Implicit Self-Adjusting Computation for Purely Functional Programs

Yan Chen  Jana Dunfield  Matthew A. Hammer  Umut A. Acar

Max Planck Institute for Software Systems
chenyan@mpi-sws.org, jd169@queensu.ca, {hammer, umut}@mpi-sws.org

Abstract

Computational problems that involve dynamic data, such as physics simulations and program development environments, have been an important subject of study in programming languages. Building on this work, recent advances in self-adjusting computation have developed techniques that enable programs to respond automatically and efficiently to dynamic changes in their inputs. Self-adjusting programs have been shown to be efficient for a reasonably broad range of problems but the approach still requires an explicit programming style, where the programmer must use specific monadic types and primitives to identify, create and operate on data that can change over time.

We describe techniques for automatically translating purely functional programs into self-adjusting programs. In this implicit approach, the programmer need only annotate the (top-level) input types of the programs to be translated. Type inference finds all other types, and a type-directed translation rewrites the source program into an explicitly self-adjusting target program. The type system is related to information-flow type systems and enjoys decidable type inference via constraint solving. We prove that the translation outputs well-typed self-adjusting programs and preserves the source program’s input-output behavior, guaranteeing that translated programs respond correctly to all changes to their data. Using a cost semantics, we also prove that the translation preserves the asymptotic complexity of the source program.

Categories and Subject Descriptors D.1.1 [Programming Techniques]: Applicative (Functional) Programming; F.3.3 [Logics and Meanings of Programs]; Studies of Program Constructs

General Terms Algorithms, Languages, Performance

1. Introduction

Dynamic changes are pervasive in computational problems: physics simulations often involve moving objects; robots interact with dynamic environments; compilers must respond to slight modifications in their input programs. Such dynamic changes are often small, or incremental, and result in only slightly different output, so computations can often respond to them asymptotically faster than performing a complete re-computation. Such asymptotic improvements can lead to massive speedup in practice but traditionally require careful algorithm design and analysis (e.g., Chiang and Tamassia [1992]; Guibas [2004]; Demetrescu et al. [2005]), which can be challenging even for seemingly simple problems.

Motivated by this problem, researchers have developed language-based techniques that enable computations to respond to dynamic data changes automatically and efficiently (see Ramalingam and Reps [1993] for a survey). This line of research, traditionally known as incremental computation, aims to reduce dynamic problems to static (conventional or batch) problems by developing compilers that automatically generate code for dynamic responses. This is challenging, because the compiler-generated code aims to handle changes asymptotically faster than the source code. Early proposals [Demers et al. 1981; Push and Teitelbaum 1989; Field and Teitelbaum 1990] were limited to certain classes of applications (e.g., attribute grammars), allowed limited forms of data changes, and/or yielded suboptimal efficiency. Some of these approaches, however, had the important advantage of being implicit: they required little or no change to the program code to support dynamic change—conventional programs could be compiled to executables that respond automatically to dynamic changes.

Recent work based on self-adjusting computation made progress towards achieving efficient incremental computation by providing algorithmic language abstractions to express computations that respond automatically to changes to their data [Ley-Wild et al. 2008; Acar et al. 2009]. Self-adjusting computation can deliver asymptotically efficient updates in a reasonably broad range of problem domains [Acar et al. 2007, 2010a, 2010b], and have even helped solve challenging open problems [Acar et al. 2010b]. Existing self-adjusting computation techniques, however, require the programmer to program explicitly by using a certain set of primitives [Carlsson 2002; Ley-Wild et al. 2008; Acar et al. 2009]. Specifically the programmer must manually distinguish stable data, which remains the same, from changeable data, which can change over time, and operate on changeable data via a special set of primitives. As a result, rewriting a conventional program into a self-adjusting program requires extensive changes to the code. For example, a purely functional program will need to be rewritten in imperative style using write-once, monadic references.

In this paper, we present techniques for implicit self-adjusting computation that allow conventional programs to be translated automatically into efficient self-adjusting programs. Our approach consists of a type system for inferring self-adjusting computation types from purely functional programs and a type-guided translation algorithm that rewrites purely functional programs into self-adjusting programs.

The type system hinges on a key observation connecting self-adjusting computation to information flow [Pottier and Simonet 2003; Sabelfeld and Myers 2003]: both involve tracking data dependencies (of changeable data and sensitive data, respectively) as well as dependencies between expressions and data. Specifi-
cally, we show that a type system that encodes the changeability of data and expressions in self-adjusting computation as secrecy of information suffices to statically enforce the invariants needed by self-adjusting computation. The type system uses polymorphism to capture stable and changeable uses of the same data or expression. Our type system admits a constraint-based formulation where the constraints are a strict subset of those needed by traditional information-flow type systems. Consequently, as with information flow, our type system admits an HM(X) inference algorithm [Odersky et al. 1999] that can infer all type annotations from top-level type specifications on the input of a program.

For this work, determination of types via type inference is not an end unto itself but a means for translating purely functional programs into self-adjusting programs. To achieve this, we first present a set of compositional, non-deterministic transformation rules. Guided by the types, the rules identify the set of all changeable expressions that operate on changeable data and rewrite them into the self-adjusting target language. Then we present a deterministic translation algorithm that applies the compositional rules judiciously, considering the type and context (enclosing expressions) of each translated subexpression, to generate a well-typed self-adjusting target program.

Taken together, the type system, its inference algorithm, and the translation algorithm enable translating purely functional source programs to self-adjusting target programs using top-level type annotations on the input type of the source program. These top-level type annotations simply mark what part of the input data is subject to change. Figure 1 illustrates how source programs written in Level ML, a purely functional subset of ML, with level types, can be translated to self-adjusting programs in the target language AFL, a language for self-adjusting computation with explicit primitives [Acar et al. 2006]. We prove three critical properties of the approach.

- **Type soundness.** On source code of a given type, the translation algorithm produces well-typed self-adjusting code of a corresponding target type (Theorem 6.1).
- **Observational equivalence.** The translated self-adjusting program, when evaluated, produces the same value as the source program (Theorem 6.5).
- **Asymptotic complexity.** The time to evaluate the translated program is asymptotically the same as the time to evaluate the source program (Theorem 6.9).

Type soundness and observational equivalence together imply a critical consistency property: that self-adjusting programs respond correctly to changing data (via the consistency of the target self-adjusting language [Acar et al. 2006]). The third property shows that the translated program takes asymptotically as long to evaluate (from scratch) as the corresponding source program. In addition, it places a worst-case bound on the time taken to self-adjust via change propagation, which can and often does take significantly less time when data changes are small. To prove this complexity result, we use a cost semantics [Sands 1990; Sansom and Peyton Jones 1995] that enables precise reasoning about the complexity of the evaluation time. We do not, however, prove tighter bounds on the complexity of self-adjustments; this would be beyond the scope of this paper.

We intend to complete an implementation of our approach as an extension of Standard ML and the MLton compiler [MLton]. However, we expect the proposed approach could be implemented in other languages such as Haskell, where self-adjusting libraries also exist [Carlsson 2002]. In general, since our approach simply generates target code, it is agnostic to implementation details of the explicit self-adjusting-computation mechanisms employed in the target language and thus can be applied broadly.

**Paper guide.** We find it better to give an overview of the proposed approach by focusing on the translation problem and working back to the type system in a “top-down” manner (Section 2). The details of the translation algorithm and our theorems, however, rely on the type system. We therefore take a “bottom-up” approach in the rest of the paper: we first present the static semantics (the syntax and the type system) (Sections 3 and 4), and then describe the target language AFL (Section 5) and the translation (Section 6). Finally, we discuss related work (Section 7) and conclude. Due to space restrictions, we include all the proofs in the appendix [Chen et al. 2011].

## 2. Overview

We present an informal overview of our approach via examples. First, we briefly describe explicit self-adjusting computation, as laid out in previous work, and which we use as a target language. Then we outline our proposed approach.

### 2.1 Explicit Self-Adjusting Computation

The key concept behind explicit approaches is the notion of a **modifiable (reference)**, which stores changeable values that can change over time [Acar et al. 2006]. The programmer operates on modifiables with **mod, read, and write** constructs to create, read from, and write into modifiables. The run-time system of a self-adjusting language uses these constructs to represent the execution as a graph, enabling efficient **change propagation** when the data changes in small amounts.

As an example, consider a trivial program that computes $x^2 + y$:

```plaintext
squareplus: int * int -> int
fun squareplus (x, y) = let x2 = x * x in  
let r = x2 + y in
  r
```

To make this program self-adjusting with respect to changes in $y$, while leaving $x$ unchanged or **stable**, we assign the type `int` **mod** (of modifiables containing integers) and **read** the contents of the modifiable. The body of the **read** is a changeable expression ending with a **write**. This function has a changeable arrow type $\rightarrow$:

```plaintext
squareplus_SC: int * int mod $\rightarrow$ int
fun squareplus_SC (x, y) = let x2 = x * x in
  read y as y' in
  let r = x2 + y' in
  write(r)
```

The **read** operation delineates the code that depends on the changeable value $y$, and the changeable arrow type ensures a critical consistency property: $\rightarrow$-functions can only be called within

---

**Figure 1.** Visualizing the translation between the source language Level ML and the target language AFL, and related properties.
the context of a changeable expression. If we change the value of y, change propagation can update the result, re-executing only the read and its body, reusing the computation of the square x2.

Suppose we wish to make x changeable while leaving y stable. We need to read x and place x2 into a modifiable (because we can only read within the context of a changeable expression), and immediately read back x2 and finish by writing the sum. (To avoid creating this modifiable would require further structural changes to the code.)

\[
\text{squareplus}_{CS} : \text{int mod} \times \text{int} \rightarrow \text{int} \\
\text{fun squareplus}_{CS}(x, y) = \\
\text{let } x' = \text{mod} (\text{read } x \text{ as } x') \text{ in write}(x' \times x') \text{ in} \\
\text{read } x2 \text{ as } x2' \text{ in} \\
\text{let } r = x2' + y \text{ in} \\
\text{write}(r)
\]

As this example shows, rewriting even a trivial program can require modifications to the code, and different choices about what is or is not changeable lead to different code. Moreover, if we need \(\text{squareplus}_{SC}\) and \(\text{squareplus}_{CS}\)—for instance, if we want to pass \(\text{squareplus}\) to various higher-order functions—we must write, and maintain, both versions.

Conservatively treating all data as changeable would require writing just one version, but treating all data as modifiable can introduce unacceptably high overhead. At the other extreme, making everything stable requires no rewriting, but forges the benefits of change propagation. Instead, we take an approach where data is modifiable only where necessary.

2.2 Implicit Self-Adjusting Computation

To make self-adjusting computation implicit, we use type information to insert \text{reads}, \text{writes}, and \text{mods} automatically. The user annotates the input type of the program; we infer types for all expressions, and use this information to guide a translation algorithm. The translation algorithm returns well-typed self-adjusting target programs. The translation requires no expression-level annotations.

For the example function \(\text{squareplus}\) above, we can automatically derive \(\text{squareplus}_{SC}\) and \(\text{squareplus}_{CS}\) from just the type of the function (expressed in a slightly different form, as we discuss next).

Level types. Uniformly describe source functions (more generally, expressions) that differ only in their “changeability”, we need a more general type system than that of the target language. This type system refines types with levels \(S\) (stable) and \(C\) (changeable). The type \(\text{int}^\delta\) is an integer whose level is \(\delta\); for example, to get \(\text{squaresum}_{CS}\) we can annotate \(\text{squaresum}_{CS}\) with the type \(\text{int}^{\text{CS}}\ × \text{int}^{\text{CS}}\).

Level types are an important connection between information-flow types [Potter and Simonet 2003] and those needed for our translation: high-security secret data (level \(H\)) behaves like changeable data (level \(C\)), and low-security public data (level \(L\)) behaves like stable data (level \(S\)). In information flow, data that depends on secret data must be secret; in self-adjusting computation, data that depends on changeable data must be changeable. Building on this connection, we develop a type system with several features and mechanisms similar to information flow. Among these is level polymorphism; our type system assigns level-polymorphic types to expressions that accommodate various “changeabilities”. (As with ML’s polymorphism over types, our level polymorphism is prenex.) Another similarity is evident in our constraint-based type inference system, where the constraints are a strict subset of those in Potter and Simonet 2003]. As a corollary, our system admits a constraint-based type inference algorithm [Akersky et al. 1999].

Translation. The main purpose of our type system is to support translation. Given a source expression and its type, translation in-

\[
\text{fun inc} : \text{int } \rightarrow \text{int} \\
\text{fun inc}(x) = x+1 \\
\begin{array}{ll}
\text{map} : (\alpha \rightarrow \beta) & \rightarrow \alpha \text{ list } \rightarrow \beta \text{ list} \\
\text{fun map} & f \ 1 = \\
\text{case } 1 \text{ of} \\
\text{nil} & \Rightarrow \text{nil} \\
\text{cons}(h, t) & \Rightarrow \text{cons}(f_\text{h}, \text{map } f \ t)
\end{array}
\]

\[
\begin{array}{ll}
\text{mapPair} : (\text{int list } \times \text{int list}) & \rightarrow (\text{int list } \times \text{int list}) \\
\text{fun mapPair} & (1, a) = (\text{map inc } 1, \text{map inc } a)
\end{array}
\]

Figure 2. Function \text{mapPair} in ML

\[
\begin{array}{ll}
\text{inc} : \text{int } \rightarrow \text{int} \\
\text{fun inc}(x) = x+1 \\
\text{map} : (\alpha \rightarrow \beta) & \rightarrow \alpha \text{ list } \rightarrow \beta \text{ list} \\
\text{fun map} & f \ 1 = \\
\text{case } 1 \text{ of} \\
\text{nil} & \Rightarrow \text{nil} \\
\text{cons}(h, t) & \Rightarrow \text{cons}(f_\text{h}, \text{map } f \ t)
\end{array}
\]

Figure 3. Function \text{mapPair} same as in Figure 1.

serves the appropriate \text{mod, read, and write} primitives and structures the code to produce an expression that is well-typed in the target language. The type system of the target language, which is explicitly self-adjusting, is monomorphic in the levels or changeability, while the implicitly self-adjusting source language is polymorphic over levels. Consequently, translation also needs to monomorphicize the source code. Our translation generates code that is well-typed, has the same input-output behavior as the source program, and is, at worst, a constant factor slower than the source program.

Since the source and target languages differ, proving these properties is nontrivial; in fact, the proofs critically guided our formulation of the type system and translation algorithm.

A more detailed example: \text{mapPair}. To illustrate how our translation works, consider a function \text{mapPair} that takes two integer lists and increments the elements in both lists. This function can be written by applying the standard higher-order \text{map} over lists. Figure 4 shows the purely functional code in an ML-like language for an implementation of \text{mapPair}, with a datatype \(\alpha \text{ list}\), an increment function \text{inc}, and a polymorphic \text{map} function. Type signatures give the types of functions.

To obtain a self-adjusting \text{mapPair}, we first decide how we wish to allow the input to change. Suppose that we want to allow insertion and deletion of elements in the first list, but we expect the length of the second list to remain constant, with only its elements changing. We can express this with the versions of the list type with different changeability:

\[
\begin{array}{ll}
\alpha \text{ list}^\delta & \text{for lists of } \alpha \text{ with changeable tails;} \\
\alpha \text{ list}^\delta & \text{for lists of } \alpha \text{ with stable tails.}
\end{array}
\]

Then a list of integers allowing insertion and deletion has type \(\text{int}^\delta \text{ list}^\delta\), and one with unchanging length has type \(\text{int}^\delta \text{ list}^\delta\).

Now we can write the type annotation on \text{mapPair} shown in Figure 4. Given only that annotation, type inference can find appropriate types for \text{inc} and \text{map} and our translation algorithm generates self-adjusting code from these annotations. Note that to obtain a self-adjusting program, we only had to provide types for the function. We call this language with level types Level ML.

Target code for \text{mapPair}. Translating the code in Figure 4 produces the self-adjusting target code in Figure 5. Note that \text{inc} and \text{map} have level-polymorphic types. In \text{map inc 1} we increment sta-
The interplay of type inference and translation. Given user annotations on the input, type inference finds a satisfying type assignment, which then guides our translation algorithm to produce self-adjusting code. In many cases, multiple type assignments could satisfy the annotations; for example, subsumption allows any stable type to be promoted to a changeable type. Translation yields target code that satisfies the crucial type soundness, operational equivalence, and complexity properties under any satisfying assignment.

Levels \( \delta, \varepsilon ::= \delta \mid \varepsilon \mid \alpha \)

Types \( \tau ::= \text{int}^\delta \mid (\tau_1 \times \tau_2)^\delta \mid (\tau_1 + \tau_2)^\delta \mid (\tau_1 \rightarrow \tau_2)^\delta \)

Constraints \( C, D ::= \text{true} \mid \text{false} \mid \exists \tilde{\alpha} \ C \land D \mid \alpha = \beta \mid \beta \mid \delta \triangleleft \tau \)

Type schemes \( \sigma ::= \tau \mid \forall \tilde{\alpha} [D], \tau \)

Figure 5. Levels, constraints, types, and type schemes

But some type assignments are preferable, especially when one considers constant factors. Choosing \( C \) levels whenever possible is always a viable strategy, but treating all data as changeable results in more overhead. As in information flow, where we want to consider data secret only when absolutely necessary, inference yields principal typings that are minimally changeable, always preferring \( S \) over \( C \).

3. From Information Flow Types to SAC

Self-adjusting computation separates the computation and data into two parts: stable and changeable. Changeable data refers to data that can change over time; all non-changeable data is stable. Similarly, changeable expressions refers to expressions that operate (via elimination forms) on changeable data; all non-changeable expressions are stable. Evaluation of changeable expressions (that is, changeable computations) can change as the data that they operate on changes: changes in data cause changes in control flow. These distinctions are critical to effective self-adjustment: previous work shows that it suffices to track and remember changeable data and evaluations of changeable expressions because stable data and evaluations of stable expressions remain invariant over time. Previous work therefore presents languages that enable the programmer to separate stable and changeable data, and type systems that enforce the correct usage of these constructs.

