Implicit self-adjusting computation for purely functional programs

YAN CHEN and JOSHUA DUNFIELD
Max Planck Institute for Software Systems, Kaiserslautern and Saarbrücken, Germany
(e-mail: {chenyan,joshua}@mpi-sws.org)

MATTHEW A. HAMMER
University of Maryland, College Park, Maryland, USA
(e-mail: hammer@mpi-sws.org)

UMUT A. ACAR
Carnegie Mellon University, Pittsburgh, Pennsylvania, USA and INRIA Paris-Rocquencourt, France
(e-mail: umut@cs.cmu.edu)

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.

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 [Chiang & 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 & 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; Pugh & Teitelbaum 1989; Field & 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. 2003, 2010a), 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 can require 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.

Our type system hinges on a key observation connecting self-adjusting computation to information flow (Pottier & Simonet 2003; Sabelfeld & Myers 2003): both involve tracking data dependencies (of changeable data and sensitive data, respectively) as well as dependencies between expressions and data. Specifically, 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. We present a constraint-based formulation of our type system where the constraints are a strict subset of those needed by traditional information-flow systems. Consequently, as with traditional 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.
Our goal is to translate conventional programs into self-adjusting programs. Types provide crucial information that enables transformation. First, we present a set of compositional, non-deterministic translation rules. Guided by the types, these rules identify the set of all changeable expressions that operate on changeable data and rewrite them into the self-adjusting target language. We then 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. Type inference assigns types to the rest of the program and the translation algorithm translates the program into self-adjusting target code. 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. 2006b). 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 6.14).

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. 2006b)). The third property shows that the translated program takes asymptotically as long to evaluate (from scratch) as the corresponding source program. To prove this complexity result, we use a cost semantics (Sands 1990; Sansom & Peyton Jones 1995) that enables precise reasoning about
the complexity of the evaluation time. The time for incremental updates via change propagation is usually asymptotically more efficient than running from scratch. Proving a tight bound on the complexity of change propagation is beyond the scope of this paper. Interested readers can refer to Ley-Wild et al. (2009) for more detail.

We have implemented our approach as an extension of Standard ML and the MLton compiler (MLton). The implementation takes SML code annotated with level types and generates self-adjusting code that can be linked with a previously published, publicly available library for self-adjusting computation (Acar et al. 2009). We evaluate the effectiveness of our compiler by considering a range of benchmarks involving lists, vectors, and matrices, as well as a ray tracer. For these benchmarks, our compiler incrementalizes existing code with only trivial amounts of annotation. The resulting programs are often asymptotically more efficient, leading to orders of magnitude speedups in practice. A detailed experimental evaluation is beyond the scope of this paper; interested readers can refer to Chen et al. (2012).

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 could be applied more broadly, at least for other strict languages with self-adjusting libraries (Carlsson 2002).

**Paper guide.** To describe our approach in the overview section (Section 2), we start with the translation problem and work back to the type system, because we feel that motivates well the problem and our proposed solution. When presenting the technical material, however, we start with the type system, because the details of the translation algorithm and our theorems rely on it. 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.

**Previous version.** This article is an extended version of a paper that appeared in the Proceedings of the 2011 International Conference on Functional Programming (Chen et al. 2011). Apart from many smaller improvements and corrections, this version fixes a major problem with one of the proofs. Note that only the proof was flawed, not its conclusion; the results claimed do, in fact, hold.

## 2 Overview

We present an informal overview of our approach via examples in an extension of SML with features for implicit self-adjusting computation. An implementation of this approach, including support for algebraic datatypes, Hindley-Milner polymorphism and imperative programs, was described in Chen et al. (2012). However, to simplify the theoretical presentation, our formalism will only consider a core subset of this language. We start with a brief description of our target language, explicit self-adjusting computation, as laid out in previous work. After this description, we outline our proposed approach.
Implicit self-adjusting computation for purely functional programs

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. 2006b). The programmer operates on modifiabes with `mod`, `read`, and `write` constructs to create, read from, and write into modifiabes. The run-time system of a self-adjusting language uses these constructs to represent the execution as a (directed, acyclic) dependency 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 \rightarrow 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 \(x\) unchanging or *stable*, we assign \(y\) 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 \(\rightarrow_C\):

```plaintext
squareplus_SC: int * int mod \rightarrow_C 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 delimits the code that can directly inspect the changeable value \(y\), and the changeable arrow type ensures an important consistency property: \(\rightarrow_C\)-functions can only be called within 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, and thus reusing the computation of the square \(x^2\).

Note that the result type of `squareplus_SC` is `int`, not `int mod`; `squareplus_SC` does not itself create a modifiable, it just writes to the modifiable created by the caller of the function in the context of a (dynamically) enclosing `mod` expression. In fact, programming directly in the explicit self-adjusting computation setting requires extensive knowledge of such non-obvious details of the type system. Our implicit approach also has a nontrivial type system, but manages to expose fewer sharp corners to the user.

Now suppose we wish to make \(x\) changeable while leaving \(y\) stable. We can read \(x\) and place \(x^2\) into a modifiable (because we can only read within the context of a changeable expression), and immediately read back \(x^2\) and finish by writing the sum\[1\]:

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

---

1 This is not the only way to express the computation. For instance, one could bind \(x' * x'\) to \(x^2\) and do the addition within the body of `read x`. The code shown here is the same as the code produced by our translation, and has the property that the scope of each `read` is as small as possible, which leads to more efficient updates during change propagation.
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 `squareplus_SC` and `squareplus_CS`—for instance, if we want to pass `squareplus` to various higher-order functions—we must write, and maintain, both versions. If we conservatively treat all data as modifiable, we would only need to write one version of each function, but this would introduce unacceptably high overhead. It is also possible to take the other extreme and treat all data as stable, but this would yield a non-self-adjusting program. Our approach treats data as modifiable only where necessary.

**Meta operations.** The run-time system of a self-adjusting language also supplies meta operations: `change` for inspecting and changing the values stored in modifiables and `propagate` for performing change propagation. The `change` function is similar to the `write` construct: it assigns a new value to the modifiable to a new value. The `propagate` function runs the change-propagation algorithm, which updates a computation based on the changes made since the last execution or the last change propagation. The meta operations can only be used at the top level—the run-time system guarantees correct behavior only if meta operations are not used inside the core self-adjusting program. Interested readers can refer to Acar et al. (2006a) for a more detailed discussion of the meta operations, and the change propagation algorithms used in self-adjusting computation.

As an example, consider calling the `squareplus_SC` function in a Standard ML implementation of self-adjusting runtime:

