Bool}_g) \), then also by Lemma E.56, \( \neg \text{obs}_{\varepsilon_0}(\phi''_{11} \phi''_{11} g_c) \).

Then:

\[
\rho_1(t^U) \mid \mu_i \xrightarrow{\phi'_i} \langle j_{i+1} \rangle \preceq^{k-j_i} \rho_1''(e_{2} \rho_1(t_{\varepsilon_2})) \mid \mu_i'
\]

\[
\rho_2(t^U) \mid \mu_2 \xrightarrow{\phi'_i} \langle j_{i+2} \rangle \preceq^{k-j_i} \rho_2''(e_{3} \rho_2(t_{\varepsilon_3})) \mid \mu'_2
\]

But because \( \neg \text{obs}_{\varepsilon_0}(\phi \triangleright e_{11} \text{Bool}_g) \) then either \( \neg \text{obs}_{\varepsilon_0}(\phi, \phi, g_c) \) or \( \neg \text{obs}_{\varepsilon_0}(\text{ilbl}(e_{11} g)) \). Then as \( \phi_1 \leq_{\varepsilon_0} \phi''_{11} \) by Lemma E.60,

\[
\langle \phi_1, \text{prot}^U_{\text{ilbl}(e_{11})} \phi''_{11} (e_2 \rho_1(t_{\varepsilon_2})), \mu'_i \rangle \approx^{k} \langle \phi_2, \text{prot}^U_{\text{ilbl}(e_{21})} \phi''_{22} (e_3 \rho_2(t_{\varepsilon_3})), \mu'_2 \rangle : C(U)
\]

and the result holds by backward preservation of the relations (Lemma E.43).

Now consider if \( \text{obs}_{\varepsilon_0}(\phi \triangleright v_{11}) \), then \( \text{obs}_{\varepsilon_0}(\phi \triangleright e_{11} b_{11} \triangleright \text{Bool}_g) \) may hold or not. If its not observable we proceed like we just did for the non-observable case. Let us consider that \( \text{obs}_{\varepsilon_0}(\phi \triangleright e_{11} b_{11} \triangleright \text{Bool}_g) \) holds.

Then by definition of \( \preceq_{\varepsilon_0} \) on boolean values, \( b_{11} = b_{21} \) Because \( b_{11} = b_{21} \), both \( \rho_1(t^U) \) and \( \rho_2(t^U) \) step into the same branch of the conditional. Let us assume the condition is true (the other case is similar):

Then by induction hypotheses \( \langle \phi_1, \rho_1(t_{\varepsilon_2}), \mu'_i \rangle \approx^{k} \langle \phi_2, \rho_2(t_{\varepsilon_2}), \mu'_2 \rangle : C(U_2) \). Also we know that \( \text{ilbl}(e_{11}) \approx_{\varepsilon_0} \text{ilbl}(e_{21}) \), and as \( \phi'_1 \approx_{\varepsilon_0} \phi'_2 \), by Lemma E.56, \( \phi''_{11} \approx_{\varepsilon_0} \phi''_{22} \), then as \( \phi_1 \leq_{\varepsilon_0} \phi''_{11} \), by Lemma E.61,

\[
\langle \phi_1, \text{prot}^U_{\text{ilbl}(e_{11})} \phi''_{11} (e_2 \rho_1(t_{\varepsilon_2})), \mu'_i \rangle \approx^{k} \langle \phi_2, \text{prot}^U_{\text{ilbl}(e_{21})} \phi''_{22} (e_2 \rho_2(t_{\varepsilon_2})), \mu'_2 \rangle : C(U)
\]
and the result holds by backward preservation of the relations (Lemma E.43).

Case \( \text{prot()} \). Direct by using Lemma E.61.