In this section, we describe the self-adjusting computation types that we infer for purely functional programs. A key insight behind our approach is that in information-flow type systems, secret (high-security) data is infectious: any data that depends on secret data itself must be secret. This corresponds to self-adjusting computation: data that depends on changeable data must itself be changeable. In addition, self-adjusting computation requires expressions that inspect changeable data—elimination forms—to be changeable. To encode this invariant, we extend function types with a mode, which is either stable or changeable; only changeable functions can inspect changeable data. This additional structure preserves the spirit of information flow-based type systems, and, moreover, supports constraint-based type inference in a similar style.

The starting point for our formulation is Pottier and Simone[2003]. Our types include two (security) levels, stable and changeable. We generally follow their approach and notation. The two key differences are that (1) since Level ML is purely functional, we need no “program counter” level “pc”; (2) we need a mode \( \varepsilon \) on function types.

Levels \( \delta, \varepsilon ::= \delta \mid \varepsilon \mid \alpha \)

Types \( \tau ::= \text{int}^\delta \mid (\tau_1 \times \tau_2)^\delta \mid (\tau_1 + \tau_2)^\delta \mid (\tau_1 \rightarrow \tau_2)^\delta \)

Constraints \( C, D ::= \text{true} \mid \text{false} \mid \exists \tilde{\alpha} \ C \land D \mid \alpha = \beta \mid \beta \mid \delta \triangleleft \tau \)

Type schemes \( \sigma ::= \tau \mid \forall \tilde{\alpha} [D], \tau \)

1 In Pottier and Simone[2003], product types are low-security (stable) because pairing adds no extra information. In our setting, changeable products give more control over the granularity of change propagation.
\( \delta \leq \delta' \) (subint)

\( \tau_1 :<: \tau'_1 \quad \tau_2 :<: \tau'_2 \quad \delta :<: \delta' \) (subProd)

\( \delta \leq \delta' \)

\( \tau_1 :<: \tau'_1 \quad \tau_2 :<: \tau'_2 \quad \delta :<: \delta' \) (subSum)

\( \epsilon = \epsilon' \)

\( \delta :<: \delta' \)

\( \tau_1 :<: \tau'_1 \quad \tau_2 :<: \tau'_2 \) (subArrow)

**Figure 6.** Subtyping

\( \frac{\delta :<: \int^\sigma}{\tau :<: \int^\tau} \) (<-Int)

\( \frac{\delta :<: \int^\sigma}{\tau :<: \int^\tau} \) (<-Prod)

\( \frac{\delta :<: \tau}{\delta :<: \tau} \) (<-Arrow)

\( \frac{\delta :<: \tau}{\delta :<: \tau} \) (<-Sum)

**Figure 7.** Lower bound of a type

\( \frac{\tau_1 :<: \tau_2}{\int^\tau \leq \int^\sigma} \) O.S.

\( \frac{\tau_1 :<: \tau_2}{\int^\tau \leq \int^\sigma} \) O.S.

\( \frac{\tau_1 :<: \tau_2}{\int^\tau \leq \int^\sigma} \) O.S.

\( \frac{\tau_1 :<: \tau_2}{\int^\tau \leq \int^\sigma} \) O.S.

\( \frac{\tau_1 :<: \tau_2}{\int^\tau \leq \int^\sigma} \) O.C.

\( \frac{\tau_1 :<: \tau_2}{\int^\tau \leq \int^\sigma} \) O.C.

\( \frac{\tau_1 :<: \tau_2}{\int^\tau \leq \int^\sigma} \) O.C.

\( \frac{\tau_1 :<: \tau_2}{\int^\tau \leq \int^\sigma} \) O.C.

\( \frac{\tau_1 :<: \tau_2}{\int^\tau \leq \int^\sigma} \) O.C.

\( \frac{\tau_1 :<: \tau_2}{\int^\tau \leq \int^\sigma} \) O.C.

**Figure 8.** Outer-stable and outer-changeable types, and equality up to outer levels

The mode \( \varepsilon \) is the level of the computation encapsulated by the function. This mode determines how a function can manipulate changeable values: a function in stable mode cannot directly manipulate changeable values; it can only pass them around. By contrast, a changeable-mode function can directly manipulate changeable values. The outer level \( \delta \) is the level of the function itself, as a value. We say that a type is *ground* if it contains no level variables.

**Subtyping.** Figure 6 shows the subtyping relation \( \tau :<: \tau' \), which is standard except for the levels. It requires that the outer level of the subtye is smaller than the outer level of the supertype and that the modes match in the case of functions: a stable-mode function is never a subtype of supertype of a changeable-mode function. (It would be sound to make stable-mode functions subtypes of changeable-mode functions, but changeable mode functions are more expensive; silent coercion would make performance less predictable.)

**Levels and types.** We rely on several relations between levels and types to ascertain various invariants. A type \( \tau \) is *higher than* \( \delta \), written \( \delta :<: \tau \), if the outer level of the type is at least \( \delta \). In other words, \( \delta \) is a lower bound of the outer level(s) of \( \tau \). Figure 6 defines this relation. We distinguish between outer-stable and outer-changeable types (Figure 8). We write \( \tau \) O.S. if the outer level of \( \tau \) is \( \mathbb{S} \). Similarly, we write \( \tau \) O.C. if the outer level of \( \tau \) is \( \mathbb{C} \). Finally, two types \( \tau_1 \) and \( \tau_2 \) are *equal up to their outer levels*, written \( \tau_1 \cong \tau_2 \), if \( \tau_1 = \tau_2 \) or they differ only in their outer levels.

**Constraints.** To perform type inference, we extend levels with level variables \( \alpha \) and \( \beta \), and use a constraint solver to find solutions for the variables. Our constraints \( \Gamma, D \) include level-variable comparisons \( \leq \) and level-type comparisons \( \delta :<: \tau \), which type inference composes into conjunctions of satisfaction predicates \( \exists \alpha \exists \tau \).

The subtyping and lower bound relations defined in Figures 6 and 7 consider closed types only. For type inference, we can extend these with a constraint to allow non-closed types.

A (ground) assignment, written \( \phi \), substitutes concrete levels \( \mathbb{S} \) and \( \mathbb{C} \) for level variables. An assignment \( \phi \) satisfies a constraint \( \Gamma \), written \( \phi \vdash \Gamma \), if and only if \( \Gamma \) holds true after the substitution of variables to ground types as specified by \( \phi \). We say that \( \Gamma \) *entails* \( \Delta \), written \( \Gamma \models D \), if and only if every assignment \( \phi \) that satisfies \( \Gamma \) also satisfies \( \Delta \). We write \( \phi(\alpha) \) for the solution of \( \alpha \in \phi \), and \( [\phi] \tau \) for the usual substitution operation on types. For example, if \( \phi(\alpha) = \mathbb{S} \) then \( [\phi] \) \( (\int^\alpha + \int^\tau) \) \( ^\mathbb{S} \) \( = (\int^\alpha + \int^\tau) \). 

**Type schemes.** A type scheme \( \sigma \) is a type with universally quantified level variables: \( \sigma = \forall \alpha [\phi(\alpha) \sigma(\alpha)] \). We say that the variables \( \alpha \) are bound by \( \sigma \). The type scheme is bounded by the constraint \( \Delta \), which specifies the conditions that must hold on the variables. As usual, we consider type schemes equivalent under capture-avoiding renaming of their bound variables. Ground types can be written as type schemes, e.g. \( \int^\mathbb{C} \) as \( \forall \alpha [\text{true}] \int^\alpha \).

4. Source Language

4.1 Static Semantics

**Syntax.** Figure 9 shows the syntax for our source language Level ML, a purely functional language with integers (as base types), products, and sums. The expressions consist of values (integers, pairs, tagged values, recursive functions), projections, case expressions, function applications, and let bindings. For convenience, we consider only expressions in A-normal form, which names intermediate results. A-normal form simplifies some technical issues, while maintaining expressiveness.

**Constraint-based type system.** We could define types as

\[ \tau ::= \int | \tau_1 \times \tau_2 | \tau_1 + \tau_2 | \tau_1 \rightarrow \tau_2 \]

Such a type system would be completely standard. Instead, we use a richer type system that allows us to directly translate Level ML programs into self-adjusting programs in AFL. This constraint-based type system has the level-decorated types, constraints, and type schemes in Figure 5 and described in Section 4.2. After discussing the rules themselves, we will look at type inference (Section 4.3).

Typing takes place in the context of a constraint formula \( \Gamma \) and a typing environment \( \Gamma \) that maps variables to type schemes: \( \Gamma ::= \cdot \mid \tau \vdash \phi \mid \Gamma, x : \tau \)

The typing judgment \( \Gamma, \tau \vdash \varepsilon \tau \) has a constraint \( \Gamma \) and typing environment \( \Gamma \), and infers type \( \tau \) for expression \( \varepsilon \) in mode \( \varepsilon \). Beyond the usual typing concerns, there are three important aspects of the typing rules: the determination of modes and levels, level polymorphism, and constraints. To help separate concerns, we discuss constraints later in the section—at this time, the reader can ignore the constraints in the rules and read \( \Gamma, \tau \vdash \varepsilon \tau \) read \( \Gamma \vdash \delta \leq \tau \), as \( \delta \leq \tau \), and so on.

The mode of each typing judgment affects the types that can be used “directly” by the expression being typed. Specifically, the mode discipline prevents the elimination forms from being applied
Under constraint $C$ and source typing environment $\Gamma$, source expression $e$ has type $\tau$:

$$C; \Gamma \vdash e : \tau$$

### Typing rules for Level ML

#### (SVar)

$$C; \Gamma \vdash e : \tau \quad \text{and} \quad e \in \text{int}$$

#### (SLetV)

$$C; \Gamma \vdash \text{let } x = : \tau_1 \times \tau_2 \gamma \quad e_1 : \epsilon \quad e_2 : \tau \quad C \vdash \epsilon \leq \tau$$

#### (SPrim)

$$C; \Gamma \vdash x : (\tau_1 \times \tau_2 \gamma) \delta \quad C \vdash \delta \leq \epsilon$$

#### (SApp)

$$C; \Gamma \vdash x : \tau \quad C; \Gamma \vdash e : \tau' \quad C; \Gamma \vdash x : \tau'' \propto e_2 : \tau \quad C \vdash \tau' \triangleq \tau''$$

#### (SLetE)

$$C; \Gamma \vdash e : \epsilon = \epsilon$$

#### (SSum)

$$C; \Gamma \vdash \text{inr } (x_1, x_2) : \text{int}^t$$

#### (SCase)

$$C; \Gamma \vdash \text{case } x \text{ of } \{x_1 : \epsilon_1, x_2 : \epsilon_2\} : \tau$$

### Figure 10. Typing rules for Level ML

---

To changeable values in the stable mode. This is a key principle of the type system.

No computation happens in values, so they can be typed in either mode. The typing rules for variables (SVar), integers (SLetV), pairs (SPair), and sums (SSum) are otherwise standard (we omit the symmetric judgment $\text{inr } v$). Rule (SVar) instantiates a variable’s polymorphic type. For clarity, we also make explicit the renaming of the quantified type variables $\alpha$ to some fresh $\beta$ (which will be instantiated later by constraint solving). To type a function (SFun), we type the body in the mode $\epsilon$ specified by the function type $(\tau_1 \to \tau_2) \gamma$, and require the result type $\tau_2$ to be higher than the mode, $\epsilon \leq \tau_2$. As a result, a changeable-mode function must have a changeable return type. This captures the idea that a changeable-mode function is a computation that depends on changeable data, and thus its result must accommodate changes to that data. Primitive operators $\oplus$ take two stable integers and return a stable integer result.

As is common in Damas-Milner-style systems, when typing let we can generalize variables in types (in our system, level variables) to yield a polymorphic value only when the bound expression is a value. This value restriction is not essential because Level ML is pure, but facilitates adding side effects at a later date. In the first case (SLetE), the expression bound may be a non-value, so we do not generalize and simply type the body in the same mode as the whole let, assuming that the bound expression has the specified type in any mode $\epsilon$. We allow subsumption only when the subtype and supertype are equal up to their outer levels, e.g. from a bound expression $c_1$ of subtype $\text{int}^t$ to an assumption $x : \text{int}^t$. This simplifies the translation, with no loss of expressiveness: to handle "deep" subsumption, such as $(\text{int}^t \to \text{int}^t)^t \leq (\text{int}^t \to \text{int}^t)^t$, we can insert coercions into the source program before typing it with these rules. (This process could easily be automated.)

In the second case (SLetV), when the expression bound is a value, we type the let expression in mode $\epsilon$ by typing the body in the same mode $\epsilon$, assuming that the value bound is typed in the stable mode (the mode is ignored in the rules typing values). As in (SLetE), we allow subsumption on the bound value only when the types are equal up to their outer level. Because we are binding a value, we generalize its type by quantifying over the type’s free level variables.

Function application, $\oplus$, $\text{fst}$, and $\text{case}$ are the forms that eliminate values of changeable type. An application is typed in the mode $\epsilon$ of the function being applied because changeable functions can operate on changeable values; the typing mode must match $(\epsilon \leq \epsilon)$. Furthermore, the result of the function must be higher than the function’s level: if a function is itself changeable, $(\tau_1 \to \tau_2) \gamma$, then it could be replaced by another function and thus the result of this application must be changeable. (Due to let-subsumption, checking this in (SFun) alone is not enough.)

The rule (SCase) types a case expression, in either mode $\epsilon$, by typing each branch in $\epsilon$. The mode $\epsilon$ must be higher than the level $\delta$ of the scrutinee to ensure that a changeable sum type is not inspected at the stable mode. Furthermore, the level of the result $\tau$ must also be higher than $\delta$: if the scrutinee changes, we may take the other branch, requiring a changeable result.

Rule (SLetF) enforces a condition, similar to (SCase), that we can project out of a changeable tuple of type $(\tau_1 \times \tau_2 \gamma)^t$ only in changeable mode. We omit the symmetric rule for $\text{snd}$.

Our premises on variables, such as the scrutinee of (SCase), are stable-mode ($\geq t$), but this was an arbitrary decision; since (SVar) is the only rule that can derive such premises, their mode is irrelevant.

#### 4.2 Constraints and Type Inference

Many of the rules simply pass around the constraint $C$. An implementation of rules with constraint-based premises, such as (SFun), implicitly adds those premises to the constraint, so that $C = \ldots \land (\epsilon \leq \tau_2)$. Rule (SLetV) generalizes level variables instead of type variables, with the “occurs check” $\alpha \cap \text{FV}(C, \Gamma) = \emptyset$.

Standard techniques in the tradition of Damas and Milner [1982] can infer types for Level ML. In particular, our rules and constraints fall within the HM(X) framework [Odersky et al. 1999], permitting inference of principal types via constraint solving. As always, we cannot infer the types of polymorphically recursive functions.

Using a constraint solver that, given the choice between assigning $\epsilon$ or $C$ to some level variable, prefers $\epsilon$, inference finds principal typings that are minimally changeable. Thus, data and computations will only be made changeable—and incur tracking overhead—where necessary to satisfy the programmer’s annotation. This corresponds to preferring a lower security level in information flow [Pottier and Simone 2003].

---

2 In the target language, bound expressions must be stable-mode, but the translation puts changeable bound expressions inside a mod, yielding a stable-mode bound expression.
4.3 Dynamic Semantics

The call-by-value semantics of source programs is defined by a big-step judgment $e \triangleright v$, read “$e$ evaluates to value $v$”. Our rules in Figure 13 are standard; we write $[v/x]e$ for capture-avoiding substitution of $v$ for the variable $x$ in $e$.

5. Target Language

The target language AFL (Figure 11) is a self-adjusting language with modifiables. In addition to integers, products, and sums, the target type system makes a modal distinction between ordinary types (e.g. int) and modifiable types (e.g. int mod). It also distinguishes stable-mode and changeable-mode functions. Level polymorphism is supported through an explicit select construct and an explicit polymorphic instantiation. In Section 6 we describe how polymorphic source expressions become selects in AFL.

The values of the language are integers, variables, polymorphic variable instantiation $x[\vec{\alpha} = \vec{\delta}]$, locations $\ell$ (which appear only at runtime), pairs, tagged values, stable and changeable functions, and the select construct, which acts as a function and case expression on levels: if $x$ is bound to select $\{(\alpha = S) \Rightarrow e_1 \; | \; (\alpha = C) \Rightarrow e_2\}$ then $x[\vec{\alpha} = \vec{S}]$ yields $e_1$. The symbol $\vec{\delta}$ stands for a bare variable $x$ or an instantiation $x[\vec{\alpha} = \vec{\delta}]$.

We distinguish stable expressions $e^S$ from changeable expressions $e^C$. Stable expressions create purely functional values; apply$^S$ applies a stable-mode function. The mod construct evaluates a changeable expression and writes the output value to a modifiable, yielding a location, which is a stable expression. Changeable expressions are computations that end in a write of a pure value. Changeable-mode application apply$^C$ applies a changeable-mode function.

The let construct is either stable or changeable according to its body. When the body is a changeable expression, let enables a changeable computation to evaluate a stable expression and bind its result to a variable. The case expression is likewise stable or changeable, according to its case arms. The read expression binds the contents of a modifiable $\vec{\delta}$ to a variable $y$ and evaluates the body of the read.