```ml
let
  val x = 1
  val y = mod 2
  val z = mod (squareplus_SC (x, y))
  val () = change (y, 3)
  val () = propagate ()
in () end
```

When calling the `squareplus_SC` function, `z` will be a modifiable containing 3. The `change` function updates modifiable `y` to be 3. The `propagate` function triggers reevaluation of the plus operation (while the square computation is reused), and stores the result 4 into modifiable `z`.

Implicit self-adjusting computation, described below, is an alternative approach for writing the self-adjusting computation itself; the interface to the meta operations remains the same.

### 2.2 Implicit self-adjusting computation

To make self-adjusting computation implicit, we use type information to insert `reads`, `writes`, and `mods` automatically. The user annotates the input type, as well as the corresponding data declarations, 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 `squareplus` above, we can automatically derive `squareplus_SC` and `squareplus_CS` from just the type of the function (expressed in a slightly different form, as we discuss next).

**Level types.** To 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 $\mathbb{S}$ (stable) and $\mathbb{C}$ (changeable). The type $\text{int}^{\delta}$ is an integer whose level is $\delta$; for example, to get `squaresum_CS` we can annotate `squaresum`’s argument with the type $\text{int}^C \times \text{int}^S$.

Level types are an important connection between information-flow types (Pottier & 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 Pottier & Simonet (2003). As a corollary, our system admits a constraint-based type inference algorithm (Odersky et al. 1999).

**Translation.** The main purpose of our type system is to support translation. Given a source expression and its type, translation inserts the appropriate mod, read, and write primitives and restructures the code to produce an expression that is well-typed in the target language.

The implicitly self-adjusting source language is polymorphic over levels. The type system of the target language, which is explicitly self-adjusting, is also polymorphic but explicitly so: polymorphic values are given as lists of values (within a select construct), with each value in the list being the translation of the source value at specific levels. Moreover, polymorphic values are explicitly instantiated by a syntactic construct in the target language; in the source language, instantiation is implicit.

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: mapPair.** To illustrate how our translation works, consider a function `mapPair` that takes two integer lists and increments the elements in both lists. This function can be written by applying the standard higher-order `map` over lists. Figure 2 shows the purely functional code in an ML-like language for an implementation of `mapPair`, with a datatype $\alpha$ list, an increment function `inc`, and a polymorphic `map` function. Type signatures give the types of functions.

To obtain a self-adjusting `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
\[
\text{datatype } \alpha \text{ list } = \text{nil } | \text{cons of } \alpha \ast \alpha \text{ list}
\]

\[
\text{inc : int } \rightarrow \text{ int}
\]

\[
\text{fun inc } (x) = x+1
\]

\[
\text{map : } (\alpha \rightarrow \beta) \rightarrow \alpha \text{ list } \rightarrow \beta \text{ list}
\]

\[
\text{fun map } f \ l =
\text{ case } l \text{ of}
\]

\[
\text{nil } \Rightarrow \text{ nil}
\]

\[
\text{ | cons}(h,t) \Rightarrow \text{ cons}(f \ h, \text{ map } f \ t)
\]

\[
\text{mapPair : } (\text{int list } \ast \text{ int list}) \rightarrow (\text{int list } \ast \text{ int list})
\]

\[
\text{fun mapPair } (l1,l2) = (\text{map inc } l1, \text{ map inc } l2)
\]

**Fig. 2.** Function `mapPair` in ML.

\[
\text{datatype } \alpha \text{ list}^\delta = \text{nil } | \text{cons of } \alpha \ast (\alpha \text{ list}^\delta)
\]

\[
\text{mapPair} : (\text{int list}^\delta \ast \text{ int list}^\delta) \rightarrow (\text{int list}^\delta \ast \text{ int list}^\delta)
\]

\[
\text{... (}
\text{inc, map, mapPair same as in Figure 2. )}
\]

**Fig. 3.** Function `mapPair` in Level ML, with level types.

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:

- \(\alpha \text{ list}^C\) for lists of \(\alpha\) with changeable tails;
- \(\alpha \text{ list}^S\) for lists of \(\alpha\) with stable tails.

Then a list of integers allowing insertion and deletion has type \(\text{int}^S \text{ list}^C\), and one with unchanging length has type \(\text{int}^C \text{ list}^S\). Now we can write the type annotation on `mapPair` shown in Figure 3. Given only that annotation, type inference can find appropriate types for `inc` and `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 mapPair.** Translating the code in Figure 3 produces the self-adjusting target code in Figure 4. Note that `inc` and `map` have level-polymorphic types. In `map inc 11` we increment stable integers, and in `map inc 12` we increment changeable integers, so the type inferred for `inc` must be generic: \(\forall \delta. \text{int}^\delta \rightarrow \text{int}^\delta\). Our translation produces two implementations of `inc`, one per instantiation (\(\delta=S\) and \(\delta=C\)): `inc_S` and `inc_C` (in Figure 4). Since we want to use `inc` with the higher-order function `map`, we need to generate a “selector” function that takes an instantiation and picks out the appropriate implementation:
Implicit self-adjusting computation for purely functional programs

\[ \text{inc} : \forall \delta. \text{int}^{\delta} \rightarrow \text{int}^{\delta} \]
\[ \text{val inc = select } \{ \delta = S \Rightarrow \text{inc}_S \\
| \delta = C \Rightarrow \text{inc}_C \} \]

In \text{mapPair} itself, we pass a level instantiation to the selector: \text{inc}[\delta=S]. (This instantiation is known statically, so it could be replaced with inc_S at compile time.) The types of \text{inc}_S and \text{inc}_C are produced by a type-level translation that, very roughly, replaces changeable types with \text{mod} types (Section 6.1).

Observe how the single annotation on \text{mapPair} led to duplication of the two functions it uses. While \text{inc}_S is the same as the original \text{inc}, the changeable version \text{inc}_C adds a \text{read} and a \text{write}. Note also that the two generated versions of \text{map} are both different from the original.

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. But some type assignments are preferable, especially when one considers constant factors. Choosing \text{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 \text{S} over \text{C}.

A combinatorial explosion? A type scheme quantifying over \( n \) level variables has up to \( 2^n \) instances. However, our experience suggests that \( n \) is usually small: level variables tend to recur in types, as in the type of \text{inc} above. Even if \( n \) turns out to be large for some practical applications, the number of \text{used} instantiations will surely be much less than \( 2^n \), suggesting that generating instances lazily would suffice.

3 A type system for implicit self-adjusting computation

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 on explicit self-adjusting computation (Ley-Wild \textit{et al.} 2008; Acar \textit{et al.} 2009) 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. This previous work developed languages that enable the programmer to separate stable and changeable data, and type systems that enforce 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 struc-
Implicit self-adjusting computation for purely functional programs

Levels $\delta, \varepsilon ::= S \mid C \mid \alpha$

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

Constraints $C, D ::= \text{true} \mid \text{false} \mid \exists \alpha. C \mid C \land D$

Type schemes $\sigma ::= \tau \mid \forall \alpha[D]. \tau$

Fig. 5. Levels, constraints, types, and type schemes in Level ML.

The starting point for our formulation is Pottier & Simonet (2003). Types in Level ML (Figure 5) 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. The levels $S$ (stable) and $C$ (changeable) have a total order:

$$
S \leq S \\
C \leq C \\
S \leq C
$$

To support polymorphism and enable type inference, we allow level variables $\alpha, \beta$ to appear in types.

Types. Types consist of integers tagged with their level, products and sums with an associated level, and arrow (function) types. Function types $(\tau_1 \to \varepsilon \tau_2)^\delta$ carry two level annotations $\varepsilon$ and $\delta$. 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.

In practice, types in source programs can omit levels, which will be derived through type inference. For example, if the user writes $\text{int}$, the system will add a level variable $\delta$ and do type inference with $\text{int}^\delta$.

Subtyping. Figure 6 shows the subtyping relation $\tau \ll \tau'$, which is standard except for the levels. It requires that the outer level of the subtype 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 or supertype of a changeable-mode function. (It would be sound to

---

1 In Pottier & Simonet (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.

---
and use a constraint solver to find solutions for the variable $s$. Our constraints levels $	au$ are changeable types (Figure 8). We write $\delta$ is at least $\tau$.

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 $C, D$ include

**Levels and types.** We rely on several relations between levels and types to ascertain various invariants. A type $\tau$ is higher than $\delta$, written $\delta \ll \tau$, if the outer level of the type is at least $\delta$. Figure 7 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 $\subseteq$. Similarly, we write $\tau$ O.C. if the outer level of $\tau$ is $\subseteq$. Finally, two types $\tau_1$ and $\tau_2$ are equal up to their outer levels, written $\tau_1 \equiv \tau_2$, 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 $C, D$ include
Implicit self-adjusting computation for purely functional programs

Values $v : : n | x | (v_1,v_2) | \text{inl } v | \text{inr } v | \text{fun } f(x) = e$

Expressions $e : : v | ⊕(x_1,x_2) | \text{fst } x | \text{snd } x |
\text{case } x \text{ of } \{ x_1 ⇒ e_1 , x_2 ⇒ e_2 \} |
\text{apply}(x_1,x_2) | \text{let } x = e_1 \text{ in } e_2$

Fig. 9. Abstract syntax of the source language Level ML.

level-variable comparisons $≤$ and level-type comparisons $δ ≤ τ$, which type inference composes into conjunctions of satisfiability predicates $∃\vec{α}.C$.

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 $φ$, substitutes concrete levels $S$ and $C$ for level variables. An assignment $φ$ satisfies a constraint $C$, written $φ ⊨ C$, if and only if $C$ holds true after the substitution of variables to ground types as specified by $φ$. We say that $C$ entails $D$, written $C ⊩ D$, if and only if every assignment $φ$ that satisfies $C$ also satisfies $D$. We write $φ(α)$ for the solution (instantiation) of $α$ in $φ$, and $[φ]τ$ for the usual substitution operation on types. For example, if $φ(α) = S$ then $[φ](\text{int}α + \text{int}C)^α = (\text{int}^S + \text{int}^C)^S$.

Type schemes. A type scheme $σ$ is a type with universally quantified level variables: $σ = ∀\vec{α}[D]. τ$. We say that the variables $\vec{α}$ are bound by $σ$. The type scheme is bounded by the constraint $D$, 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. $\text{int}^C$ as $∀\emptyset[true]. \text{int}^C$.

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. Consider the types defined by the grammar

$$τ : : \text{int} | τ_1 × τ_2 | τ_1 + τ_2 | τ_1 → τ_2$$

We augment this type system with features that allow 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 3. After discussing the rules themselves, we will look at type inference (Section 4.2).
C; Γ ⊢ e : τ  

Under constraint C and source typing  

environment Γ, source expression e has type τ  

C; Γ ⊢ e : int (SInt)  
Γ(x) = ∀α[D]. τ  C ⊢ ∃β.[β/α]D  
C ∧ [β/α]D; Γ ⊢ x : [β/α]τ  (SVar)  

C; Γ ⊢ e : int (SPair)  
C; Γ ⊢ (v1, v2) : (τ1 × τ2)δ  
C, Γ ⊢ v1 : τ1  
C, Γ ⊢ v2 : τ2  
(SPair)  

C; Γ ⊢ e : intδ  
C ⊢ δ ≤ ε  
(SFst)  

C; Γ ⊢ x : τ1  
C; Γ ⊢ e : τ′  
C ⊢ τ′ < τ′′  
C ⊢ τ′ ≤ τ′′  
(SLetE)  

C, Γ ⊢ ∃α[D]. τ′ ⊢ e2 : τ  
C, Γ ⊢ x : ∀α[D]. τ′ ⊢ e2 : τ  
C ∧ D; Γ ⊢ v1 : τ′  
C ⊢ δ ≤ ε  
(SLetV)  

C; Γ ⊢ (v1, v2) : (τ1 × τ2)δ  
C; Γ ⊢ v1 : τ1  
C; Γ ⊢ v2 : τ2  
(SApp)  

C; Γ ⊢ x : (τ1 + τ2)δ  
C ⊢ δ ≤ ε  
C ⊢ δ < τ  
C ⊢ δ ≤ τ2  
C ⊢ δ < τ2  
(CCase)  

Fig. 10. Typing rules for Level ML.

Typing takes place in the context of a constraint formula C and a typing environment Γ that maps variables to type schemes: Γ ::= ∅ | Γ, x : σ. The typing judgment C; Γ ⊢ e : τ has a constraint C and typing environment Γ, and infers type τ for expression e in mode ε. 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 C; Γ ⊢ e : τ as Γ ⊢ e : τ, read C ⊢ δ ≤ τ2 as δ < τ2, 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 to changeable values in the stable mode. This is a key principle of the type system.
Implicit self-adjusting computation for purely functional programs