The typing rules in Figure 12 follow the structure of the expressions. Rule (TSelect) checks that each monomorphized expression $e_i$ in a select has type $||\vec{\delta}/\vec{\alpha}||\tau$, where $||\vec{\delta}/\vec{\alpha}||\tau$ is a source-level polymorphic type with the levels $\vec{\delta}$ substituted for the variables $\vec{\alpha}$, and $||\_\_\_\_||\tau$ translates source types to target types (see Section 6.1). Rule (TPVar) is a standard rule for variables of monomorphic type, but rule (TVar) gives the instantiation $x[\vec{\alpha} = \vec{\delta}]$ of a variable $x$ of polymorphic type, the type $||\vec{\delta}/\vec{\alpha}||\tau$—matching the monomorphic expression from the select to which $x$ is bound.

5.1 Dynamic Semantics

For the source language, our big-step evaluation rules (Figure 13) are standard. In the target language AFL, our rules (Figure 14) model the evaluation of a first run of the program: modifiables are created, written to (once), and read from (any number of times), but never updated to reflect changes to the program input. Both sets of rules permit expressions that are not in A-normal form, enabling
In the store $\rho$, target expression $e$ evaluates to $w$ with updated store $\rho'$.

\[
\rho \vdash e \downarrow \rho' \downarrow w
\]
returns a type of the form $\langle \cdots \rangle \, \text{mod}$; however, since the value being returned may contain subexpressions that will be placed into modifiables, we use $|||\cdot|||$ for the inner types. For instance, $|||\langle x + x \rangle\,\text{mod}|||$.

These functions are defined on closed contexts—types with no free level variables. Before applying one of these functions to a type found by the constraint typing rules, we always need to apply the satisfying assignment $\phi$ to the type, so for convenience we write $|||\phi\,\tau|||$ for $|||\phi\,|||\tau|||$, and so on. Because the translation only makes sense for closed types, type schemes $\forall\alpha(D)\,\tau$ cannot be translated. The translation $|||\cdot|||$ therefore translates only monomorphic types $\tau$; type schemes are left alone (except for replacing the symbol $\forall$ with $\Pi$) until instantiation. Once instantiated, the type scheme is an ordinary closed source type, and can be translated by rule (TVar).

### 6.2 Translating Expressions

We define the translation of expressions as a type of set-directed rules. Given (1) a derivation of $C; \Gamma \vdash \alpha : \tau$ in the constraint-based typing rules and (2) a satisfying assignment $\phi$ for $C$, it is always possible to produce a correctly typed stable target expression $e^C$ and a correctly typed changeable target expression $e^\tau$ (see Theorem $6.3$ below). The environment $\Gamma$ in the translation rules is a source stable environment, but must have no free level variables. Given an environment $\Gamma$ from the constraint typing, we apply the satisfying assignment $\phi$ to eliminate its free level variables before using it for the translation: $|||\phi\,\Gamma|||$. With the environment closed, we need not refer to $C$.

Many of the rules in Figure $17$ are purely syntax-directed and are similar to the constraint-based rules. One exception is the (Var) rule, which needs the source type to know how to instantiate the level variables in the type scheme. For example, given the polymorphic $\alpha : \forall\alpha(\text{true})\to(\text{int}^\alpha)\,\text{mod}$, we need the type from $C; \Gamma \vdash x : (\text{int}^\alpha \to \text{int}^\alpha)\,\text{mod}$ so we can instantiate $\alpha$ in the translated term $x[\alpha = C]$.

![Figure 15. Stabilization of types $|\tau|^C$; translations $|||\cdot|||$ and $|||\cdot|||^C$ of types; translation of typing environments $|||\Gamma|||$](image)

**Figure 15.** Stabilization of types $|\tau|^C$; translations $|||\cdot|||$ and $|||\cdot|||^C$ of types; translation of typing environments $|||\Gamma|||$.

Our rules are nondeterministic, avoiding the need to “decorate” them with context-sensitive details. Our algorithm in Section $6.3$ resolves the nondeterminism through type information.

**Stable rules.** The rules (Int), (Var), (Pair), (Fun), (Sum), (Fst) and (Prim) can only translate in the stable mode. To translate to a changeable expression, use a rule that shifts to changeable mode.

**Shifting to changeable mode.** Given a translation of $e$ in the stable mode to some $e^\tau$, the rules (Write) and (ReadWrite) at the bottom of Figure $17$ translate $e$ in the changeable mode, producing an $e^C$. If the expression’s type $\tau$ is outer stable (say, $\text{int}^C$), the (Write) rule simply binds it to a variable and then writes that variable. If $\tau$ is outer changeable (say, $\text{int}^\tau$) it will be in a modifiable at runtime, so we read it into $\tau'$ and then write it. (The let-binders merely satisfy the requirements of $A$-normal form.)

**Shifting to stable mode.** To generate a stable expression $e^\tau$ based on a changeable expression $e^C$, we have the (Lift) and (Mod) rules. These rules require the source type $\tau$ to be outer changeable: in (Lift), the premise $|\tau|^C = \tau'$ requires that $|\tau|^C$ is defined, and it is defined only for outer changeable $\tau$; in (Mod), the requirement is explicit: $|\tau|^C \o O\,C$.

(Mod) is the simpler of the two: if $e$ translates to $e^C$ at type $\tau$, then $e$ translates to the stable expression $\text{mod} e^C$ at type $\tau$. In (Lift), the expression is not translated at the given type $\tau$ but at its stabilized $|\tau|^C$, capturing the “shallow subsumption” in the constraint typing rules (SLetE) and (SLetV); a bound expression of type $\tau_0^C$ can be translated at type $\tau_0^C$ to $e^C$, and then “promoted” to type $\tau_0^\tau$ by placing it inside a mod.

**Reading from changeable data.** To use an expression of changeable type in a context where a stable value is needed—such as passing some $x : \text{int}^C$ to a function expecting $\text{int}^C$—the (Read) rule generates a target expression that reads the value out of $x : \text{int}^C$ into a variable $x' : \text{int}^\tau$. The variable-removing judgment $\Gamma \vdash e \sim (x \gg x') : \tau \to e'$ takes the expression $e$, finds a variable $x$ about to be used, and yields an expression $e'$ with that occurrence replaced by $x'$. For example, $\Gamma \vdash \text{case}\, x\,\text{of}\,\cdots\sim (x \gg x') : \tau \to \text{case}\, x'\,\text{of}\,\cdots$. This judgment is derivable only for $\text{apply}$, $\text{case}$, $\text{fst}$, and $\oplus$, because these are the elimination forms for outer-changeable data. For $\oplus(x_1, x_2)$, we need to read both variables, so we have one rule for each. The rules are given in Figure $16$. 

![Figure 16. Renaming the variable to be read (elimination forms)](image)
Monomorphization. A polymorphic source expression has no directly corresponding target expression: the map function from Section 5 corresponds to the two functions map,SC and map,CS. Given a polymorphic source value \( v : \forall \alpha [D] \), the (LetV) rule translates \( v \) once for each instantiation \( \delta_i \) that satisfies the constraint \( D \) (each \( \delta_i \) such that \( \alpha \equiv \delta_i \vdash D \)). That is, we translate the value at source type \( [\delta_i / \alpha][\tau] \). This yields a sequence of source expressions \( e_1, \ldots, e_n \) for the \( n \) possible instances. For example, given \( \forall \alpha [\tau] \), \( \tau \), we translate the value at type \( \forall \alpha [\tau] \) yielding \( e_1 \) and at type \( \forall \alpha [\tau] \) yielding \( e_2 \). Finally, the rule produces a select expression, which acts as a function that takes the desired instance \( \delta_i \) and returns the appropriate \( e_i \).

Since (LetV) generates one function for each satisfying \( \delta_i \), it can create up to \( 2^n \) instances for \( n \) variables. However, dead-code elimination can remove functions that are not used. Moreover, the functions that are used would have been handwritten in an explicit setting, so while the code size is exponential in the worst case, the saved effort is as well.

6.3 Algorithm

The system of translation rules in Figure 17 is not deterministic. In fact, if the wrong choices are made it can produce painfully inefficient code. Suppose we have \( 2 : \text{int} \), and want to translate it to a stable target expression. Choosing rule (Int) yields the target expression 2. But we could use (Int), then (ReadWrite)—which generates \( e_2 \) with a let, a read and a write—then (Mod), which wraps that \( e_2 \) into a mod. Clearly, we should have stopped with (Int).

To resolve this nondeterminism in the rules would complicate them further. Instead, we give the algorithm in Figure 18 which examines the source expression \( e \) and, using type information, applies the rules necessary to produce an expression of mode \( e \).

6.4 Properties

Given a constraint-based source typing derivation and assignment \( \phi \) for some term \( e \), there are translations from \( e \) to (1) a stable \( e^\delta \) and (2) a changeable \( e^\tau \), with appropriate target types:

**Theorem 6.1 (Translation Type Soundness).**

If \( C ; \Gamma \vdash e : \tau \) and \( \phi \) is a satisfying assignment for \( C \) then

1. (there exists \( e^\phi \) such that \( \phi \vdash e : \tau \))
2. (there exists \( e^\phi \) such that \( \phi \vdash e : \tau \) and \( \|C\|_\phi \vdash e : \tau \))

The proof (in the appendix [Chen et al. 2011]) is by induction on the height of the given derivation of \( C ; \Gamma \vdash e : \tau \). If the concluding rule was (SLet), we use a substitution property (Lemma A.2) for each \( \delta_i \) to get a monomorphic constraint typing derivation; that derivation is no larger than the input derivation, so we can apply the induction hypothesis to get a translated \( e_i \). The proof constructs the same translation derivations as the algorithm in Figure 18 (in fact, we extracted the algorithm from the proof).

We also prove that running a translated program gives the same result as running the source program. Theorem 6.5 states that in an initially empty store \( s \), if evaluating the translated program \( e' \) yields \( v' \) with new store \( s' \), then \( e \) evaluates to \( v \) where \( v \) corresponds to \( [s'/\delta_i] \) (the result of substituting values in the store \( s' \) for locations appearing in \( v' \)).

To define this correspondence, we use a device somewhat similar to logical relations: a relation \( \approx \) on source and target expressions, allowing us to show that if \( e : \tau \approx e' : \tau \), then \( v : \tau \approx [\delta_i / \alpha] [\tau] \). Both \( e \) and \( e' \) must be closed. Our definition is weaker than the equivalence relations used in logical relations proofs: \( \text{apply}(id, 4) \not\approx 4 \), for example. It does not attempt to equate all programs that have the same meaning, but only particu-
We also relate substitutions: a source substitution \(s\) and a target substitution \(\tau\):

\[
\tau = v_1/x_1, \ldots, v_n/x_n
\]

are related at their environments \(\Gamma = x_1 : \tau_1, \ldots, x_n : \tau_n\) and \(\Gamma' = x_1 : \tau_1', \ldots, x_n : \tau_n', \) written

\[
(v_1/x_1, \ldots, v_n/x_n) : (x_1 : \tau_1, \ldots, x_n : \tau_n)
\]

\[
\tau = v_1/x_1, \ldots, v_n/x_n : \Gamma
\]

if, for all \(k\) from 1 to \(n\), we have \(\tau_k = \tau_k \circ \tau_i : \tau_i\).

The key lemma (Lemma 6.3) is that if \(e \equivalence e'\), the target program \(e'\) is related to \(e\). Combined with Theorem 6.4, which shows that related programs evaluate to related values, this means that the translated program \(e'\) evaluates to the same value that \(e\) does. (Actually, \(e'\) is a value related to that value; only at \(\int^\downarrow/\int^\uparrow\), and products thereof, are they identical.)

We begin by defining a store substitution operation:

**Definition 6.2.** The store substitution \([\rho]e\) is defined as an ordinary substitution, except for \(e = \xi\) in which case \([\rho]e = [\rho](\mod \xi)\).

For example, \([\xi_1 \mapsto 1, \xi_2 \mapsto 2](\xi_1, \xi_2) = (\mod 1, \mod 2)\).

Proofs and several other lemmas can be found in the appendix [Chen et al. 2011].

**Lemma 6.3 (Relation of Translation).** If \(\Gamma \vdash e : \tau \equivalence e'\) and \(\vdash s : \Gamma \rightarrow s : [\Gamma]\) and \(\Gamma' = \Gamma \circ s : [\Gamma]\) then

\[
[s]e :: [s]e' \equivalence : [s]\tau'
\]

where \(\tau' = ||\tau||\) if \(\xi = S\) and \(\tau' = ||\tau||^\downarrow\downarrow\) if \(\xi = C\).

**Theorem 6.4 (Generalized Translation Soundness).**

\[
\xi = [\rho]e' : \tau' \downarrow [\rho]\uparrow \downarrow w \downarrow
\]

then \(\tau' : e \downarrow v \downarrow\) where \(v = \xi \circ [\rho]w : [\rho]\xi\).

**Translation soundness** now follows from Lemma 6.3 and Theorem 6.4.

**Theorem 6.5 (Translation Soundness).** If \(\vdash e : \tau \equivalence e'\) and \(\vdash e' \downarrow [\rho]\uparrow w\), then \(e \downarrow v\) where \(v = [\rho]w : [\rho]\xi\).

Finally, we extend Theorem 6.5 to further show that the size \(W(D)\) of the derivation of the target-language evaluation is within a constant factor of the size \(W(D')\) of the derivation of \(e \downarrow v\). We need a few definitions and intermediate results, which can be found in the appendix. The proof hinges on classifying the keywords added by the translation, such as \texttt{write}, as “dirty”: a dirty keyword will lead to applications of the dirty rule (TEvWrite) in the evaluation derivation; such applications have no equivalent in the source-language evaluation.

We then define the “head cost” \(HC\) of terms and derivations, which counts the number of dirty rules applied near the root of the term, or the root of the derivation, without passing through clean parts of the term or derivation. Just counting all the dirty keywords in a term would not rule out a \(\beta\)-reduction duplicating a particularly dirty part of the term. By defining head cost and proving that the translation generates terms with bounded head cost—including for all subterms—we ensure that no part of the term is too dirty; consequently, substituting a subterm during evaluation yields terms that are not too dirty.

**Definition 6.6.** A term \(e\) is shallowly \(k\)-bounded if \(HC(e) \leq k\).

A term \(e\) is deeply \(k\)-bounded if every subterm of \(e\) (including \(e\) itself) is shallowly \(k\)-bounded. Similarly, a derivation \(D\) is shallowly \(k\)-bounded if \(HC(D) \leq k\), and deeply \(k\)-bounded if all its subderivations are shallowly \(k\)-bounded.

**Theorem 6.7.** If \(\trans(e, e') = e'\) then \(e'\) is deeply \(6\)-bounded.
where for every subderivation \( D \) of
provides a fully automatic incremental invariant checker. The ap-
2008; Hammer et al. 2009]. DITTO [Shankar and Bodik 2007]
syntactically separating stable and changeable data, as well as code
features allow writing self-adjusting programs but these require
self-adjusting computation include dynamic dependence graphs,
extensively [Ramalingam and Reps 1993; Demers et al. 1981; Pugh
and Teitelbaum 1989; Abadi et al. 1998]. Key techniques behind
self-adjusting computation include dynamic dependence graphs,
which allows a fully general change propagation mechanism [Acar
et al. 2008], and a form of memoization that allows inexact compu-
tations to be reused via memoized computations that are (recurs-
features allow writing self-adjusting programs but these require
syntactically separating stable and changeable data, as well as code
that operates on such data [Acar et al. 2006, 2009; Levy-Wild et al
2008; Hammer et al. 2009]. DITTO [Shankar and Bodik 2007]
shows the benefits of eliminating user annotations. By customiz-
ing dependency tracking for invariant checking programs, DITTO
provides a fully automatic incremental invariant checker. The ap-
proach, however, is domain-specific and only works for certain pro-
gramming [e.g., functions cannot return arbitrary values]: it is unsound
in general.

Information flow and constraint-based type inference. A num-
ber of information flow type systems have been developed to check
security properties, including the SLam calculus [Heintze and
Riecke 1998], JFlow [Myers 1999] and a monadic system [Crary
et al. 2005]. Our type system uses many ideas from Pottier and
Simonet [2003], including a form of constraint-based type inference
[Odersky et al. 1999], and is also broadly similar to other
systems that use subtyping constraints [Simonet 2003; Foster et al
2006].

Cost semantics. To prove that our translation yields efficient self-
adjusting target programs, we use a simple cost semantics. The idea
of instrumenting evaluations with cost information goes back to the
early ’90s [Sands 1990]. Cost semantics is particularly important in
lazy [Sands 1990; Sansom and Peyton Jones 1995] and parallel
languages [Spothower et al. 2008] where it is especially difficult
to relate execution time to the source code, as well as in self-
adjusting computation [Lev-Wild et al. 2009].

8. Conclusion
This paper presents techniques for translating purely functional
programs to programs that can automatically self-adjust in re-
sponse to dynamic changes to their data. Our contributions in-
clude a constraint-based type system for inferring self-adjusting-
computation types from purely functional programs, a type-directed
translation algorithm that rewrites purely functional programs into
self-adjusting programs, and proofs of critical properties of the
translation: type soundness and observational equivalence, as well as
the intrinsic property of time complexity. Perhaps unsurprisingly,
the theorems and their proofs were critical to the determination of the type systems and the translation algorithm; many of our initial attempts at the problem resulted in target programs that were not type sound, that did not ensure observational equivalence, or were asymptotically slower than the source.

These results take an important step towards the development of languages and compilers that can generate code that can respond automatically to dynamically changing data correctly and asymptotically optimally, without substantial programming effort. Remaining open problems include generalization to imperative programs with references, techniques and proofs to determine or improve the asymptotic complexity of dynamic responses, and a complete and careful implementation and its evaluation.

Acknowledgments

We thank the anonymous ICFP reviewers, as well as Arthur Charguéraud, for their useful comments on the submitted version of this paper.

References


Appendix to Chen et al., Implicit self-adjusting computation for purely functional programs (ICFP 2011)

In Section A we show that translation maps source types to corresponding target types. We further prove, in Section B that translated programs evaluate to the same (corresponding) values as source programs. Finally, we show in Section C that translated programs take (at worst) a constant factor longer than source programs.