Typing rules for values. No computation happens in values, so they can be typed in either mode. The typing rules for variables (SVar), integers (SInt), pairs (SPair), and sums (SSumLeft) are otherwise standard (we omit the symmetric rule typing $\text{inr} \ v$). Rule (SVar) instantiates a variable’s polymorphic type. For clarity, we also make explicit the renaming of the quantified type variables $\vec{\alpha}$ to some fresh $\vec{\beta}$ (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 $(\tau_1 \rightarrow^{\epsilon} \tau_2)^{\delta}$, and require the result type $\tau_2$ to be higher than the mode, $\epsilon \lhd \tau_2$. That is, 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. (We could instead do this check in rule (SApp), where functions are applied, but then we would have functions that are well-typed but can never be applied.)

Typing primitive operators. Rule (SPrim) allows primitive operators $\oplus$ to be applied to two stable integers, returning a stable integer, or to two changeable integers, returning a changeable integer. Allowing a mix of stable and changeable arguments in this rule would be sound, but is already handled by outer-level subsumption (discussed below).

Typing let-expressions. 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 its presence facilitates support for side effects in extensions of the language (such as the extension of full Standard ML supported by our implementation).

- (SLetE): In the first let-rule (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 $\epsilon^{[\delta]}$.
- Subsumption on outer levels: We allow subsumption only when the subtype and supertype are equal up to their outer levels, e.g. from a bound expression $\epsilon_1$ of subtype int$^S$ to an assumption $x : \text{int}^C$. This simplifies the translation, with no loss of expressiveness: to handle “deep” subsumption, such as

$$(\text{int}^S \rightarrow^{\delta} \text{int}^C)^S \lhd (\text{int}^S \rightarrow^C \text{int}^C)^C$$

we can insert coercions (essentially, eta-expanded identity functions) into the source program before typing it with these rules. This technique of eta-expanding terms to eliminate the need for nontrivial subsumption goes back to (at least) Barendregt et al. (1983), and could easily be automated.

- (SLetV): In the second let-rule (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

$^3$ 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.
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.

**Typing elimination forms.** Function application, ⊕ (discussed above), fst, and case are
the forms that eliminate values of changeable type.

Rule (SApp) types applications. Two additional constraints are needed, beyond the one
enforced in (SFun) (that changeable-mode functions have changeable result types: \( \varepsilon \triangleleft \tau_2 \)):

- The mode \( \varepsilon' \) of the function being called must match the current mode \( \varepsilon \) (the caller’s
  mode): \( \varepsilon' = \varepsilon \).
  To see why, first consider the case where we are in stable mode and try to apply
  a changeable-mode function (\( \varepsilon = \text{S} \) and \( \varepsilon' = \text{C} \)). Changeable data can be directly
  inspected only in changeable mode; since changeable-mode functions can directly
  inspect changeable data, the call would allow us to inspect changeable data from
  stable mode, breaking the property that stable data depends only on stable data.
  Now consider the case where we are in changeable mode, and try to call a stable-
  mode function (\( \varepsilon = \text{C} \) and \( \varepsilon' = \text{S} \)). This call would not directly violate the same
  property; we forbid it to simplify translation to a target language that distinguishes
  stable and changeable modes. Since the rules (SLetV) and (SLetE) can switch from
  changeable mode to stable mode, we lose no expressive power.

- The outer level of the result of the function, \( \tau_2 \), must be higher than \( \delta \), the function’s
  level: \( \delta \triangleleft \tau_2 \).
  The situation we disallow is when \( \delta = \text{C} \) and \( \tau_2 \) is outer-stable, that is, when the
  called function has a type like \( (\tau_1 \to^{\varepsilon} \text{int}^\delta)^\text{C} \). Here, the result type \( \text{int}^\delta \) is stable
  and therefore must not depend on changeable data. But the type \( (\tau_1 \to^{\varepsilon} \text{int}^\delta)^\text{C} \) is
  changeable: a change in program input could cause it to be entirely replaced by
  another function, which could of course return a different result!
  (Assuming “deep” subsumption, we lose no expressive power: we can coerce a
  function of type \( (\tau_1 \to^{\varepsilon} \text{int}^\delta)^\text{C} \) to type \( (\tau_1 \to^{\varepsilon} \text{int}^\text{C})^\text{C} \), which satisfies the constraint.)

Note that neither of these constraints could be enforced via (SFun). The first depends
on the current (caller’s) mode, so it must be checked at the call site. The second depends
on the outer level \( \delta \), which might have been originally declared as \( \text{S} \), but can rise to \( \text{C} \) via
subsumption.

The rule (SCase) types a case expression, in either mode \( \varepsilon \), by typing each branch in \( \varepsilon \).
The mode \( \varepsilon \) 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 (SFst) enforces a condition, similar to (SCase), that we can project out of a changeable
tuple of type \( (\tau_1 \times \tau_2)^\text{C} \) 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 (\( \to^{\text{S}} \)), but
this was an arbitrary decision; since (SVar) is the only rule that can derive such premises,
their mode is irrelevant.
Implicit self-adjusting computation for purely functional programs

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 $C = \ldots \land (e \ll \tau_2)$. Rule (SLetV) generalizes level variables instead of type variables, with the “occurs check” $\vec{a} \cap FV(C, \Gamma) = \emptyset$.

Standard techniques in the tradition of [Damas & 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 $S$ or $C$ to some level variable, prefers $S$, 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 & Simonet 2003].

Our formulation of the constraint-based rules follows a standard presentation style [Odersky et al. 1999]. That style, while relatively concise, obscures how constraints are manipulated in practice: It is tempting to read the typing rules in Figure 10 as taking in a constraint $C$ as input. But in an actual constraint-based typechecker, $C$ cannot be input, because $C$ is not known until the program has been traversed! In practice, $C$ should be thought of as both input and output: at the start of typechecking, $C$ is empty (equivalently, is true); as the typechecker traverses the program, $C$ is extended with additional constraints. For example, the premise $C \models \delta \leq \epsilon$ in (SFst) really corresponds to adding $\delta \leq \epsilon$ to the “current” $C$, not to checking $\delta \leq \epsilon$ under a known constraint.

An alternative would be to use a judgment with both an input constraint and an output constraint. For a typing of the entire program, the input constraint would be true (at the beginning of typechecking) and the output constraint would correspond to the “final” $C$ in the current formulation. Such a formulation would be closer to an algorithm, but would require explicitly threading the constraint through the rules. Moreover, our meta-theoretical development would become more complicated; in the meta-theory, we care about the result of type inference, not internal details of the algorithm.

4.3 Dynamic semantics

The call-by-value semantics of source programs is defined by a big-step judgment $e \Downarrow v$, 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 $e$. To simplify the presentation, we omit the symmetric rules (SEvSumRight), (SEvSnd) and (SEvCaseRight).

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 `select` in AFL. The type schemes used in the target are identical to those in the source language; \( \sigma = \forall \alpha[D], \tau \) quantifies over source types \( \tau \) (from Figure 5), not target types \( \tau \). We cannot quantify over target types here, because no single type scheme over target types can represent exactly the set of types corresponding to the instances of a source type scheme. For example, the source type scheme \( \forall \alpha[true], \text{int} \) corresponds to \( \text{int} \) if \( \alpha \) is instantiated with \( \text{int} \), and to \( \text{int mod} \) if \( \alpha \) is instantiated with \( \text{int} \), but the set of types \{\( \text{int}, \text{int mod} \)\} does not correspond to the instances of any type scheme.

The values \( w \) of the language are integers, variables, polymorphic variable instantiation \( x[\alpha = \delta] \), 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` \{\( \alpha = \text{S} \) \( \Rightarrow e_1 \) | \( \alpha = \text{C} \) \( \Rightarrow e_2 \)\} then \( x[\alpha = \delta] \) yields \( e_1 \). The symbol \( \delta \) stands for a bare variable \( x \) or an instantiation \( x[\alpha = \delta] \).

We distinguish stable expressions \( e^S \) from changeable expressions \( e^C \). Stable expressions create purely functional values; \( \text{apply}^S \) 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,
 Implicit self-adjusting computation for purely functional programs  

The read expression binds the contents of a modifiable \( x \) 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 \( e_i \) within a select has type \( ∥[\delta/\bar{\alpha}]/\tau∥ \), where \( [\delta/\bar{\alpha}]\tau \) is a source-level polymorphic type with the levels \( \delta \) substituted for the variables \( \bar{\alpha} \), and \( ∥-∥ \) 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 \( x[\bar{\alpha} = \delta] \), of a variable \( x \) of polymorphic type, the type \( ∥[\delta/\bar{\alpha}]/\tau∥ \)—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. Again, we omit symmetric rules such as (SEvSumRight).

According to the grammar in Figure 11, \( x[\bar{\alpha} = \delta] \) is a value. It might seem that evaluation (Figure 14) could replace the variable \( x \) by a select expression, yielding \( \text{select} \{ \ldots \}[\bar{\alpha} = \delta] \), which does not evaluate to itself. However, \( x[\bar{\alpha} = \delta] \) is not closed, and we only evaluate closed target expressions.

6 Translation

We specify the translation from Level ML to the target language AFL by a set of a rules. Because AFL is a modal language that distinguishes stable and changeable expressions, with a corresponding type system (Section 5), the translation is also modal: the translation in the stable mode \( \rightarrow_S \) produces a stable AFL expression \( e^S \), and the translation in the changeable mode \( \rightarrow_C \) produces a changeable expression \( e^C \).

It is not enough to generate AFL expressions of the right syntactic form; they must also have the right type. To achieve this, the rules are type-directed: we translate a source expression \( e \text{ at type } \tau \). But we are transforming expressions from one language to another, where each language has its own type system; translating some \( e : \tau \) cannot produce some \( e' : \tau \), but some \( e' : \tau' \) where \( \tau' \) is a target type that corresponds to \( \tau \). To express this vital property, we need to translate types, as well as expressions. We developed the translation of expressions and types together (along with the proof that the property holds); the translation of types was instrumental in getting the translation of expressions right. To understand how to translate expressions, it is helpful to first understand how we translate types.

6.1 Translating types

Figure 15 defines the translation of types via two mutually recursive functions from Level ML types to AFL types. The first function, \( ∥\tau∥ \), tells us what type the target expression \( e^S \) should have when we translate \( e \) in the stable mode, \( e : \tau \rightarrow_S e^S \). We also use it to translate
\[ \Lambda; \Gamma \vdash w : \sigma \]

Under store typing \( \Lambda \) and target typing environment \( \Gamma \), target value \( w \) has type scheme \( \sigma \)

for all \( \vec{\delta} \) such that \( \vec{\alpha} = \vec{\delta} \upharpoonright D \)

\[ \Lambda; \Gamma \vdash e_1 : \|\vec{\delta}/\vec{\alpha}\| \quad (\text{TSelect}) \]

\[ \Lambda; \Gamma \vdash e^\ell : \tau \]

Under store typing \( \Lambda \) and target typing environment \( \Gamma \), target expression \( e^\ell \) has type target \( \tau \)

\[ \Lambda(\ell) = \vec{\xi} \quad (\text{TLoc}) \]
\[ \Lambda; \Gamma \vdash e : \xi \quad (\text{TInt}) \]

\[ \Gamma(x) = \vec{\xi} \quad (\text{TPVar}) \]
\[ \Lambda; \Gamma \vdash x : \xi \quad (\text{TVar}) \]

\[ \Lambda; \Gamma \vdash e_1^\ell : \xi_1 \quad (\text{TPair}) \]
\[ \Lambda; \Gamma \vdash e_2^\ell : \xi_2 \]

\[ \Lambda; \Gamma \vdash (e_1^\ell, e_2^\ell) : \xi_1 \times \xi_2 \]

\[ \Lambda; \Gamma \vdash \text{inl} e : \xi_1 \quad (\text{TSumLeft}) \]
\[ \Lambda; \Gamma \vdash \text{inr} e : \xi_2 \]

\[ \Lambda; \Gamma \vdash e^\prime = e_1 \vdash e_2 : \xi \quad (\text{TPrim}) \]

\[ \Lambda; \Gamma \vdash \text{let } x = e_1^\ell \text{ in } e_2 : \xi \quad (\text{TLet}) \]

\[ \Lambda; \Gamma \vdash \text{apply}^\ell(e_1^\ell, e_2^\ell) : \xi_1 \quad (\text{TApp}) \]

\[ \Lambda; \Gamma \vdash \text{case} e^\ell \text{ of } (x_1 \Rightarrow e_1, x_2 \Rightarrow e_2) : \xi \quad (\text{TCase}) \]

\[ \Lambda; \Gamma \vdash \text{read} e_1^\ell \text{ as } x \text{ in } e_2^\ell : \xi \quad (\text{TRead}) \]

\[ \Lambda; \Gamma \vdash e_1^\ell : \xi \quad \text{for all } \vec{\delta} \text{ such that } \vec{\alpha} = \vec{\delta} \upharpoonright D \]