A. Translation Type Soundness

Lemma A.1 (Translation of Outer Levels).

\[\phi \vdash \text{O.C.} \iff \|\tau\|_\phi = \|\tau\|_\phi^C\mod;\]

\[\phi \vdash \text{O.S.} \iff \|\tau\|_\phi = \|\tau\|_\phi^C.\]

Proof. Case analysis on \(\phi\), using the definitions of – O.S., – O.C., \(\|\_\|_\phi\) and \(\|\_\|_\phi^C\).

Lemma A.2 (Substitution). Suppose \(\phi\) is a satisfying assignment for \(C\), and \(\phi(\vec{a}) = \vec{\delta}\), where \(\vec{\alpha} \subseteq \text{FV}(C)\).

1. If \(D\) derives \(C; \Gamma \vdash e : \tau\), then there exists \(D'\) deriving \(C; [\vec{\delta}/\vec{\alpha}]\Gamma \vdash e : [\vec{\delta}/\vec{\alpha}]\tau\), where \(D'\) has the same height as \(D\).
2. If \(C \vdash \delta' \triangleleft \tau\), then \(C \vdash [\vec{\delta}/\vec{\alpha}]\delta' \triangleleft [\vec{\delta}/\vec{\alpha}]\tau\).
3. If \(C \vdash \tau' \triangleleft \tau''\), then \(C \vdash [\vec{\delta}/\vec{\alpha}]\tau' \triangleleft [\vec{\delta}/\vec{\alpha}]\tau''\).
4. If \(C \vdash \tau' \equiv \tau''\), then \(C \vdash [\vec{\delta}/\vec{\alpha}]\tau' \equiv [\vec{\delta}/\vec{\alpha}]\tau''\).

Proof. By induction on the given derivation.

Lemma A.3. Given \(\tau' \triangleleft \tau''\) and \(\tau' \equiv \tau''\):

1. If \(\tau''\) O.S. then \(\tau' = \tau''\).
2. If \(\tau''\) O.C. then either \(\tau' = \tau''\) or \(\tau' = \lfloor |\tau''|\rfloor\).

Proof. By induction on the derivation of \(\tau' \triangleleft \tau''\).

- Case (subInt): \(\tau' = \text{int}^{\delta'}\) and \(\tau'' = \text{int}^{\delta''}\), where \(\delta' \leq \delta''\).
  1. If \(\tau''\) O.S. then \(\delta'' = \emptyset\). So \(\tau' = \tau''\).
  2. If \(\tau''\) O.C. then \(\delta'' = \mathbb{S}\) then \(\lfloor |\tau''|\rfloor = \text{int}^{\delta'} = \text{int}^{\delta''} = \tau'\); if \(\delta' = \mathbb{C}\) then \(\tau'' = \text{int}^{\delta} = \text{int}^{\delta''} = \tau'\).
- Case (subPred):
  1. By definition of \(\delta\), \(\tau' = \tau''\).
  2. \(\tau''\) O.C. is impossible.
- Case (subSum):
  1. If \(\tau''\) O.S. then \(\tau'' = \text{int}^{\delta}'\). By inversion on (subSum), \(\tau' = \text{int}^{\delta} = \text{int}^{\delta} = \tau'\). Therefore \(\tau' = \tau''\).
  2. If \(\tau''\) O.C. then \(\tau'' = \text{int}^{\delta} = \text{int}^{\delta} = \tau'\). By inversion on (subSum), \(\tau' = \text{int}^{\delta} = \text{int}^{\delta} = \tau'\). By definition of \(\delta\), \(\tau' = \tau''\).

- Case (subArrow): Similar to the (subSum) case.

Theorem A.1 (Translation Type Soundness). If

\[(a)\ C; \Gamma \vdash e : \tau\] and \(\phi\) is a satisfying assignment for \(C\) then

\[(1)\ \text{there exists } \bar{e}^\phi \text{ such that } [\phi]\Gamma \vdash e : [\phi]\tau \iff \bar{e}^\phi\] and \([\Gamma][\bar{e}^\phi] : [\tau]_\phi\], and if \(e\) is a value, then \(\bar{e}^\phi\) is a value;

\[(2)\ \text{there exists } \bar{e}^\phi \text{ such that } [\phi]\Gamma \vdash e : [\phi]\tau \iff \bar{e}^\phi\] and \([\Gamma][\bar{e}^\phi] : [\tau]_\phi^C\].

Proof. By induction on the height of the derivation of \(C; \Gamma \vdash e : \tau\).

We present the proof in a line-by-line style, with the justification for each step on the right. Since we need to show that four different judgments are derivable (translation in the \(\mathbb{S}\) mode, typing in the \(\mathbb{S}\) mode, translation in the \(\mathbb{C}\) mode, and typing in the \(\mathbb{C}\) mode), and often arrive at some of them early, we indicate them with ⋆.*
Appendix to Chen et al., ICFP 2011

Proof of Theorem 6.1

Case \( \frac{\text{SInt}}{C; \Gamma \vdash e \ n : \text{int}^\top} \)

Part (1): Let \( e^\delta \) be \( n \).
\[ [\emptyset] \Gamma \vdash n : \text{int}^\top \rightarrow \text{int}^\top \]  
By (Int)
\[ [\emptyset] \Gamma \vdash e : [\emptyset]([\phi]^{\text{int}^\delta} \rightarrow \text{int}^\delta) \text{ and } e^\delta \text{ is a value.} \]
By \( n = e \) and defn. of substitution
\[ \vdash [\text{int}^\top]_\phi \vdash n : \text{int} \quad \text{By (TInt)} \]
\[ \vdash [\text{int}^\delta]_\phi \vdash e^\delta : [\text{int}^\delta]_\phi \quad \text{By int} = [\text{int}^\delta]_\phi = [\emptyset]([\phi]^{\text{int}^\delta} = [\text{int}^\delta]_\phi \text{ and } n = e^\delta \]
By \( \tau = \text{int}^\delta \)

Part (2): Let \( e^C \) be let \( r = n \) in \( \text{write}(r) \).
\[ [\emptyset] \Gamma \vdash n : \text{int}^\top \rightarrow \text{int}^\top \]  
By (TInt)
\[ [\emptyset] \Gamma \vdash e : [\emptyset]([\phi]^{\text{int}^C} \rightarrow \text{int}^C) \quad \text{By } n = e \text{ and defn. of substitution and } e^C \]
\[ \vdash [\text{int}^\top]_\phi \vdash n : \text{int} \]  
By (TVar)
\[ \vdash [\text{int}^\delta]_\phi \vdash r : \text{int} \quad \text{By (TWrite)} \]
\[ \vdash [\text{int}^\delta]_\phi \vdash e^C : \text{int} \quad \text{By defn. of } e^C \]
\[ \vdash [\text{int}^\delta]_\phi \vdash \text{write}(r) : \text{int} \quad \text{By (TLet)} \]
\[ \vdash [\text{int}^\delta]_\phi \vdash e^C : [\text{int}^\delta]_\phi \quad \text{By int} = [\text{int}^\delta]_\phi \]
\[ \vdash [\text{int}^\delta]_\phi \vdash \text{write}(r) : \text{int} \quad \text{By defn. of } \text{write}(r) \]

Case \( \frac{\text{SVar}}{\Gamma(x) = \forall \alpha[D]. \tau_0 \quad C \vdash \exists \beta. [\beta/\alpha]D} \)

Part (1): Let \( e^\delta \) be \( x[\alpha = \delta] \).
\[ \Gamma(x) = \forall \alpha[D]. \tau_0 \]
By Premise
\[ [\emptyset] \Gamma \vdash x : [\emptyset]([\forall \alpha[D]. \tau_0] = \forall \alpha[[\emptyset] D]. [\emptyset] \tau_0] \quad \text{By defn. of substitution} \]
\[ [\emptyset] \Gamma \vdash x : [\emptyset][\beta/\alpha][\phi]\tau_0 \rightarrow [\emptyset][\beta/\alpha][\phi]\tau_0 \quad \text{By (Var)} \]
\[ [\emptyset] \Gamma \vdash x : [\emptyset][\beta/\alpha][\phi]\tau_0 \rightarrow [\emptyset][\beta/\alpha][\phi]\tau_0 \quad \text{By defn. of } e^\delta \]
\[ [\emptyset] \Gamma \vdash x : [\emptyset][\beta/\alpha][\phi]\tau_0 \rightarrow [\emptyset][\beta/\alpha][\phi]\tau_0 \quad \text{Intermediate subst.} \]
\[ [\emptyset] \Gamma \vdash e : [\emptyset][\delta/\beta][\phi]\tau_0 \rightarrow [\emptyset][\delta/\beta][\phi]\tau_0 \quad \text{Intermediate subst.} \]
\[ [\emptyset] \Gamma \vdash e : [\emptyset][\delta/\beta][\phi]\tau_0 \rightarrow [\emptyset][\delta/\beta][\phi]\tau_0 \quad \text{By } e = x \text{ and } \tau = [\beta/\alpha]\tau_0 \text{ and } e^\delta = x[\alpha = \delta] \]

Part (2), subcase (a) where \( [\emptyset] \tau \ O.S.: \text{ Let } e^C \text{ be let } r = x[\alpha = \delta] \text{ in write}(r) \).
\[ [\emptyset] \Gamma \vdash x : [\emptyset][\beta/\alpha][\phi]\tau_0 \rightarrow [\emptyset][\beta/\alpha][\phi]\tau_0 \quad \text{Above} \]
\[ [\emptyset] \Gamma \vdash e : [\emptyset][\delta/\beta][\phi]\tau_0 \rightarrow [\emptyset][\delta/\beta][\phi]\tau_0 \quad \text{By } e = x \text{ and defn. of } e^\delta \]

Part (2), subcase (b) where \( [\emptyset] \tau \ O.C.: \text{ Let } e^C = \text{ let } r = e^\delta \text{ in read } r \text{ as } r' \text{ in write}(r') \).
[\phi] \Gamma \vdash x : [\phi] \tau \quad \overset{\text{\text{Case}}}{{\vdash}} \quad \text{O.C.}

[\phi] \Gamma \vdash x : [\phi] \tau \quad \overset{\text{\text{Case}}}{{\vdash}} \quad \text{O.C.}

\text{Subcase (b) assumption}

[\phi] \Gamma \vdash x : [\phi] \tau \quad \overset{\text{\text{Case}}}{{\vdash}} \quad \text{O.C.}

\text{Above}

\text{Subcase (b) assumption}

[\phi] \Gamma \vdash x : [\phi] \tau \quad \overset{\text{\text{Case}}}{{\vdash}} \quad \text{O.C.}

\text{By (TVar)}

\text{By (TPVar)}

\text{By (TRead)}

\text{By Lemma [A,1]}

\text{By previous line}

[\phi] \Gamma \vdash x : [\phi] \tau \quad \overset{\text{\text{Case}}}{{\vdash}} \quad \text{O.C.}

\text{By (TLet)}

\text{Part (1), stable mode translation:}

C; \Gamma \vdash e_\ell : \tau_1 \quad \overset{\text{\text{Case}}}{{\vdash}} \quad C; \Gamma \vdash e_\ell : (\tau_1 \times \tau_2) \quad \overset{\text{\text{(SPair)}}}{{\vdash}} \quad \text{Subderivation}

\text{By i.h.}

\text{By (Pair)}

\text{By def. of substitution and } e^\phi = (e_1, e_2)

\text{By (TPair)}

\text{By defn. of } ||-||_\phi

\text{Part (2), changeable mode translation: Let } e^\phi \text{ be let } r = e^\phi \text{ in write}(r).

[\phi] \Gamma \vdash e : [\phi] \tau \quad \overset{\text{\text{Case}}}{{\vdash}} \quad \text{O.S.}

\text{Above}

\text{By definition of O.S.}

\text{Above}

\text{By (TPVar)}

\text{By (TWrite)}

\text{By Lemma [A,1]}

\text{By above equality}

\text{By (TLet)}

\text{Case}

C; \Gamma \vdash e : (\tau_1 \times \tau_2) \quad \overset{\text{\text{Case}}}{{\vdash}} \quad \text{O.S.}

\text{Above}

\text{By definition of O.S.}

\text{Above}

\text{By (TPVar)}

\text{By (TWrite)}

\text{By Lemma [A,1]}

\text{By above equality}

\text{By (TLet)}

\text{Case}

C; \Gamma \vdash f : (\tau_1 \rightarrow \tau_2) \quad \overset{\text{\text{Case}}}{{\vdash}} \quad \text{(SFun)}

(a) Suppose [\phi]e = S.
\[ C; \Gamma, x : \tau_1, f : (\tau_1 \rightarrow \tau_2)^\circ \vdash e' : \tau_2 \quad \text{Subderivation} \]
\[ [\phi](\Gamma, x : \tau_1, f : (\tau_1 \rightarrow \tau_2)^\circ) \vdash e : [\phi]\tau_2 \vdash e' \quad \text{By i.h. and } [\phi]e = \mathbb{S} \]
\[ \vdash \Gamma, x : \tau_1, f : (\tau_1 \rightarrow \tau_2)^\circ \vdash e : [\phi]\tau_2 \vdash e' \quad \text{By defn. of } \vdash \text{and } [\phi]\tau_2 \]

Let \( e^C \) be fun \( f(x) = e'_C \).
\[ (1)\vdash \] [\( e^C \)] \Gamma \vdash e : [\phi]\tau \vdash e^C \quad \text{and } e^C \text{ is a value} \]
\[ \vdash \Gamma, x : \tau_1, f : \tau_1 \vdash e : [\phi]\tau_2 \vdash e' \quad \text{By defn. of } \vdash \text{and } [\phi]\tau_2 \]

(2) Suppose \( [\phi]e = C \).
\[ \vdash \Gamma, x : \tau_1, f : (\tau_1 \rightarrow \tau_2)^\circ \vdash e : [\phi]\tau_2 \vdash e'_C \quad \text{By i.h. and } [\phi]e = \mathbb{S} \]
\[ \vdash \Gamma, x : \tau_1, f : (\tau_1 \rightarrow \tau_2)^\circ \vdash e : [\phi]\tau_2 \vdash e'_C \quad \text{By defn. of } \vdash \text{and } [\phi]\tau_2 \]

Let \( e^C \) be fun \( f(x) = e'_C \).
\[ (1)\vdash \] [\( e^C \)] \Gamma \vdash e : [\phi]\tau \vdash e^C \quad \text{and } e^C \text{ is a value} \]
\[ \vdash \Gamma, x : \tau_1, f : \tau_1 \vdash e : [\phi]\tau_2 \vdash e' \quad \text{By defn. of } \vdash \text{and } [\phi]\tau_2 \]

(2) \[ \vdash \Gamma, x : \tau_1, f : \tau_1 \vdash e : [\phi]\tau_2 \vdash e' \quad \text{let } r = e^C \text{ in write}(r) \]

Analogous to (a)

\[ \begin{array}{c}
\text{Case 1: } ( \times ) \quad C; \Gamma, x : (\tau_1 \times \tau_2)^\circ \\
\text{Part (1): } C; \Gamma, x : \tau_1 \vdash \text{Subderivation} \\
\text{Part (2): Similar to (SPair), using } (\tau_1 + \tau_2)^\circ \text{ O.S.} \\
\end{array} \]

\[ \begin{array}{c}
\text{Case 2: } (\text{SSt}) \\
\text{Part (1): } C; \Gamma, x : (\tau_1 \times \tau_2)^\circ \\
\text{Part (2): Similar to (SVar):} \\
\end{array} \]

Suppose \( [\phi]\delta = \mathbb{S} \).

Part (1): \[ C; \Gamma, x : (\tau_1 \times \tau_2)^\circ \vdash x : [\phi][\delta] \quad \text{by } \vdash \text{and } [\phi][\delta] \]
\[ \vdash \Gamma, x : \tau_1, f : \tau_1 \vdash x : [\phi][\delta] \quad \text{By i.h.} \]
\[ \vdash \Gamma, x : \tau_1, f : \tau_1 \vdash \text{fst } z : \tau_1 \quad \text{By (Fst)} \]

Let \( e^C = \text{fst } z \\
\[ \vdash \Gamma, x : \tau_1, f : \tau_1 \vdash \text{fst } z : [\phi][\delta] \quad \text{By (TFst)} \]

Part (2): Similar to (SVar):

- If \( \tau_1 \text{ O.S.}, \text{ let } e^C \text{ be let } r = \text{fst } z \text{ in write}(r) \text{ and apply rule (Write).} \\
- If \( \tau_1 \text{ O.C.}, \text{ let } e^C \text{ be let } r = \text{fst } z \text{ in read } r \text{ as } r' \text{ in write}(r') \text{ and apply rule (ReadWrite).} \]
• Suppose $[\phi] \delta = C$. We have the premise $C \vdash \delta \leq \varepsilon$, so $[\phi] \varepsilon = C$; we only need to show part (2).

Part (2):

- If $\tau_1$ O.S., let $e_C^C$ be read $\varpi$ as $x'$ in let $r = \text{fst } x'$ in $\text{write}(r)$ and apply rule (Read) with $(\text{LWrite})$.

\[
\begin{align*}
\tau_1 \varpi & \vdash r : \tau_1, \\
\tau_1 \varpi & \vdash e_C^C \text{ write}(r) : \tau_1 \vdash \tau_1 \vdash C \vdash \text{write}(r) : \tau_1 \downarrow \downarrow C & \text{By (TPVar)} \\
\tau_1 \varpi & \vdash \text{fst } x' : \tau_1 & \text{By (TVar)} \\
\tau_1 \varpi & \vdash x' : \tau_1 \times \tau_1, \\
\tau_1 \varpi & \vdash \text{let } r = \text{fst } x' \text{ in write}(r) : \tau_1 \downarrow \downarrow C & \text{By (TLet)} \\
\tau_1 \varpi & \vdash \text{let } r = \text{fst } x' \text{ in write}(r) : \tau_1 \downarrow \downarrow C & \text{By (TVar) then (TWrite)} \\
\tau_1 \varpi & \vdash \text{let } r = \text{fst } x' \text{ in write}(r) : \tau_1 \downarrow \downarrow C & \text{By (TRead)}
\end{align*}
\]

- If $\tau_1$ O.C., then $[\tau_1] = \tau' \mod$ for some $\tau'_\varepsilon$.