\[ \Lambda; \Gamma \vdash \|\vec{\delta}/\vec{\alpha}\| \]

Fig. 12. Typing rules of the target language AFL.
the types in the environment \( \Gamma \). The second function, \( \| \tau \|_C^- \), makes sense in two related situations: translating the type \( \tau \) of an expression \( e \) in the changeable mode \( (e : \tau \rightarrow e^C) \) and translating the codomain of changeable functions.

In the stable mode, values of stable type can be used and created directly, so the “stable” translation \( \| \text{int} \| \) of a stable integer is just \text{int}. In contrast, a changeable integer cannot be inspected or directly created in stable mode, but must be placed into a modifiable: \( \| \text{int}^C \| = \text{int mod} \). The remaining parts of the definition follow this pattern: the target type is wrapped with \text{mod} if and only if the outer level of the source type is \( C \). When we translate a changeable-mode function type (with \( C \) below the arrow), its codomain is translated “output-changeable”: \( \| (\tau_1 \rightarrow \tau_2)^S \| = \| \tau_1 \|_C^- \| \tau_2 \|_C^- \). The reason is that a changeable-mode function can only be applied in the changeable mode; the function result is not placed into a modifiable until we return to the stable mode, so putting \text{a mod} on the codomain would not match the dynamic semantics of AFL.

The second function \( \| \tau \|_C^- \) defines the type of a changeable expression \( e \) that writes to a modifiable containing \( \tau \), yielding a changeable target expression \( e^C \). The source type has an outer \( C \), so when the value is written, it will be placed into a modifiable and have \text{mod} type. But inside the evaluation of \( e^C \), there is no outer \text{mod} on the type. Thus the translation \( \| \tau \|_C^- \) ignores the outer level (using the function \( \lceil - \rceil^S \), which replaces an outer level \( C \) with \( S \)), and never returns a type of the form \( \cdots \text{mod} \). However, since the value being returned may contain subexpressions that will be placed into modifiabes, we use \( \lceil - \rceil \) for the inner types. For instance, \( \| (\tau_1 \tau_2)^S \|_C^- = \| \tau_1 \|_C^- \| \tau_2 \|_C^- \).

These functions are defined on closed types—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 \( \| \tau \|_\phi \) for \( \| \phi \| \tau \| \), and so on.

---

[4] In this respect, \text{mod} behaves like a monadic or computational type constructor, like the \( \odot \) modality of lax logic [Pfenning & Davies 2001]: \text{inside} a computation-level (changeable) expression, the result type is \( \tau \), but outside of the computation/monad, the result has type \( \odot \tau \).
In the store ρ, target expression e evaluates to w with updated store ρ’

\[ \rho \vdash e \downarrow (\rho' \vdash w) \]

(TEvValue)

\[ \rho \vdash w \downarrow (\rho \vdash w) \]

(TEvVal)

\[ \rho \vdash e_1 \downarrow (\rho_1 \vdash w_1) \]

(TEvPair)

\[ \rho \vdash e_2 \downarrow (\rho' \vdash w_2) \]

\[ \rho \vdash e \downarrow (\rho' \vdash w) \]

(TEvSumLeft)

\[ \rho \vdash e_1 \downarrow (\rho_1 \vdash w_1) \]

\[ \rho \vdash (w_1, w_2) = w' \]

(TEvPrimop)

\[ \rho \vdash e \downarrow (\rho' \vdash (w_1, w_2)) \]

(TEvFst)

\[ \rho \vdash e \downarrow (\rho' \vdash w_1) \]

(TEvLet)

\[ \rho \vdash e_1 \downarrow (\rho_1 \vdash \text{inl } w_1) \]

\[ \rho \vdash [w_1 / x] e_2 \downarrow (\rho' \vdash w) \]

(TEvCaseLeft)

\[ \rho \vdash e \downarrow (\rho' \vdash w) \]

(TEvApply)

\[ \rho \vdash e \downarrow (\rho' \vdash w) \]

(TEvWrite)

\[ \rho \vdash e \downarrow (\rho' \vdash w) \]

(TEvRead)

\[ \rho \vdash e \downarrow (\rho' \vdash w) \]

(TEvSelect)

\[ \rho \vdash e \downarrow (\rho' \vdash w) \]

(TEvMod)

Fig. 14. Dynamic semantics for first runs of AFL programs.

Because the translation only makes sense for closed types, type schemes \( \forall \alpha [D] \), \( \tau \) cannot be translated before instantiation. Consider the type \( \forall \alpha [\text{true}] \). int\( ^\alpha \), and the translations of its instantiations:

\[ \| \text{int} \| = \text{int} \]

\[ \| \text{int mod} \| = \text{int mod} \]

No single type scheme over target types can represent exactly the set of types \{ int, int mod \}. The translation \( \| \Gamma \| \), therefore, translates only monomorphic types: type schemes are left alone until instantiation. Once instantiated, the type scheme is an ordinary closed source type, and can be translated by rule (Var) in Figure 10.
environments

We define the translation of expressions as a set of type-directed rules. Given (1) a derivation of $C;\Gamma \vdash_\varphi e : \tau$ in the constraint-based typing system and (2) a satisfying assignment $\phi$ for $C$, it is always possible to produce a correctly typed stable target expression $e^S$ and a correctly typed changeable target expression $e^C$ (see Theorem 6.1 below). The environment $\Gamma$ in the translation rules is a source typing environment, but must have no free level variables. Given an environment $\Gamma$ from the constraint typing, we apply the satisfying
Under closed source typing environment $\Gamma$, source expression $e$ is translated at type $\tau$ in mode $\varepsilon$ to target expression $e^\varepsilon$.

$\Gamma \vdash e : \tau \overset{\varepsilon}{\rightarrow} e^\varepsilon$

### Int

- $\Gamma \vdash n : \text{int}\delta \overset{\varepsilon}{\rightarrow} n$

### Var

- $\Gamma \vdash \alpha : \text{id}_{\tau} \overset{\varepsilon}{\rightarrow} \alpha$

### Pair

- $\Gamma \vdash v_1 : \tau_1 \overset{\varepsilon}{\rightarrow} v'_1$
- $\Gamma \vdash v_2 : \tau_2 \overset{\varepsilon}{\rightarrow} v'_2$

### Fun

- $\Gamma, x : \tau_1, f : (\tau_1 \overset{\varepsilon}{\rightarrow} \tau_2) \overset{\varepsilon}{\rightarrow} e \overset{\varepsilon}{\rightarrow} e^\varepsilon$

### SumLeft

- $\Gamma \vdash \text{in} \overset{\varepsilon}{\rightarrow} (\tau_1 + \tau_2) \overset{\varepsilon}{\rightarrow} \text{in} v'$

### Prim

- $\Gamma \vdash \text{let} x = e_1 \overset{\varepsilon}{\rightarrow} e_2 \overset{\varepsilon}{\rightarrow} e^\varepsilon$

### App

- $\Gamma \vdash \text{apply}(x_1, x_2) : \tau_1 \overset{\varepsilon}{\rightarrow} \tau_2 \overset{\varepsilon}{\rightarrow} \text{apply}^\varepsilon(x_1, x_2)$

### Case

- $\Gamma \vdash \text{case} x \overset{\varepsilon}{\rightarrow} \text{of} \{ x_1 \Rightarrow e_1, x_2 \Rightarrow e_2 \} : \tau$

### Lift

- $\Gamma \vdash e : \tau' \overset{\varepsilon}{\rightarrow} e^C$ | $| \tau | = \tau'$

### Mod

- $\Gamma \vdash e : \tau \overset{\varepsilon}{\rightarrow} \text{mod } e^C$

### LetE

- $\Gamma \vdash \text{let } x = e_1 \overset{\varepsilon}{\rightarrow} e_2 : \tau \overset{\varepsilon}{\rightarrow} \text{let } x = e_2 \overset{\varepsilon}{\rightarrow} e_2$