Let $e_C^C$ be read $\varpi$ as $x'$ in let $r = \text{fst } x'$ in $\text{read r as } x'$ in $\text{write}(r')$ and apply rule $(\text{Read})$ with $(\text{LWrite})$.

\[
\begin{align*}
\tau_1 \varpi & \vdash e_C^C \text{ write}(r') : \tau'_\varepsilon, \\
\tau_1 \varpi & \vdash e_C^C \text{ write}(r') : \tau_1 \downarrow \downarrow C, \\
\tau_1 \varpi & \vdash e_C^C \text{ write}(r') : \tau_1 \downarrow \downarrow C & \text{By (TPVar) then (TWrite)} \\
\tau_1 \varpi & \vdash e_C^C \text{ write}(r') : \tau_1 \downarrow \downarrow C & \text{By (TVar) then (TWrite)} \\
\tau_1 \varpi & \vdash e_C^C \text{ read as } x' \text{ in let } r = \text{fst } x' \text{ in write}(r) : \tau_1 \downarrow \downarrow C & \text{By (TRead)}
\end{align*}
\]

The remaining steps are similar to the $\tau_1$ O.S. subcase immediately above.

\[
\begin{array}{c}
C; \Gamma \vdash e_1 : \tau' \quad C; \Gamma, x : \tau'' \vdash e_2 : \tau \\
\Delta \vdash \tau' < \tau'' & C \vdash \tau' \vdash \tau'' & C \vdash \tau' \vdash \tau'' \\
\hline
C; \Gamma \vdash e_1 \in \text{let } x = e_2 : \tau & (\text{SLetE})
\end{array}
\]

(a) Subcase for $[\phi] \tau''$ O.C.

\[
\begin{align*}
C; \Gamma \vdash e_1 : \tau' & \quad C; \Gamma \vdash e_1 : [\phi] \tau' \vdash e_C^C & \text{Subderivation} \\
C \vdash \tau' < \tau'' & \quad [\phi] \tau' < [\phi] \tau'' & \text{By i.h.} \\
C \vdash \tau' \equiv \tau'' & \quad [\phi] \tau'' \equiv [\phi] \tau'' \quad & \text{By Lemma A.2} \\
C \vdash \tau'' \quad & \quad [\phi] \tau'' \quad \text{O.C.} & \text{Subcase (a) assumption} \\
[\phi] \tau' = [\phi] \tau'' & \quad [\phi] \tau'' = [\phi] \tau'' & \text{By Lemma A.2} \\
\end{align*}
\]

If the former, then:

\[
[\phi] \Gamma \vdash e_1 : [\phi] \tau' \vdash e_C^C \quad \text{By (Mod)}
\]

If the latter, then:

\[
[\phi] \Gamma \vdash e_1 : [\phi] \tau'' \vdash e_C^C \quad \text{By (Lift)}
\]

Now we have the same judgment no matter which equation Lemma A.3 gave us.

\[
\begin{align*}
\vdash \Gamma \vdash e_C^C : \tau'' \vdash e_C^C : \tau'' \vdash e_C^C & \text{By def of } [\phi] \tau'' \vdash e_C^C : \tau'' \vdash e_C^C \\
\vdash \Gamma \vdash e_C^C \mod e_C^C : \tau'' \vdash e_C^C \mod e_C^C \vdash e_C^C & \text{By (TMod)} \\
\vdash \Gamma \vdash e_C^C \mod e_C^C : \tau'' \vdash e_C^C \mod e_C^C \vdash e_C^C & \text{By def of } [\phi] \tau'' \vdash e_C^C : \tau'' \vdash e_C^C \\
\vdash \Gamma \vdash e_C^C \mod e_C^C : \tau'' \vdash e_C^C \mod e_C^C & \text{Subcase (a) assumption} \\
\vdash \Gamma \vdash e_C^C \mod e_C^C : \tau'' \vdash e_C^C \mod e_C^C & \text{Subcase (a) assumption} \\
\vdash \Gamma \vdash e_C^C \mod e_C^C : \tau'' \vdash e_C^C \mod e_C^C & \text{By Lemma A.1} \\
\vdash \Gamma \vdash e_C^C \mod e_C^C : \tau'' \vdash e_C^C \mod e_C^C & \text{By above equation}
\end{align*}
\]

(b) Subcase for $[\phi] \tau''$ O.S.

\[
\begin{align*}
C; \Gamma \vdash e_1 : \tau' & \quad C; \Gamma \vdash e_1 : [\phi] \tau' \vdash e_C^C & \text{By i.h.} \\
C \vdash e_C^C : \tau'' & \quad [\phi] \tau'' \text{ O.S.} & \text{Subcase (b) assumption} \\
C \vdash e_C^C : \tau'' & \quad [\phi] \tau'' = [\phi] \tau' & \text{By Lemma A.3(1)} \\
C \vdash e_C^C : \tau'' & \quad [\phi] \tau'' = [\phi] \tau' & \text{By above equation}
\end{align*}
\]
Appendix to Chen et al., ICFP 2011

Proof of Theorem 6.1

For both subcases, we have:

\[ C; \Gamma, x : \tau'' \vdash e_2 : \tau \]
\[ [\phi] \Gamma, x : [\phi] \tau'' \vdash e_2 : [\phi] \tau \supset e_2^\phi \]
\[ \vdash \parallel \Gamma \parallel_\phi, x : \parallel \tau'' \parallel_\phi \vdash e_2^\phi : \parallel \tau \parallel_\phi \]

- Subderivation
- By i.h. and defn. of substitution
- By i.h. and defn. of \( \parallel - \parallel_\phi \)

\[(1)\text{w}\]
\[ [\phi] \Gamma \vdash e : [\phi] \tau \quad \text{let} \ x = e_2^\phi \in e_2^\phi \]
By (LetE)

\[(1)\text{w}\]
\[ \vdash \parallel \Gamma \parallel_\phi, x : \parallel \tau'' \parallel_\phi \vdash e_2^\phi : \parallel \tau \parallel_\phi \]
By (TLet)

\[(2)\text{w}\]
\[ [\phi] \Gamma \vdash e : [\phi] \tau \quad \text{let} \ x = e_2^\phi \in e_2^\phi \]
By (LetE)

\[(2)\text{w}\]
\[ \vdash \parallel \Gamma \parallel_\phi, x : \parallel \tau'' \parallel_\phi \vdash e_2^\phi : \parallel \tau \parallel_\phi \]
By (TLet)

\[\begin{array}{c}
C \land D; \Gamma \vdash \forall_v : \tau' \\
\vdash \parallel C \land D \parallel_\phi \vdash \forall_v : \parallel \tau' \parallel_\phi \\
\end{array}\]

- Case

\[ C \land \exists \alpha. D; \Gamma \vdash \forall_v : \tau' \]
\[ C \land \exists \alpha. D; \Gamma \vdash \forall_v : \parallel \tau' \parallel_\phi \]

For all \( \delta_i \) such that \( \delta_i = \delta_i \parallel D \): 

- (a) Suppose \( [\phi] \delta_i / \alpha \tau'' \) O.S., that is, this \( i \)th monomorphic instance is outer-stable, and will not need a mod in the target.

\[ C \land D: \Gamma \vdash \forall_v : \tau' \]
\[ \alpha \cap \text{FV}(C, \Gamma) = \emptyset \]

\[ C \land D: [\delta_i / \alpha] \Gamma \vdash \forall_v : [\delta_i / \alpha] \tau' \]

- Subderivation
- Let \( v_1 \) be \( \forall_v \).

\[ [\phi] \Gamma \vdash \forall_v : [\phi] ([\delta_i / \alpha] \tau') \supset v_1 \]
By i.h., using the lemma’s guarantee about derivation height

\[ \alpha \not\text{ free in } \Gamma \]
Above disjointness

\[ [\phi] \Gamma \vdash \forall_v : [\phi] ([\delta_i / \alpha] \tau') \supset v_1 \]
By above line

\[ \vdash \parallel \Gamma \parallel_\phi, \forall_v : \parallel [\delta_i / \alpha] \tau' \parallel_\phi \]
By i.h. and defn. of substitution

- Premise
- By Lemma A.2

\[ [\phi] \Gamma \vdash \forall_v : [\phi] ([\delta_i / \alpha] \tau') \supset v_1 \]
Above

\[ \alpha \cup \text{dom}(\phi) = \emptyset \]
By \( \alpha \cap \text{FV}(C, \Gamma) = \emptyset \) and appropriateness of \( \phi \) wrt \( C \)

\[ [\phi] \Gamma \vdash \forall_v : [\delta_i / \alpha] ([\phi] \tau'') \supset v_1 \]
By \( [\phi] \tau'' = [\phi] \tau'' \) and \( \varepsilon_i = v_1 \)

\[ \vdash \parallel \Gamma \parallel_\phi, \forall_v : \parallel [\delta_i / \alpha] \tau'' \parallel_\phi \]
Above and \( \varepsilon_i = v_1 \)

\[ [\phi] \Gamma \vdash \forall_v : [\delta_i / \alpha] ([\phi] \tau'') \supset v_1 \]
By \( [\phi] \tau'' = [\phi] \tau'' \)

\[ \vdash \parallel \Gamma \parallel_\phi, \forall_v : \parallel [\delta_i / \alpha] \tau'' \parallel_\phi \]
By \( \alpha \cup \text{dom}(\phi) = \emptyset \)

End of subcase (a)

- (b) Suppose \( [\phi] [\delta_i / \alpha] \tau'' \) O.C., that is, this \( i \)th monomorphic instance is outer-changeable, and therefore needs a mod in the target.
\[ C \land D; \Gamma \vdash \varepsilon \vdash \tau' \]
\[ \bar{\alpha} \cap FV(C, \Gamma) = 0 \]
\[ C \land D; [\bar{\delta}/\bar{\alpha}] \Gamma \vdash \varepsilon \vdash [\bar{\delta}/\bar{\alpha}] \tau' \]
\[ [\phi][\bar{\delta}/\bar{\alpha}] \Gamma \vdash \varepsilon \vdash [\phi][\bar{\delta}/\bar{\alpha}] \tau' \text{ or } [\phi][\bar{\delta}/\bar{\alpha}] \tau' = [\phi][\bar{\delta}/\bar{\alpha}] \tau'' \]
\[ \vdash [\parallel]; [\parallel] \Gamma \vdash \phi \text{ or } \vdash [\parallel] \Gamma \vdash \phi \]
\[ \vdash [\parallel]; [\parallel] \Gamma \vdash \phi \]

If the former, then:
\[ [\phi][\bar{\delta}/\bar{\alpha}] \tau' \vdash e_2 \vdash \tau' \text{ or } [\phi][\bar{\delta}/\bar{\alpha}] \tau' \vdash e_2 \vdash \tau' \]
\[ [\phi][\bar{\delta}/\bar{\alpha}] \tau' \vdash e_2 \vdash \tau' \text{ mod } e_2 \]

By (Lift)

If the latter, then:
\[ [\phi][\bar{\delta}/\bar{\alpha}] \tau'' \vdash e_2 \vdash \tau'' \text{ or } [\phi][\bar{\delta}/\bar{\alpha}] \tau'' \vdash e_2 \vdash \tau'' \]
\[ [\phi][\bar{\delta}/\bar{\alpha}] \tau'' \vdash e_2 \vdash \tau'' \text{ mod } e_2 \]

By (Mod)

Let \( e_2 \) be \( \text{mod } e_2 \).
\[ \vdash [\parallel] \parallel [\parallel] \tau'' \parallel \parallel \parallel \text{mod } e_2 \]
\[ \vdash [\parallel] \parallel [\parallel] \tau'' \parallel \parallel \parallel \text{mod } e_2 \]
\[ \vdash [\parallel] \parallel [\parallel] \tau'' \parallel \parallel \parallel \text{mod } e_2 \]

By (TMod)

\[ \vdash [\parallel] \parallel [\parallel] \tau'' \parallel \parallel \parallel \text{mod } e_2 \]
\[ \vdash [\parallel] \parallel [\parallel] \tau'' \parallel \parallel \parallel \text{mod } e_2 \]
\[ \vdash [\parallel] \parallel [\parallel] \tau'' \parallel \parallel \parallel \text{mod } e_2 \]

By definition of \( \parallel \parallel \parallel \) (shuffling)

Let \( e_2 \) be \( \text{let } x = \text{select } \{ \bar{\delta} \Rightarrow e_1 \} \text{ in } e_2 \), and let \( e_2' \) be \( \text{let } x = \text{select } \{ \bar{\delta} \Rightarrow e_1 \} \text{ in } e_2 \).
\[ \vdash [\parallel] \parallel [\parallel] \tau'' \parallel \parallel \parallel \text{mod } e_2 \]
\[ \vdash [\parallel] \parallel [\parallel] \tau'' \parallel \parallel \parallel \text{mod } e_2 \]
\[ \vdash [\parallel] \parallel [\parallel] \tau'' \parallel \parallel \parallel \text{mod } e_2 \]

By extending \( \Gamma \)

\[ \vdash [\parallel] \parallel [\parallel] \tau'' \parallel \parallel \parallel \text{mod } e_2 \]
\[ \vdash [\parallel] \parallel [\parallel] \tau'' \parallel \parallel \parallel \text{mod } e_2 \]

By (TSelect)

\[ \vdash [\parallel] \parallel [\parallel] \tau'' \parallel \parallel \parallel \text{mod } e_2 \]
\[ \vdash [\parallel] \parallel [\parallel] \tau'' \parallel \parallel \parallel \text{mod } e_2 \]

By (TLet)

\[ \vdash [\parallel] \parallel [\parallel] \tau'' \parallel \parallel \parallel \text{mod } e_2 \]
\[ \vdash [\parallel] \parallel [\parallel] \tau'' \parallel \parallel \parallel \text{mod } e_2 \]

By (TApp)

\[ C; \Gamma \vdash \varepsilon = \varepsilon \]
\[ C; \Gamma \vdash \delta \triangleleft \tau \]
\[ (\text{SApp}) \]

We distinguish four subcases “S-S”, “C-S”, “C-C”, “S-C” according to \( [\phi] \varepsilon' \) and \( [\phi] \delta \) respectively.

- **Subcase “S-S”** for \( [\phi] \varepsilon' = S, [\phi] \delta = S \).
  Part (1):
  \[ C; \Gamma \vdash x_2 : \tau_1 \]
  \[ [\phi] \Gamma \vdash x_2 : [\phi][\bar{\delta}/\bar{\alpha}] \tau_2 \]
  \[ [\parallel]; [\parallel] \Gamma \vdash \tau_1 \]
  \[ C; \Gamma \vdash \varepsilon \] Subderivation

- **Subcase “C-S”** for \( [\phi] \varepsilon' = S, [\phi] \delta = C \).
  Part (2):
  \[ C; \Gamma \vdash x_2 : \tau_1 \]
  \[ [\phi] \Gamma \vdash x_2 : [\phi][\bar{\delta}/\bar{\alpha}] \tau_2 \]
  \[ [\parallel]; [\parallel] \Gamma \vdash \tau_1 \]
  \[ C; \Gamma \vdash \varepsilon \] Subderivation

- **Subcase “C-C”** for \( [\phi] \varepsilon' = C, [\phi] \delta = C \).
  Part (3):
  \[ C; \Gamma \vdash x_2 : \tau_1 \]
  \[ [\phi] \Gamma \vdash x_2 : [\phi][\bar{\delta}/\bar{\alpha}] \tau_2 \]
  \[ [\parallel]; [\parallel] \Gamma \vdash \tau_1 \]
  \[ C; \Gamma \vdash \varepsilon \] Subderivation

- **Subcase “S-C”** for \( [\phi] \varepsilon' = S, [\phi] \delta = C \).
  Part (4):
  \[ C; \Gamma \vdash x_2 : \tau_1 \]
  \[ [\phi] \Gamma \vdash x_2 : [\phi][\bar{\delta}/\bar{\alpha}] \tau_2 \]
  \[ [\parallel]; [\parallel] \Gamma \vdash \tau_1 \]
  \[ C; \Gamma \vdash \varepsilon \] Subderivation
\[ [\phi] \Gamma \vdash \begin{array}{l} x_1 : [\phi] r \rightarrow x_1 \quad \text{By i.h.} \\
|\Gamma|_{\phi} \vdash x_1 : (|\Gamma|_{\phi} \rightarrow r)_{\phi} \\
|\Gamma|_{\phi} \vdash (|(\Gamma \vdash x_1)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi}) \\
|\Gamma|_{\phi} \vdash x_1 : ((|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \end{array} \]

Part (2):

- **Subcase “C-S” where \([\phi]\epsilon = C\) and \([\phi]\delta = S\):**

  **Part (2):**
  \[ [\phi] \Gamma \vdash x_1 : [\phi] r \rightarrow x_1 \quad \text{From subcase S-S above} \]
  \[ [\phi] \Gamma \vdash x_2 : [\phi] r \rightarrow x_2 \quad \text{From subcase S-S above} \]

  Let \( e^C = \text{apply}_C(x_1, x_2) \).

  - By (App)
    \[ [\phi] \Gamma \vdash e : [\phi] r \rightarrow \text{apply}_C(x_1, x_2) \]
    \[ [\Gamma]_{\phi} \vdash x_1 : (|\Gamma|_{\phi} \rightarrow r)_{\phi} \quad \text{By i.h.} \]
    \[ [\Gamma]_{\phi} \vdash x_2 : (|\Gamma|_{\phi} \rightarrow r)_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash (|(\Gamma \vdash x_1)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi}) \\
      \vdash (|(\Gamma \vdash x_2)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi}) \\
      \vdash (|(\Gamma \vdash x_1)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash x_1 : ((|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash x_2 : ((|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash (|(\Gamma \vdash x_1)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash (|(\Gamma \vdash x_2)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash (|(\Gamma \vdash x_1)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash (|(\Gamma \vdash x_2)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash (|(\Gamma \vdash x_1)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash (|(\Gamma \vdash x_2)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash (|(\Gamma \vdash x_1)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash (|(\Gamma \vdash x_2)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash (|(\Gamma \vdash x_1)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash (|(\Gamma \vdash x_2)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash (|(\Gamma \vdash x_1)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash (|(\Gamma \vdash x_2)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \]

  - By (TApp)
    \[ [\Gamma]_{\phi} \vdash x_1 : (|\Gamma|_{\phi} \rightarrow r)_{\phi} \\
      \vdash x_1 : (|\Gamma|_{\phi} \rightarrow r)_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash x_2 : (|\Gamma|_{\phi} \rightarrow r)_{\phi} \\
      \vdash x_2 : (|\Gamma|_{\phi} \rightarrow r)_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash (|(\Gamma \vdash x_1)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash (|(\Gamma \vdash x_2)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash (|(\Gamma \vdash x_1)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash (|(\Gamma \vdash x_2)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash (|(\Gamma \vdash x_1)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash (|(\Gamma \vdash x_2)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash (|(\Gamma \vdash x_1)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash (|(\Gamma \vdash x_2)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash (|(\Gamma \vdash x_1)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \]
    \[ [\Gamma]_{\phi} \vdash (|(\Gamma \vdash x_2)_{\phi} \rightarrow (|\Gamma|_{\phi} \rightarrow r)_{\phi})_{\phi} \]

- **Subcase “C-C” where \([\phi]\epsilon = C\) and \([\phi]\delta = C\):**

  **Part (2):**
Proof of Theorem 6.1

Appendix to Chen et al., ICFP 2011

\[(\Gamma, x' : (\tau_1 \rightarrow \tau_2)) (x') = \forall \delta \exists \phi \delta. true, (\tau_1 \rightarrow \tau_2)\]

By defn. of \(\Gamma\)

\[C ; \Gamma \vdash \exists \delta. true\]

By defn. of \(\vdash\)

\[C ; \Gamma, x' : (\tau_1 \rightarrow \tau_2) \vdash \delta_s x' : (\tau_1 \rightarrow \tau_2)\]

By (SVar)

\[[\phi] \Gamma, x' : ([\phi]_1 \rightarrow [\phi]_2) \vdash x' : ([\phi]_1 \rightarrow [\phi]_2) \rightarrow [\phi]_2\]

By (Var)

\[[\phi] \Gamma, x' : ([\phi]_1 \rightarrow [\phi]_2) \vdash \text{apply}^C(x', x_2) : [\phi]_2 \rightarrow \text{apply}^C(x', x_2)\]

By (App)

\[[\phi] \Gamma, x' : ([\phi]_1 \rightarrow [\phi]_2) \vdash \text{apply}^C(x', x_2) \rightarrow [\phi]_2 \rightarrow \text{apply}^C(x', x_2)\]

By defn. of substitution and \(-\rightarrow^C\)

\[\ldots\]

Part (1):

\[C \vdash \delta \rightarrow \tau\]

Premise

\[[\phi] \tau \Gamma \vdash \text{O.C.}\]

By [\phi]_\delta = C

\[\vdash \text{read} x_1 \rightarrow \text{apply}^C(x', x_2)\]

By (Read)

Let \(e^C\) be \(\text{read} x_1 \rightarrow \text{apply}^C(x', x_2)\)

\[\vdash [\Gamma]_\phi, \delta \vdash \text{read} x_1 \rightarrow \text{apply}^C(x', x_2)\]

By (TPV ar)

\[\vdash [\Gamma]_\phi, \delta \vdash \text{apply}^C(x', x_2) \rightarrow \text{apply}^C(x', x_2)\]

By (TApp)

\[\vdash [\Gamma]_\phi \vdash \text{read} x_1 \rightarrow \text{apply}^C(x', x_2)\]

By (TRead) (**)

Subcase “S-C” where \(\phi\) \(\phi' = S\) and \(\phi\) \(\delta = C\):

Part (2):

\[[\phi] \Gamma, x' : ([\phi]_1 \rightarrow [\phi]_2) \vdash \text{apply}^C(x', x_2) : [\phi]_2 \rightarrow \text{apply}^C(x', x_2)\]

Above and substitute \(x_1\) with \(x'\)

\[[\phi] \Gamma, x' : ([\phi]_1 \rightarrow [\phi]_2) \vdash x' \rightarrow \text{apply}^C(x', x_2) : [\phi]_2 \rightarrow \text{apply}^C(x', x_2)\]

By defn. of \(-\rightarrow^C\) and substitution

\[\vdash [\Gamma]_\phi, \delta \vdash \text{read} x_1 \rightarrow \text{apply}^C(x', x_2)\]

By (I.h.)

Let \(e^C\) = \(\text{read} x_1 \rightarrow \text{apply}^C(x', x_2)\)

\[\vdash [\Gamma]_\phi \vdash \text{read} x_1 \rightarrow \text{apply}^C(x', x_2)\]

By (TRead)

Part (1): Similar to Part (1) of the subcase for \(\Box/C\).

Case

\[C ; \Gamma \vdash x_1 : \text{int}^C\]

\[C ; \Gamma \vdash x_2 : \text{int}^C\]

\[C \vdash \delta_1 = \delta_2 \vdash \text{int} \times \text{int} \rightarrow \text{int}\]

(SPrim)

\[C ; \Gamma \vdash \text{read} (x_1, x_2) : \text{int}^C\]

If \(\phi\) \(\delta_1 = \phi\) \(\delta_2 = S\) then:

\[\ldots\]
As the immediately preceding Part (2), but then using rule (Mo d).

\[
\vdash \Gamma \vdash e : \text{int}^C \quad \text{By (Prim)}
\]

Let \( e^0 = (x_1, x_2) \).

\[
\vdash \Gamma \vdash \text{write}(r) : \text{int} \quad \text{By (Var) then (TWrite)}
\]

Part (2): Similar to (SPair); note that \( \tau \) O.S. holds.

If \( \psi \delta_2 \vdash \psi \delta_2 = C \) then:

Part (2):

\[
\vdash \Gamma, y_1 : \text{int}^C, y_2 : \text{int}^C \vdash (y_1, y_2) : \text{int}^C \quad \text{By (Var), (Var), (Prim)}
\]

\[
\vdash \Gamma, y_1 : \text{int}^C, y_2 : \text{int}^C \vdash (y_1, y_2) : \text{int}^C, \psi \delta_2 = (y_1, y_2) \quad \text{By (Write)}
\]

\[
\vdash \Gamma, y_1 : \text{int}^C, y_2 : \text{int}^C \vdash (\text{read}_{x_2} \text{as } y_2) \text{in let } r = (y_1, y_2) \text{ in write}(r) \quad \text{By (LPrimop2) then (Read)}
\]

Part (1): As the immediately preceding Part (2), but then using rule (Mod).

\[
\text{Case } C; \Gamma \vdash x : (\tau_1 + \tau_2)^C \quad \text{Subderivation}
\]

\[
\vdash \Gamma \vdash \text{case } x \text{ of } \{ x_1 \Rightarrow e_1, x_2 \Rightarrow e_2, \ldots \} : \tau \quad \text{(SCase)}
\]

(a) Suppose \( \psi \delta_1 = \psi \).

\[
\vdash \Gamma \vdash x : (\tau_1 + \tau_2)^C \quad \text{By i.h.}
\]

\[
\vdash \Gamma \vdash \text{case } x \text{ of } \{ x_1 \Rightarrow e_1, x_2 \Rightarrow e_2, \ldots \} : \tau \quad \text{(SCase)}
\]

(b) Suppose \( \psi \delta_1 = \psi \delta_2 = C \).
By induction on the given derivation. All cases are straightforward. Proof. By (LCase)

Above but with \(x'\) in place of the first \(x\)

By defn. of \(\circ\).

\[\begin{align*}
\Gamma, x' : (\Gamma \land \alpha) & \vdash (x'/x)e : [\alpha] \circ e^0 \\
: \Gamma & \vdash \text{case of } \{x_1 \Rightarrow e_1, x_2 \Rightarrow e_2\} \\
\end{align*}\]

Popping out of the quantifier, we have \((\alpha \land \alpha) \vdash e : [\alpha] \circ e^0\) from which \(e : [\alpha] \circ e' : x'\) follows by the definition of substitution (moving the \([\alpha]\) outward).
• **Case (Int):** \(e = n\) and \(e' = n\).

It follows from the definition of \(\tau\), that \(\tau \vdash n : \text{int}\) is the same as \([s]n : \text{int} \vdash [s]n : \text{int}\), which was to be shown.

• **Case (Var):**

\[
\begin{align*}
\Gamma \vdash x : [\alpha \delta] \tau_0 \vdash \alpha x = \delta \\
\vdash [s]x : \forall \alpha[D], \tau_0 & \text{ From } \vdash s : \Gamma \\
\vdash [s]x : \forall \alpha[D], \tau_0 & \text{ From } \vdash s : \|\Gamma\| \\
\vdash [s]x : \Pi \alpha[D], \tau_0 \vdash [\alpha x] = \delta & \text{ From } s : \Gamma \vdash [s]' : \|\Gamma\| \\
\vdash [s]x : \Pi \alpha[D], \tau_0 \vdash [\alpha x] = \delta & \text{ By def. of } \vdash \gamma \\
\vdash [s]x : \Pi \alpha[D], \tau_0 \vdash [\alpha x] = \delta & \text{ By def. of subst.}
\end{align*}
\]

• **Case (Pair):**

\[
\begin{align*}
\Gamma \vdash (v_1, v_2) : (\tau_1 \times \tau_2) & \vdash (v_1', v_2') \text{ Given} \\
\vdash v_1 : \tau_1 & \vdash \tau_1' \vdash v_1' \text{ Subd.} \\
\vdash v_2 : \tau_2 & \vdash \tau_2' \vdash v_2' \text{ By i.h.} \\
\vdash [s]v_1 : \tau_1 \vdash [s]v_1' : \|\tau_1\| & \text{ By def. of } \vdash \gamma \\
\vdash [s]v_2 : \tau_2 \vdash [s]v_2' : \|\tau_2\| & \text{ By i.h.} \\
\vdash [s](v_1, v_2) : (\tau_1 \times \tau_2) & \vdash [s](v_1', v_2') : \|\tau_1\| \times \|\tau_2\| & \text{ By def. of subst. and } \vdash \gamma
\end{align*}
\]

• **Case (Fun):**

\[
\begin{align*}
\Gamma \vdash \text{fun} f(x) = e & : (\tau_1 \rightarrow \tau_2)^{\alpha} \vdash \text{fun}^f f(x) = e^f \text{ is given. Suppose } v : \tau_1 \vdash w : \|\tau_1\|. \\
\vdash s' = s, v/x, (\text{fun} f(x) = e)/f. & \text{ Let } s' = s, w/x, (\text{fun}^f f(x) = e')/f. \\
\text{We show the case for } e = C. \text{ The case for } e = S \text{ is similar, using } |\cdot| \text{ instead of } \|\cdot\|^{-C}. \\
\vdash x : \tau_1, f : (\tau_1 \rightarrow \tau_2)^{\alpha} & \vdash e : \tau_2 \vdash e^f \text{ Subd.} \\
\vdash s' e : \tau_2 & \vdash [s'] e^f : \|\tau_2\|^{-C} & \text{ By i.h.} \\
\vdash \vdash s, v/x, \vdots /f e : \tau_2 \vdash [s, w/x, (\text{fun} f(x) = e')/f] e^f : \|\tau_2\|^{-C} & \text{ By def. of } s' \text{ and } s' e^f \\
\vdash \vdash s, v/x, \vdots /f e : \tau_2 \vdash [s, w/x, (\text{fun} f(x) = e')/f] e^f : \|\tau_2\|^{-C} & \text{ By def. of subst.} \\
\text{By definition of } \vdash \gamma, \text{ for } \text{fun}, \text{ we have } \text{fun} f(x) = e : (\tau_1 \rightarrow \tau_2)^{\alpha} \vdash (\text{fun}^f f(x) = e^f) : \|\tau_1\| \rightarrow \|\tau_2\|^{-C}.
\end{align*}
\]

• **Case (Sum):**

\[
\begin{align*}
\Gamma \vdash \text{inl} v : (\tau_1 + \tau_2)^{\alpha} & \vdash \text{inl}^f v \text{ Given} \\
\vdash v : \tau_1 & \vdash \tau_1' \vdash v' \text{ Subd.} \\
\vdash \text{inl} ([s]v) : (\tau_1 + \tau_2) & \vdash \text{inl} ([s]v') : \|\tau_1\| + \|\tau_2\| & \text{ By i.h.} \\
\vdash \text{inl} ([s]v) : (\tau_1 + \tau_2) & \vdash \text{inl} ([s]v') : \|\tau_1\| + \|\tau_2\| & \text{ By def. of } \vdash \gamma \\
\text{By def. of subst. and } \vdash \gamma.
\end{align*}
\]

• **Case (Fst):**

\[
\begin{align*}
\Gamma \vdash \text{fst} x : \tau & \vdash \tau_1 \vdash \tau_1' \vdash \text{fst} \text{ Given} \\
\vdash x : (\tau \times \tau_2)^{\alpha} & \vdash \tau \vdash \tau_2 \vdash \tau_2' \vdash x \text{ Subd.} \\
\vdash [s]x : (\tau \times \tau_2)^{\alpha} & \vdash [s]x : \|\tau \times \tau_2\| \text{ By i.h.} \\
\vdash [s]x : (\tau \times \tau_2)^{\alpha} & \vdash [s]x : \|\tau \times \tau_2\| \text{ By def. of } \vdash \gamma \\
\vdash \text{fst} [s]x : \tau & \vdash \text{fst} [s]x : \|\tau\| \text{ By def. of } \vdash \gamma \\
\text{By def. of subst.}
\end{align*}
\]

• **Case (Prim):**

\[
\begin{align*}
\Gamma \vdash ((x_1, x_2) : \tau & \vdash ((x_1, x_2) \vdash \text{Given} \\
\vdash x_1 : \tau & \vdash \tau_1 \vdash \tau_1' \vdash x \text{ Subd.} \\
\vdash [s]x_1 : \tau & \vdash \tau_1 \vdash \tau_1' \vdash x \text{ By i.h.} \\
\vdash [s]x_2 : \tau & \vdash \tau_2 \vdash \tau_2' \vdash x \text{ By similar reasoning for } x_2 \\
\vdash (\text{inl}[s]x, [s]x_2) : \tau & \vdash \text{inl}[s]x, [s]x_2) : \|\tau\| \text{ By def. of } \vdash \gamma \\
\text{By def. of subst.}
\end{align*}
\]

Appendix to Chen et al., ICFP 2011

Proof of Lemma[6.3]
• **Case (App):** \( e = \text{apply}^c(x_1, x_2) \).

Let \(|-|^c\) be \(|-|\) when \( e = S \), and \(|-|^{\text{in}C}\) when \( e = C \).

\[ \Gamma \vdash \text{apply}(x_1, x_2) : \tau_2 \xrightarrow{c} \text{apply}^c(x_1, x_2) \]  

Given

\[ \Gamma \vdash x_1 : (\tau_1 \xrightarrow{c} \tau_2)^c \xrightarrow{c} x_1 \]  

Subd.

\[ [\cdot]x_1: (\tau_1 \xrightarrow{c} \tau_2)^c \equiv [\cdot][\cdot] : \| (\tau_1 \xrightarrow{c} \tau_2)^c \| \]  

By i.h.

\[ [\cdot]x_1: (\tau_1 \xrightarrow{c} \tau_2)^c \equiv [\cdot][\cdot] : \| \tau_2 \|^c \]  

By def. of \(|-|\)

\[ \Gamma \vdash x_2 : \tau_1 \xrightarrow{c} x_2 \]  

Subd.

\[ [\cdot]x_2 : \tau_1 \xrightarrow{c} x_2 \]  

By i.h.

\[ \text{apply}([\cdot]x_1, [\cdot]x_2) : \tau_2 \equiv \text{apply}^c([\cdot]x_1, [\cdot]x_2) : \| \tau_2 \|^c \]  

By def. of \( \equiv \)

\[ \Rightarrow [\cdot]\text{apply}(x_1, x_2) : \tau_2 \equiv [\cdot]\text{apply}^c(x_1, x_2) : \| \tau_2 \|^c \]  

By def. of subst.