### LetV

- $\Gamma \vdash \text{let } x = v \overset{\varepsilon}{\rightarrow} e \overset{\varepsilon}{\rightarrow} \text{let } x = \text{select } \{ (\alpha = \delta) \Rightarrow e'_1 \} : \tau$ 

### Read

- $\Gamma \vdash e \overset{\varepsilon}{\rightarrow} \text{read } x \overset{\varepsilon}{\rightarrow} \text{as } x' \overset{\varepsilon}{\rightarrow} e^C$

### Write

- $\Gamma \vdash e : \tau \overset{\varepsilon}{\rightarrow} \text{let } r = e^\varepsilon \overset{\varepsilon}{\rightarrow} \text{write}(r)$

### WriteRead

- $\Gamma \vdash e : \tau \overset{\varepsilon}{\rightarrow} \text{let } r = e^\varepsilon \overset{\varepsilon}{\rightarrow} \text{read } r \overset{\varepsilon}{\rightarrow} \text{write}(r)$

Fig. 16. Monomorphizing translation.
Under source typing $\Gamma$, renaming the "head" $x$ in $e$ to $x' : \tau$ yields expression $e'$

$$\begin{align*}
\Gamma \vdash e \leadsto (x \gg x' : \tau \vdash e')
\end{align*}$$

LPrimop1: $\Gamma \vdash x_1 : \tau$

$$\frac{\Gamma \vdash \oplus(x_1,x_2) \leadsto (x_1 \gg x'_1 : \tau \vdash \oplus(x'_1,x'_2))}{\Gamma \vdash \oplus(x_1,x_2) \leadsto (x_2 \gg x'_2 : \tau \vdash \oplus(x_1,x'_2))}$$

LPrimop2: $\Gamma \vdash x : \tau$

$$\frac{\Gamma \vdash \text{fst} \ x \leadsto (x \gg x' : \tau \vdash \text{fst} \ x')}{\Gamma \vdash \text{fst} \ x \leadsto (x \gg x' : \tau \vdash \text{fst} \ x')}$$

LFst: $\Gamma \vdash x_1 : \tau$

$$\frac{\Gamma \vdash \text{apply} \ (x_1,x_2) \leadsto (x_1 \gg x' : \tau \vdash \text{apply} \ (x',x_2))}{\Gamma \vdash \text{apply} \ (x_1,x_2) \leadsto (x_1 \gg x' : \tau \vdash \text{apply} \ (x',x_2))}$$

LApply: $\Gamma \vdash x : \tau$

$$\frac{\Gamma \vdash \text{case} \ x \text{ of} \ \{ x_1 \Rightarrow e_1 \ , \ x_2 \Rightarrow e_2 \}}{\Gamma \vdash \text{case} \ x \text{ of} \ \{ x_1 \Rightarrow e_1 \ , \ x_2 \Rightarrow e_2 \}}$$

(LError)

$LCase$: $\Gamma \vdash x_1 : \tau$

$$\frac{\Gamma \vdash \text{apply} \ (x_1,x_2) \leadsto (x_1 \gg x' : \tau \vdash \text{apply} \ (x'_1,x_2))}{\Gamma \vdash \text{apply} \ (x_1,x_2) \leadsto (x_1 \gg x' : \tau \vdash \text{apply} \ (x'_1,x_2))}$$

$LApply$: $\Gamma \vdash x : \tau$

$$\frac{\Gamma \vdash \text{case} \ x \text{ of} \ \{ x_1 \Rightarrow e_1 \ , \ x_2 \Rightarrow e_2 \}}{\Gamma \vdash \text{case} \ x \text{ of} \ \{ x_1 \Rightarrow e_1 \ , \ x_2 \Rightarrow e_2 \}}$$

$LCase$: $\Gamma \vdash x : \tau$

$$\frac{\Gamma \vdash x : \tau}{\Gamma \vdash x : \tau}$$

$LCase$:

Fig. 17. Renaming the variable to be read (elimination forms).

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 16 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 $x : \forall \alpha \text{true}, (\alpha \rightarrow \alpha \rightarrow \alpha \rightarrow \alpha) \rightarrow (\alpha \rightarrow \alpha)$, we need the type from $C; \Gamma \vdash e \ x \ : \ (\alpha \rightarrow \alpha \rightarrow \alpha \rightarrow \alpha) \rightarrow (\alpha \rightarrow \alpha)$ so we can instantiate $\alpha$ in the translated term $x[\alpha = C]$.

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), (SumLeft), (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 $e^S$, the rules (Write) and (ReadWrite) at the bottom of Figure 16 translate $e$ in the changeable mode, producing an $e^C$. If the expression’s type $\tau$ is outer stable (say, $\text{int}^S$), the (Write) rule simply binds it to a variable and then writes that variable. If $\tau$ is outer changeable (say, $\text{int}^C$) it will be in a modifiable at runtime, so we read it into $r'$ and then write it. (The let-bindings merely satisfy the requirements of A-normal form.)

**Shifting to stable mode.** To generate a stable expression $e^S$ 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 $|\tau|^S = \tau'$ requires that $|\tau|^S$ is defined, and it is defined only for outer changeable $\tau$; in (Mod), the requirement is explicit: $\vdash \tau \ O.C.$
(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 translated not at the given type \( \tau \) but at its stabilized \( |\tau|^S \), capturing the “shallow subsumption” in the constraint typing rules (SLetE) and (SLetV): a bound expression of type \( \tau_0^S \) can be translated at type \( \tau_0^C \) to \( e_0^C \), and then “promoted” to type \( \tau_0^S \) by placing it inside a \text{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 \( x : \texttt{int}^C \) to a function expecting \( \texttt{int}^S \)—the (Read) rule generates a target expression that reads the value out of \( x : \texttt{int}^C \) into \( x' : \texttt{int}^S \). The variable-renaming judgment \( \Gamma \vdash e \bowtie (x \gg x' : \tau \vdash e') \) 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, \( \Gamma \vdash \text{case } x \text{ of } \ldots \bowtie (x \gg x' : \tau \vdash \text{case } x' \text{ of } \ldots ) \). This judgment is derivable only for \texttt{apply}, \texttt{case}, \texttt{fst}, and \texttt{⊕}, 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 17.

**Monomorphization.** A polymorphic source expression has no directly corresponding target expression: the map function from Section 2 corresponds to the two functions map_{SC} and map_{CS}. Given a polymorphic source value \( v : \forall \alpha[D]. \tau' \), the (LetV) rule translates \( v \) once for each instantiation \( \vec{a} \) that satisfies the constraint \( D \) (each \( \vec{d}_i \) such that \( \vec{a} = \vec{d}_i \vdash D \)). That is, we translate the value at source type \( [\vec{d}/\vec{a}] \tau' \). This yields a sequence of source expressions \( e_1, \ldots, e_n \) for the \( n \) possible instances. For example, given \( \forall \alpha[\texttt{true}] \). \( \tau' \), we translate the value at type \( [\alpha/\texttt{true}] \tau' \) yielding \( e_1 \) and at type \( [\alpha/\texttt{true}] \tau' \) yielding \( e_2 \). Finally, the rule produces a \text{select} expression, which acts as a function that takes the desired instance \( \vec{d}_i \) and returns the appropriate \( e_i \).

Since (LetV) generates one function for each satisfying \( \vec{d}_i \), 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 16 is not deterministic. In fact, if the wrong choices are made it can produce painfully inefficient code. Suppose we have \( 2 : \texttt{int}^C \), 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 an \( e^C \) with a \texttt{let}, a \texttt{read} and a \texttt{write}—then (Mod), which wraps that \( e^C \) in a \texttt{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 \( \varepsilon \).
function trans \((e, \epsilon)\) = case \((e, \epsilon)\) of
  | \((n, S)\) ⇒ Int
  | \((x, S)\) ⇒ Var
  | \(((v_1, v_2), S)\) ⇒ Pair(trans\((v_1, S)\), trans\((v_2, S)\))