• **Case (Case):**

\[ \Gamma \vdash \text{case} x \text{ of } \{ x_1 \Rightarrow e_1, x_2 \Rightarrow e_2 \} : \tau \xrightarrow{c} \text{case} x \text{ of } \{ x_1 \Rightarrow e'_1, x_2 \Rightarrow e'_2 \} \]  

Given

\[ \Gamma \vdash x : (\tau_1 + \tau_2)^c \xrightarrow{c} \| \]  

Subd.

\[ x : (\tau_1 + \tau_2)^c \equiv \| \tau'_1 + \tau'_2 \]  

By i.h. and def. of \(|-|\)

For \( k \in \{1, 2\} \):

For all \( v : \tau_k \equiv w : \tau'_k \):

Let \( s' = s, v/x_k \) and \( s'' = s, w/x_k \).

\[ \Gamma, x_k : \tau_k \vdash e_k : \tau \xrightarrow{c} e'_k \]  

Subd.

\[ [\cdot]'s'e_k : \tau \equiv [\cdot]'s''e'_k : \tau' \]  

By i.h.

\[ [\cdot]'s'v/x_k'e_k : \tau \equiv [\cdot]'s'w/x_k'e'_k : \tau' \]  

By def. of \( s' \) and \( s'' \)

\[ [\cdot]'v/x_k'[\cdot]'s'v/x_k'e_k : \tau \equiv [\cdot]'v/x_k'[\cdot]'s''w/x_k'e'_k : \tau' \]  

By def. of subst. (\( x_k \) fresh)

Therefore \( \text{case} x \text{ of } \{ x_1 \Rightarrow [\cdot]'s'e_1, x_2 \Rightarrow [\cdot]'s''e_2 \} : \tau \equiv \text{case} x \text{ of } \{ x_1 \Rightarrow [\cdot]'s'e'_1, x_2 \Rightarrow [\cdot]'s''e'_2 \} : \tau' \).

The result follows by pushing \([\cdot]'s\) and \([\cdot]'s''\) to the outside.

• **Case (Mod):**

\[ \Gamma \vdash e : \tau \xrightarrow{c} e'^c \mod \]  

Given

\[ \Rightarrow \]  

\[ \Gamma \vdash e : \tau \xrightarrow{c} e'^c \]  

Subd.

\[ [\cdot]'s'e : \tau \equiv [\cdot]'s''e' : \| \tau \|^c \]  

By i.h.

\[ [\cdot]'s'e \equiv [\cdot]'s''e' : \| \tau \|^c \mod \]  

By def. of \( \equiv \)

\[ [\cdot]'s'e \equiv [\cdot]'s''e' : \| \tau \|^c \mod \]  

By def. of subst.

\[ \tau \text{ O.C.} \]  

Premise

\[ \| \tau \|^c \mod = \| \tau \| \]  

By Lemma(1)

\[ \Rightarrow [\cdot]'s'e \equiv [\cdot]'s''e' : \| \tau \|^c \mod \]  

By preceding equation

• **Case (Lift):**

\[ \Gamma \vdash e : \tau \xrightarrow{c} e'^c \mod \]  

Given

\[ \Rightarrow \]  

\[ \Gamma \vdash e : \| \tau \|^c \xrightarrow{c} e'^c \]  

Subd.

\[ [\cdot]'s'e \equiv [\cdot]'s''e' : \| \tau \|^c \]  

By i.h.

\[ [\cdot]'s'e \equiv [\cdot]'s''e' : \| \tau \|^c \mod \]  

By def. of \(|-|\)

\[ [\cdot]'s'e \equiv [\cdot]'s''e' : \| \tau \|^c \mod \]  

By preceding equation

\[ [\cdot]'s'e \equiv [\cdot]'s''e' : \| \tau \|^c \mod \]  

By def. of subst.

\[ \tau \text{ O.C.} \]  

By def. of \(|-|\)

\[ \Rightarrow [\cdot]'s'e \equiv [\cdot]'s''e' : \| \tau \|^c \mod \]  

By preceding equation

• **Case (Let):**

\[ \Gamma \vdash \text{let } x = v_1 \text{ in } e_2 : \tau \xrightarrow{c} \text{let} \ldots \]  

Given

For all \( \delta_i \):

\[ \Gamma \vdash v : (\delta_i / \delta' \gamma) \tau_0 \xrightarrow{c} e'_i \]  

Subd.

\[ [\cdot]'s'v : (\delta_i / \delta' \gamma) \tau_0 \equiv [\cdot]'s''e'_i : \| (\delta_i / \delta' \gamma) \tau_0 \| \]  

By i.h.
The definition of $\vdash$ gives $v : \forall \alpha[D], \tau_0 \vdash (\text{select } \{\delta^i \Rightarrow e^i\}_i) : \Pi \alpha[D], \tau_0$.

For all $v_0, w_0$ such that $v_0 : \forall \alpha[D], \tau_0 \vdash w_0 : \Pi \alpha[D], \tau_0$:

(beg)
\[
\Gamma, x : \forall \alpha[D], \tau_0 \vdash e_2 : \tau \vdash \epsilon_2 \quad \text{Subd.}
\]
\[
[s, v_0/x][e_2] : \tau \vdash [s, w_0/x][e_2] : \tau' \quad \text{By i.h.}
\]
\[
[w_0/x][s][e_2] : \tau \vdash [w_0/x][s][e_2] : \tau' \quad \text{By def. of subst.}
\]

(end)

By the definition of $\vdash$ and the definition of substitution, this gives $[s](\text{let } x = v \text{ in } e_2) : \tau \vdash [s](\text{let } x = \text{select } \{\delta^i \Rightarrow e^i\}_i \text{ in } e_2) : \tau'$.

* Case (Read):

We have a subderivation of $\Gamma \vdash e \vdash (x \Rightarrow x') : \tau_0 \vdash e'$. By inversion on the rules for such judgments, either

- (LApply) $e = \text{apply}(x, x_2)$, or
- (LCase) $e = \text{case } x \text{ of } \{x_1 \Rightarrow e_1, x_2 \Rightarrow e_2\}$, or
- (LPrimop1) $e = \oplus(x, x_2)$ and $e' = \oplus(x', x_2)$, or
- (LPrimop2) $e = \oplus(x_1, x)$ and $e' = \oplus(x_1, x')$.

Assume the first case; the others are similar.

Given: $\Gamma \vdash e : \tau \vdash \text{read } x \text{ as } x' \text{ in } e'$. Let $\tau_1 = [|\tau_0|^\beta]$ and $\tau_1' = [|\tau_1|^\beta]$ be such that $||\tau_0|| = \tau_1'$ (mod (it must be the case that $\tau_0$ has this form because $\tau_0$ O.C.). Suppose $v : \tau_1 \vdash w : \tau_1'$.

\[
\Gamma \vdash x : \tau_0 \vdash x \vdash \tau \vdash \epsilon \quad \text{Subd.}
\]
\[
[s]x : \tau_0 \vdash [s]x : ||\tau_0|| \quad \text{By i.h.}
\]
\[
\Gamma, x' : [|\tau_0|^\beta] \vdash e' : \tau \vdash \epsilon \quad \text{Subd.}
\]
\[
[s, v/x'][\text{apply}(x, x_2)] : \tau \vdash [s, w/x'][e'] : \tau' \quad \text{By i.h.}
\]
\[
[w/x'][s][\text{apply}(x, x_2)] : \tau \vdash [w/x'][s][e'] : \tau' \quad \text{By def. of subst.}
\]

Therefore, by the definition of $\vdash$ when the target expression is a read, we have

\[
[x/x']([s]\text{apply}(x, x_2)) : \tau \vdash [s]x \text{ as } x' \text{ in } [s]e' : \tau'
\]

By def. of subst., $[s][x/x'][\text{apply}(x, x_2)] : \tau \vdash [s][\text{read } x \text{ as } x' \text{ in } e'] : \tau'$.

By def. of subst., $[s][\text{apply}(x, x_2)] : \tau \vdash [s][\text{read } x \text{ as } x' \text{ in } e'] : \tau'$, which was to be shown.

* Case (Write):

\[
\Gamma \vdash e : \tau \vdash \text{let } r = e^6 \text{ in } w : \tau_1 \quad \text{Given}
\]
\[
\Gamma \vdash e : \tau \vdash e^6 \quad \text{Subd.}
\]
\[
[s]e : \tau \vdash [s]e^6 : \tau' \quad \text{By i.h.}
\]

Suppose $v : \tau \vdash w : \tau'$.
\[
[v/r]r : \tau \vdash w : \tau' \quad \text{By def. of subst.}
\]
\[
[w/r][s]r : \tau \vdash w : \tau' \quad \text{By def. of subst. (r fresh)}
\]
\[
[w/r][s]r : \tau \vdash \text{write}(w) : \tau' \quad \text{By def. of $\vdash$}
\]
\[
[v/r][s]r : \tau \vdash \text{write}(w)[r] : \tau' \quad \text{By def. of subst.}
\]
\[
[v/r][s]r : \tau \vdash \text{write}(w)[r][s] : \tau' \quad \text{By def. of subst.}
\]

By definition of $\vdash$, we have $[e/r][s]r : \tau \vdash \text{let } r = [s]e^6 \text{ in } [s](\text{write}(r)) : \tau'$.

By def. of subst., $[s]e : \tau \vdash [s]e \vdash [s][\text{let } r = e^6 \text{ in } \text{write}(r)] : \tau'$, which was to be shown.

* Case (ReadWrite):

Using techniques from the (Write) and (Read) cases.

\[\square\]

**Lemma B.5.** If $e : \tau \vdash e' : \tau'$ then $e$ and $e'$ are closed. (In particular, $e'$ has no free location variables $\ell$.)

**Proof.** Follows from the definition of $\vdash$. \[\square\]

**Lemma B.6.** If $e : \tau \vdash [p_1]e' : \tau'$ and $p_2$ extends $p_1$ then $e : \tau \vdash [p_2]e' : \tau'$.

**Proof.** By Lemma [B.5] $[p_1]e'$ is closed, so $\text{FV}(e') \subseteq \text{dom}(p_1)$. If $p_2$ extends $p_1$ then it agrees on all locations in $p_1$. Therefore $[p_2]e' = [p_1]e'$, so replacing equals with equals gives the result. \[\square\]
Lemma B.7. If \(v_1/x\)\(v_2 \downarrow v\) and \(e_1 \downarrow v_1\) then \(v_1/x\)\(v_2 \downarrow v\).

Proof. By induction on the given derivation.

Theorem 6.4 (Generalized Translation Soundness).
If \(e : \sigma \vdash [\rho]e : \sigma'\) and \(D' : \rho \vdash e' \downarrow (\rho' \vdash w)\) then \(D' : e \downarrow v\) where \(v : \sigma \vdash [\rho]'w : \sigma'\).

Proof. By induction on the derivation of \(\rho \vdash e' \downarrow (\rho' \vdash w).

Case (TEvApply):
\[
\rho \vdash \text{apply}(e_1, e_2) : \tau \\
\rho \vdash e_1 \downarrow (\rho_1 \vdash \text{fun} f(x) = e') \\
\rho_1 \vdash e_2 \downarrow (\rho_2 \vdash w_2) \\
D_3 :: \rho_2 \vdash [\text{fun} f(x) = e'/f][w_2/x]e' \downarrow (\rho' \vdash w)
\]
\[
e = \text{apply}(e_1, e_2) \text{ and } e_1 : (\tau_1 \rightarrow \tau_2)^\delta \vdash [\rho]e_1' : \tau_1 \rightarrow \tau_2' \\
e_1 : (\tau_1 \rightarrow \tau_2)^\delta \vdash [\rho]e_1' : \tau_1 \rightarrow \tau_2' \\
e_1 \downarrow v_1 \text{ and } v_1 : (\tau_1 \rightarrow \tau_2)^\delta \vdash [\rho]([\text{fun} f(x) = e']) : \tau_1 \rightarrow \tau_2' \\
v_1 : (\tau_1 \rightarrow \tau_2)^\delta \vdash [\rho][\text{fun} f(x) = e'] : \tau_1 \rightarrow \tau_2' \\
e_2 : \tau_1 \vdash [\rho]e_2' : \tau_1' \\
e_2 \downarrow v_2 \text{ and } v_2 : \tau_1 \vdash [\rho]w_2 : \tau_2'
\]

Case (TEvPair):
\[
\rho \vdash e' \downarrow (\rho' \vdash e') \\
\rho \vdash (e_1', e_2') \downarrow (\rho' \vdash (w_1, w_2)) \\
\rho \vdash e' \downarrow (\rho' \vdash (w_1, w_2)) \\
\rho \vdash (e_1, e_2) : (\tau_1 \times \tau_2)^\delta \vdash (e_1', e_2') : \tau_1' \times \tau_2' \\
e_1 : \tau_1 \vdash e_1' : \tau_1' \\
e_2 : \tau_2 \vdash e_2' : \tau_2'
\]

Case (TEvMachineValue):
\[
\rho \vdash e' \downarrow (\rho' \vdash e') \\
e : \tau \vdash [\rho]e' : \tau' \\
e \text{ is some value } v \\
v \downarrow v \text{ By def. of source values, machine values, and } \vdash \\
v \downarrow v \text{ By (SEvValue)} \\
e \downarrow v \text{ e = v } \\
\]

Case (TEvPair):
\[
\rho \vdash (e_1', e_2') \downarrow (\rho' \vdash (w_1, w_2)) \\
\rho \vdash (e_1, e_2) : (\tau_1 \times \tau_2)^\delta \vdash (e_1', e_2') : \tau_1' \times \tau_2' \\
e_1 : \tau_1 \vdash e_1' : \tau_1' \\
e_2 : \tau_2 \vdash e_2' : \tau_2'
\]

By lemma B.6
• Case (TEvSum):
  \[ \rho \vdash \text{inl} \; e_0 \Downarrow (\rho' \vdash \text{inl} \; w_0) \]  
  Given

  \[ \text{inl} \; e_0 : \tau \Rightarrow [\rho] (\text{inl} \; e_0) : \tau' \]  
  Given

  \[ \text{inl} \; e_0 : (\tau_1 + \tau_2) \Rightarrow [\rho] (\text{inl} \; e_0) : \tau'_1 + \tau'_2 \]  
  By def. of subst.

  \[ e_0 : \tau_1 \Rightarrow [\rho] e_0 : \tau'_1 \]  
  By def. of \( \Rightarrow \)

  \[ \rho \vdash e_0 \Downarrow (\rho' \vdash w_0) \]  
  Subd.

  \[ e_0 \Downarrow v_0 \]  
  By i.h.

  \[ v_0 : \tau_1 \Rightarrow [\rho'] w_0 : \tau'_1 \]  
  "

  \[ \text{inl} \; e_0 \Downarrow \text{inl} \; v_0 \]  
  By (SEvSum)

  \[ \text{inl} \; v_0 : (\tau_1 + \tau_2) \Rightarrow [\rho'] (\text{inl} \; v_0) : \tau'_1 + \tau'_2 \]  
  By def. of \( \Rightarrow \)

  \[ \text{inl} \; e_0 : \tau \Rightarrow [\rho'] (\text{inl} \; v_0) : \tau' \]  
  By def. of subst. and \( \tau = \ldots \) and \( \tau' = \ldots \)

• Case (TEvPrimop):
  \[ \rho \vdash \oplus (e_1', e_2') \Downarrow (\rho' \vdash w) \]  
  Given

  \[ \begin{array}{l}
  e : \tau \Rightarrow [\rho] (\text{inl} \; e_1, e_2) : \tau' \ \\
  e : \tau \Rightarrow [\rho] (\text{inl} \; e_1, e_2) : \tau' \\
  e = \oplus (e_1, e_2) \text{ and } e_k : \tau_k \Rightarrow e_k' : \tau'_k
  \end{array} \]  
  By def. of subst.

  \[ (\text{for all } k \in \{1, 2\}) \text{ By def. of } \Rightarrow \]

  \[ \rho \vdash e_k' \Downarrow (\rho_k \vdash w_k) \]  
  Subd.

  \[ e_k \Downarrow v_k \text{ and } v_k : \tau_k \Rightarrow w_k : \tau'_k \]  
  (for all \( k \in \{1, 2\} \)) By i.h.

  \[ v_k = w_k \]  
  (for all \( k \in \{1, 2\} \)) By def. of \( \Rightarrow \) at integer type

  \[ \oplus (w_1, w_2) = w \]  
  Premise

  \[ \oplus (v_1, v_2) = w \]  
  (for all \( k \in \{1, 2\} \)) By def. of \( \Rightarrow \) at integer type

  \[ w : \tau \Rightarrow [\rho'] \Downarrow w : \tau' \]  
  By def. of store subst.

• Case (TEvFst):
  \[ \rho \vdash \text{fst} \; e_0 \Downarrow (\rho' \vdash w) \]  
  Given

  \[ \begin{array}{l}
  (\text{fst} \; e_0) : \tau \Rightarrow [\rho] (\text{inl} \; e_0) : \tau' \ \\
  (\text{fst} \; e_0) : \tau \Rightarrow [\rho] (\text{inl} \; e_0) : \tau' \\
  e_0 : \tau \Rightarrow [\rho] e_0 : \tau'
  \end{array} \]  
  By def. of subst.

  \[ \rho \vdash e_0 \Downarrow (\rho' \vdash (w, w_2)) \]  
  Subd.

  \[ e_0 \Downarrow v_{\text{pair}} \]  
  By i.h.

  \[ v_{\text{pair}} : \tau_{\text{pair}} \Rightarrow [\rho'] (w, w_2) : \tau'_1 \times \tau'_2 \]  
  " and def. of \( \Rightarrow \)

  \[ (v, v_2) : (\tau \times \tau_2) \Rightarrow (\rho') (w, w_2) : \tau' 	imes \tau'_2 \]  
  By def. of \( \Rightarrow \)

  \[ (v, v_2) : (\tau \times \tau_2) \Rightarrow (\rho) (w, w_2) : \tau' \times \tau'_2 \]  
  By def. of subst.

  \[ v : \tau \Rightarrow [\rho'] \Downarrow w : \tau' \]  
  By def. of \( \Rightarrow \)

  \[ \text{fst} \; e_0 \Downarrow v \]  
  By (SEvFst)

• Case (TEvLet):
  \[ \rho \vdash \text{let} \; x = e_1 \; \text{in} \; e_2 \Downarrow (\rho' \vdash w) \]  
  Given

  \[ \rho \vdash e_1' \Downarrow (\rho_1 \vdash \text{inl} \; w_1) \]  
  Subd.

  \[ e_1 \Downarrow v_1 \text{ and } v_1 : \tau_1 \Rightarrow \rho_1 [\rho_1] w_1 : \tau'_1 \]  
  By i.h.

  \[ e : \tau \Rightarrow [\rho] \text{let} \; x = e_1 \; \text{in} \; e_2 : \tau' \]  
  Given

  \[ e : \tau \Rightarrow [\rho] \text{let} \; x = e_1 \; \text{in} \; e_2 : \tau' \]  
  By def. of substitution

  By the definition of \( \Rightarrow \) with a target \text{let}, either \( e = \text{(let} \; x = e_1 \; \text{in} \; e_2) \) or \( e = [e_1/x] e_2 \).

  In the former case:

  \[ e = (\text{let} \; x = e_1 \; \text{in} \; e_2) \text{ and } e_1 : \tau_1 \Rightarrow [\rho] e_1 : \tau'_1 \]  
  By def. of \( \Rightarrow \)

  \[ [v_1/x] e_2 : \tau \Rightarrow [\rho] [\rho_1] w_1/x [\rho] e_2 : \tau' \]  
  Subd.

  \[ v : \tau \Rightarrow [\rho'] \Downarrow w : \tau' \]  
  i.h.

  \[ e \Downarrow v \]  
  By (SEvLet)

  In the latter case, also use Lemma B.7.
Proof of Theorem 6.4

Appendix to Chen et al., ICFP 2011

• Case (TEvCaseLeft):

\[ \rho \vdash \text{case } e_0 \text{ of } \{ x_1 \Rightarrow e_1', x_2 \Rightarrow e_2' \} \Downarrow (\rho' \vdash w) \]

Given

\[ \text{case } e_0 \text{ of } \{ x_1 \Rightarrow e_1, x_2 \Rightarrow e_2 \} : \tau \vdash [\rho](\text{case } e_0 \text{ of } \{ x_1 \Rightarrow e_1', x_2 \Rightarrow e_2' \}) : \tau' \]

Given

\[ \rho \vdash e_0 \Downarrow \quad \text{and} \quad u : \tau_0 \vdash [\rho_1](\text{inl } w_1) : \tau'_0 \]

Subd.

\[ [v_1/x_1]e_1 : \tau \vdash [v_1/x_1]e'_1 : \tau' \]

By def. of \( \vdash \)

\[ \rho_1 \vdash [w_1/x]e'_1 \Downarrow (\rho' \vdash w) \]

Subd.

\[ [v_1/x_1]e_1 \Downarrow u \quad \text{and} \quad v : \tau \vdash \rho w : \tau' \]

By i.h.

\[ \text{case } e_0 \text{ of } \{ x_1 \Rightarrow e_1, x_2 \Rightarrow e_2 \} \Downarrow u \]

By (SEvCaseLeft)

• Case (TEvRead):

\[ \rho \vdash \text{read } e'_1 \text{ as } x \text{ in } e'_2 \Downarrow (\rho' \vdash w) \]

Given

\[ e : \tau \vdash \rho[e'_1 \text{ as } x \text{ in } e'_2] : \tau' \]

Given

\[ e = [e_1/x]e_2 \quad \text{and} \quad e_1 : \tau_1 \vdash \rho[e'_1] : \tau'_1 \]

By def. of \( \vdash \)

for all \( v : \tau_1 \vdash \rho w : \tau'_1 \)

we have \([v/x]e_2 : \tau \vdash [v/x]e'_2 : \tau' \]

"Above with \( v = v_1 \) and \( w = w_1 \)

\[ \rho_1 \vdash [\rho_1(x)/x][\rho]e'_2 \Downarrow (\rho' \vdash w) \]

Subd.

\[ [v_1/x]e_2 \Downarrow u \quad \text{and} \quad v : \tau \vdash \rho w : \tau' \]

By i.h.

\[ e_1 \Downarrow v_1 \quad \text{and} \quad v_1 : \tau_1 \vdash [\rho_1]e : \tau'_1 \]

By i.h.

\[ [e_1/x]e_2 \Downarrow u \]

By Lemma 15.7

• Case (TEvWrite):

\[ \mathcal{D} :: \rho \vdash \text{write}(e_0) \Downarrow (\rho' \vdash w) \]

Given

\[ e : \tau \vdash \text{write}(e_0) : \tau' \]

Given

\[ e : \tau \vdash \rho_0 : \tau'_0 \]

By def. of \( \vdash \)

\[ \mathcal{D}_1 :: \rho \vdash e_0 \Downarrow (\rho' \vdash w) \]

Subd.

\[ \mathcal{D}' :: e \Downarrow v \]

By i.h.

\[ v : \tau \vdash \rho w : \tau' \]

"Above with \( \rho = \rho_0, \ell \mapsto w \) and \( \tau = \tau'_0 \)

\[ \rho \vdash \text{mod } e \Downarrow \left( (\rho_0, \ell \mapsto w) \vdash e \right) \]

Given

\[ \rho \vdash e \Downarrow \left( (\rho_0) \vdash w \right) \]

Subd.

\[ e : \tau \vdash \rho(e) : \tau'_0 \]

By def. of \( \vdash \)

\[ e : \tau \vdash \rho(e) : \tau'_0 \]

By def. of \( \vdash \)

\[ e \Downarrow v \quad \text{and} \quad v : \tau \vdash \rho w : \tau'_0 \]

By i.h.

\[ v : \tau \vdash [\rho_0](\text{mod } w) : \tau'_0 \]

By def. of \( \vdash \)

\[ v : \tau \vdash [\rho_0, \ell \mapsto w]e : \tau'_0 \]

By def. of store substitution

\[ v : \tau \vdash [\rho_0]e : \tau'_0 \]

By \( \rho' = \rho_0, \ell \mapsto w \) and \( \tau' = \tau'_0 \)

\[ e : \tau \vdash \rho e : \tau' \]

By i.h.

\[ e \Downarrow v \quad \text{and} \quad v : \tau \vdash \rho w : \tau' \]

"Above with \( \rho = \rho_0, \ell \mapsto w \) and \( \tau = \tau'_0 \)

\[ \rho \vdash \text{select } \{ \ldots, \delta \Rightarrow e_i, \ldots \} \Downarrow (\rho' \vdash w) \]

Given

\[ e : \tau \vdash \rho \left( \text{select } \{ \ldots, \delta \Rightarrow e_i, \ldots \} \right) \Downarrow (\rho' \vdash w) \]

Given

\[ e : \tau \vdash [\rho]\left( \text{select } \{ \ldots, \delta \Rightarrow e_i, \ldots \} \right) \Downarrow (\rho' \vdash w) \]

By def. of subst.

\[ \tau = [\delta/\bar{\delta}]\tau_0 \quad \text{and} \quad \tau' = [\delta/\bar{\delta}]\tau_0 \]

By def. of \( \vdash \)

\[ e : \forall \bar{\delta}[D], \tau_0 \vdash \text{select } \{ \rho[e_i], \ldots \} : \Pi \bar{\delta}[D], \tau_0 \]

"By def. of \( \vdash \)

\[ [\delta/\bar{\delta}]\tau_0 \]

By i.h.

\[ \rho \vdash e_i \Downarrow (\rho' \vdash w) \]

Subd.

\[ e \Downarrow v \quad \text{and} \quad v : \tau \vdash [\rho]w \]

"Above with \( \rho = \rho_0, \ell \mapsto w \) and \( \tau = \tau'_0 \)
Theorem 6.5 (Translation Soundness). If \( \vdash e : \tau \models e' \) and \( \vdash e' \downarrow (\rho' \downarrow w) \), then \( e \downarrow v \) where \( v : \tau \models [\rho']w : \tau' \).

Proof. Let \( \Gamma = \cdot \) and let \( s \) and \( \rho \) be empty substitutions. By Lemma 6.3, \( [s]e : \tau \models [s]e' : \tau' \). Because \( s \) and \( \rho \) are empty, we have \( e : \tau \models e' : \tau' \).

Let \( \rho = \cdot \) (the empty store). By Theorem 6.4, \( e \downarrow v \) and \( v : \tau \models [\rho']w : \tau' \), which was to be shown.

C. Worst-Case Evaluation Time

To extend the result above with a guarantee that the evaluation derivation \( D \) is not too large—within a constant factor of the source evaluation derivation \( D' \)—we need several definitions:

Definition C.1. The weight \( W(D) \) of a derivation \( D \) is the number of rule applications (that is, the number of horizontal lines) in \( D \).

Next, we define the “head cost” of a derivation. This measures the overhead introduced by translation, in the part of the derivation that is near its conclusion (the root of the derivation tree). To measure the overhead, we count the number of “dirty” rules applied near the root.

Definition C.2. The rules (TEvMachineValue), (TEvPair), (TEvSum), (TEvPrimop), (TEvFst), (TEvCase), and (TEvApply) are clean.

The rule (TEvLet) is clean iff it is applied to a \( \text{let} \) generated by (LetE) or (LetV), and dirty otherwise.

The rules (TEvWrite), (TEvMod), (TEvRead) and (TEvSelectE) are dirty.

Definition C.3. The head cost \( HC(D) \) of a derivation \( D \) is the number of dirty rule applications reachable from the root of \( D \) without passing through any clean rule applications.

For a similar purpose, we define the head cost of a term: roughly, it measures the number of “dirty” keywords—operations added by the translation. Since the translation added them, they do not occur in the source term; they are overhead that can lead to a larger target evaluation derivation. (Just counting all the “dirty” keywords in the term is too weak: it does not rule out a \( \beta \)-reduction duplicating a particularly dirty part of the term. By defining the head cost and proving that the translation generates terms that are “deeply \( k \)-bounded”, we ensure that no part of the term is too dirty; consequently, substituting a subterm during evaluation yields terms that are not too dirty.)

The head cost \( HC(e) \) of a term \( e \) is defined in Figure 20.

![Figure 20. Definition of the “head cost” \( HC(e) \) of a target expression \( e \)](image)

Definition C.4. A term \( e \) is shallowly \( k \)-bounded if \( HC(e) \leq k \).

A term \( e \) is deeply \( k \)-bounded if every subterm of \( e \) (including \( e \) itself) is shallowly \( k \)-bounded.

Similarly, a derivation \( D \) is shallowly \( k \)-bounded if \( HC(D) \leq k \), and deeply \( k \)-bounded if all its subderivations are shallowly \( k \)-bounded.

Theorem 6.7 If \( \text{trans} \ (e, e') = e' \) then \( e' \) is deeply 6-bounded.

Proof. By lexicographic induction on \( e \) and \( e' \), with \( S \) considered smaller than \( C \).

- If \( e \in \{n, x, (v_1, v_2), \text{fun} \ldots, \text{inl} v \} \) then:
Theorem C.5 (Costed Generalized Translation Soundness).

If \( e : \sigma \Rightarrow [\rho]e' : \sigma' \) and \( D :: \rho \vdash e' \downarrow (\rho' \downarrow w) \) and \([\rho]e'\) is deeply k-bounded

then \( D' :: e \downarrow v \) where \( v : \sigma \Rightarrow [\rho']w : \sigma' \) and \([\rho']w\) is deeply k-bounded

and for every subderivation \( D^* :: \rho_1 \vdash e^* \downarrow (\rho_2 \downarrow w^* ) \) of \( D \) (including \( D \))

and the number of clean rule applications in \( D \) equals \( W(D') \).

Proof. The differences from Theorems 5.4 require additional reasoning:

- The 7 cases for the “clean” rules (TEvMachineValue), (TEvPair), (TEvSum), (TEvPrimop), (TEvFst), (TEvCaseLeft), and (TEvApply) are straightforward: the induction hypothesis shows that the HC condition holds for all proper subderivations of \( D \) and \( HC(D) = 0 \) by definition of \( HC(D) \), which is certainly not greater than \( HC(e') \). Finally, each one of these cases generates a single application of an SEV^t rule, which together with the i.h. satisfies the last condition (that the number of clean rule applications in \( D \) equals \( W(D') \)).

In (TEvCaseLeft) and (TEvApply), observe that we are substituting machine values; for all machine values \( w^* \) we have \( HC(w^*) = 0 \), and by i.h. the \( w^* \) we substitute are deeply k-bounded, so the result of substitution is deeply k-bounded.

Note that this reasoning holds for (TEvMachineValue) even when \( w \) is a select: (TEvMachineValue) is a clean rule so \( HC(D) = 0 \).

- (TEvWrite) We have \( D :: \rho \vdash write(e_0) \downarrow (\rho' \downarrow w) \) with subderivation \( D_0 :: \rho \vdash e_0 \downarrow \ldots \) By i.h., \( HC(D_0) \leq HC(e_0) \). Therefore \( HC(D_0) + 1 \leq HC(e_0) \). By the definitions of HC we have \( HC(D) = HC(D_0) + 1 \) and \( HC(write(e_0)) = 1 + HC(e_0) \), so our inequality becomes \( HC(D) \leq HC(write(e_0)) \), which was to be shown. Lastly, the \( \cdots = W(D') \) condition from the i.h. is exactly what we need, because the \( D' \) is the same and (TEvWrite) is not clean.

- (TEvMod) Similar to the (TEvWrite) case.

- (TEvLet) Here we must distinguish lets generated by the translation rules (Write) and (ReadWrite), which add entirely new lets, from lets that are generated by (LetE) and (LetV). The latter kind come from the translation rules (LetE) and (LetV); even though (LetV) replaces the source binding with one that binds a select, it does not add a new let, it merely replaces one.
If we have the latter kind of \texttt{let} then its $HC(-)$ is 0 in our definition, we consider the rule “clean”, and things go as smoothly as for the 7 unambiguously clean rules (in TEvLet, reasoning analogous to TEvCaseLeft to deal with the substitution).

On the other hand, if we have \texttt{let $x = e_1$ in $e_2$} resulting from (Write) or (ReadWrite), we rely on the definition of $HC(\texttt{let ...})$ to guarantee the that the bound variable $x$ is used exactly once, justifying the definition’s adding $HC(e_1)$ and $HC(e_2)$, which would be nonsensical if $x$ didn’t appear exactly once in $e_2$.

• (TEvRead) For $HC(\texttt{read ...})$ to be defined, the variable bound is used exactly once and contributes to the $HC$ of the term accordingly, justifying the equation $HC([\rho_i/\ell]/x)[e'] = HC(e') + HC(\rho_1(\ell))$.

• (TEvSelectE)
  \[
  \begin{align*}
  HC(D_1) &\leq HC(e_1) & \text{i.h.} \\
  1 + HC(D_1) &\leq 1 + HC(e_1) & +1 \text{ each side}
  \end{align*}
  \]
  
  (R) \quad 1 + HC(e_1) \leq HC((\texttt{select \{\ldots\}})[\ldots]) \quad \text{By def. of $HC(e_1)$ and property of maxima}

  \[
  \begin{align*}
  1 &\leq HC(D_1) \leq HC(e') \quad \text{By (L), (R), transitivity, $e' = (\texttt{select \{\ldots\}})[\ldots]$
  \end{align*}
  \]

  \[
  HC(D) \leq HC(e') \quad \text{By def. of $HC(D)$}
  \]

  The $HC(e') \leq k$ part of the conclusion is easily shown: in each case, it must be shown for each premise and for the conclusion; the induction hypothesis shows it for the premises, and since we know that $[\rho]|e'$ is deeply $k$-bounded, $HC(e') \leq k$ (applying $[\rho]$ cannot decrease head cost).

  Showing that the value $w$ is deeply $k$-bounded is quite easy. For (TEvMachineValue) it follows from the assumption that $e' = w$ is bounded. For any rule whose conclusion produces the same $w$ as one of its premises—(TEvLet), (TEvCaseLeft), (TEvApply), (TEvWrite), (TEvRead), (TEvSelectE)—it is immediate by the i.h. In (TEvPair), $w_1$ and $w_2$ are bounded by i.h., so $(w_1, w_2)$ is too. The value returned by (TEvSum) and (TEvFst) is a subterm of a value in a premise, which is by i.h. deeply $k$-bounded, so the subterm is too. (TEvMod) returns $\ell$ where $\ell \mapsto w$, and $w$ is deeply $k$-bounded.

\[\square\]

Theorem 6.9. (Cost Result). Given $D :: \rho \vdash e' \downarrow (\rho' \vdash w)$ where for every subderivation $D' :: \rho_1' \vdash e' \downarrow (\rho_2' \vdash w')$ of $D$ (including $D$), $HC(D') \leq k$; then the number of dirty rule applications in $D$ is at most $\frac{k}{k+1} W(D)$.

\[\text{Proof.}\] By the definition of $HC(D)$, if $D$ is deeply $k$-bounded, there is no contiguous region of $D$ consisting only of dirty rule applications that is larger than $k$; since the only rule with no premises is TEvMachineValue, and TEvMachineValue is clean, at least one of every $k + 1$ rule applications is clean, $W(D)$ simply counts the total number of rule applications, so $D$ contains at least $\frac{W(D)}{k+1}$ clean rule applications, so no more than $\frac{k}{k+1} W(D)$ of $D$’s rule applications are dirty.

\[\square\]

Theorem 6.10. If \texttt{trans} $(e, e) = e'$ and $D :: \vdash e' \downarrow (\rho' \vdash w)$, then $D' :: e \downarrow v$ where $v : \tau \mapsto [\rho']w : \tau'$ and $W(D') \leq 7W(D)$.

\[\text{Proof.}\] By Theorem 6.7, $e'$ is deeply 6-bounded.

The algorithm \texttt{trans} merely applies the translation rules, so $\vdash e : \tau \mapsto e'$. We can show $e : \tau \mapsto e' : \tau$ as in Theorem 6.5. By Theorem C.5, $D' :: e \downarrow v$ where $v : \sigma \mapsto [\rho']w : \sigma'$ and $D$ and all its subderivations have $HC$ bounded by $k$.

By Theorem 6.8, the number of dirty rule applications in $D$ is $\leq \frac{1}{k+1} W(D)$.

Since every rule application is either clean or dirty, $W(D) \leq (k+1)W(D')$, where $k = 6$.

\[\square\]