  | \((\text{fun } f(x) = e' : (\tau_1 \rightarrow \tau_2)^\delta, S)\) ⇒ Fun(trans\((e', \epsilon')\))
  | \((\text{inl } v, S)\) ⇒ SumLeft(trans\((v, S)\))
  | \((\text{fst } x : (\tau_1 \times \tau_2)^\delta, \epsilon)\) ⇒ case \((\epsilon, \epsilon)\) of
    | \((S, S)\) ⇒ \(\text{fst }\) trans\((x, S)\)
    | \((S, C)\) ⇒ if \(\tau_1\) o.s. then Write(trans\((e, S)\))
    | \((C, C)\) ⇒ Read(LFst, trans\((\text{fst } (x : (\tau_1 \times \tau_2)^\delta), C)\), trans\((x, S)\))
  | \(\langle x_1 : \text{inf}^\delta, x_2 : \text{inf}^\delta, \rangle, S)\) ⇒ Prim(trans\((x_1, S)\), trans\((x_2, S)\))
  | \(\langle x_1 : \text{inf}^\delta, x_2 : \text{inf}^\delta, C\rangle\) ⇒ Write(trans\((e, S)\))
  | \(\langle x_1 : \text{inf}^\delta, x_2 : \text{inf}^\delta, \rangle, C\) ⇒ Read(LPrimop1,
            Read(LPrimop2,
            Write(trans\((\langle x_1', x_2'\rangle, S\)),
            trans\((x_1, S)\))
  | \((x : \tau'' = e_1 : \epsilon) : \epsilon)\) ⇒
    \(\langle x : \forall \epsilon : t. \epsilon = e_2, \epsilon \rangle\) ⇒
    let \(\epsilon = \langle x : \forall \epsilon : t. \epsilon = e_2, \epsilon \rangle\) ⇒
    \(\text{case } (\epsilon', \delta, \epsilon)\) of
    | \((S, S, S)\) ⇒ App(trans\((x_1, S)\), trans\((x_2, S)\))
    | \((C, C, C)\) ⇒ App(trans\((x_1, S)\), trans\((x_2, S)\))
    | \((S, C, C)\) ⇒ if \(\tau_2\) o.s. then Write(trans\((e, S)\))
    | \((\epsilon', C, C)\) ⇒ Read(LApply,
            \(\langle x_1 : (\tau_1 \rightarrow \tau_2)^\delta, x_2\rangle, C\),
            trans\((x_1, S)\))
    | \((C, S, C)\) ⇒ Mod(trans\((e, C)\))
    | \((\epsilon', C, C)\) ⇒ Mod(trans\((e, C)\))
  | \((x : \tau, C)\) ⇒ if \(\tau\) o.s. then Write(trans\((e, S)\))
  | \((\text{fun } f(x) = e', C)\) ⇒ \(\text{fun } f(x) = e', C)\)
Given a constraint-based source typing derivation and assignment $\phi$ for some term $e$, it is possible to translate $e$ to (1) a stable $e^S$ and (2) a changeable $e^C$, 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 $e^S$ such that $[\phi]|\Gamma \vdash e^S : \tau$ and $\cdot \parallel \Gamma \parallel \phi \vdash e^S : \parallel \tau \parallel \phi$ and, if $e$ is a value, then $e^S$ is a value;
2. there exists $e^C$ such that $[\phi]|\Gamma \vdash e^C : \tau$ and $\cdot \parallel \Gamma \parallel \phi \vdash e^C : \parallel \tau \parallel \phi$.

The proof (Appendix A) is by induction on the height of the given derivation of $C; \Gamma \vdash e : \tau$. If the concluding rule was (SLetE), we use a substitution property (Lemma A.2) for each $\delta_i$ to get a monomorphic constraint typing derivation; that derivation is not 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).

When applying the theorem “from the outside”, it suffices to get an expression of the same mode as the the typing derivation: given $C; \Gamma \vdash e : \tau$, use part (1) to get $e^S$; given $C; \Gamma \vdash e : \tau$, use part (2) to get $e^C$. However, inside the proof, we need both parts (1) and (2). For example, in the (SLetE) case of the proof, we apply the induction hypothesis to the typing derivation for the let-bound subexpression; in one subcase, the subexpression $e_1$ is typed in stable mode, but we need a changeable-mode translation of $e_1$.

**6.5 Translation soundness**

Having shown that the translated programs have appropriate types, we now prove that running a translated program gives the same result as running the source program.

Theorem 6.5 states that if evaluating the translated program $e'$ (in an initially-empty store) yields a (target-language) value $w$ under a new store $\rho'$, then the source program $e$ evaluates to $v$ where $v$ corresponds to $[\rho']w$ (the result of substituting values in the store $\rho'$ for locations appearing in $w$).

We define this correspondence via a back-translation $[e']$ which, given some $e'$ which resulted from translating $e$, essentially yields $e$. The modifier “essentially” is necessary because, to facilitate the proof of translation soundness, the result of back-translation is not literally $e$—it may add some let expressions. The result of back-translation is, however, equivalent to $e$: if $[e'] \downarrow v$ then $e \downarrow v$.

Concretely, the back-translation removes all the constructs related to the store: write $(x)$ becomes $x$; read expressions are replaced with lets; mod expressions are replaced with...
their bodies. The back-translation also removes level superscripts: \texttt{apply} becomes \texttt{apply}, etc. Finally, the back-translation drops instantiations of polymorphic variables, replacing \(x([α = β])\) with \(x\), and replaces \texttt{select} expressions with the back-translation of a branch. (The translation guarantees that all branches of a \texttt{select} will have semantically equivalent back-translations, a property we call \texttt{select}-uniformity.) We give the full definition in Figure 19.

\[
\[
\begin{align*}
[x] & = x \\
[e(α = β)] & = [e] \\
\text{apply}(e_1, e_2) & = \text{apply}([e_1], [e_2]) \\
\text{fun } f(x) = e & = \text{fun } f(x) = [e] \\
\text{select } \{(α_1 = β_1) \Rightarrow e_1\} & = [e_1] \\
\text{mod } e & = [e] \\
\text{write}(e) & = [e] \\
\text{read } e_1 \text{ as } y \text{ in } e_2 & = \text{let } y = [e_1] \text{ in } [e_2] \\
[n] & = n \\
\{e_1, e_2\} & = ([e_1], [e_2]) \\
\text{fst } e & = \text{fst } [e] \\
\text{snd } e & = \text{snd } [e] \\
\text{inl } e & = \text{inl } [e] \\
\text{inr } e & = \text{inr } [e] \\
\text{case } e \text{ of } \{x_1 \Rightarrow e_1, x_2 \Rightarrow e_2\} & = \text{case } [e] \text{ of } \{[e_1], [e_2]\} \\
\oplus(e_1, e_2) & = \oplus([e_1], [e_2]) \\
\text{let } x = e_1 \text{ in } e_2 & = \text{let } x = [e_1] \text{ in } [e_2]
\end{align*}
\]

Fig. 19. Back-translation, used for correspondence between target and source dynamic semantics

The details of soundness depend on a simple notion of source equivalence (source terms are equivalent if they either evaluate to the same value, or diverge), and on an ordinary substitution \(\rho[e]\) on target terms.

**Definition 6.2.** Source expressions \(e_1, e_2\) are **equivalent**, \(e_1 \sim e_2\), iff both evaluate to the same value, or both diverge: if there exists \(v_1\) such that \(e_1 \triangleright v_1\) then \(e_2 \triangleright v_1\), and if there exists \(v_2\) such that \(e_2 \triangleright v_2\) then \(e_1 \triangleright v_2\).

**Definition 6.3.** Given a store \(\rho\), which maps locations \(\ell\) to target terms \(\rho(\ell)\), and a target term \(e\), the **store substitution** operation \(\rho[e]\), for all \(\ell \in \text{dom}(\rho)\), replaces each occurrence of \(\ell\) in \(e\) with \(\rho(\ell)\).

For example, \([\ell_1 \mapsto 1, \ell_2 \mapsto (\ell_1, 2)](\ell_1, \ell_2) = (1, (1, 2))\).

**Theorem 6.4** (Evaluation Soundness). If \(\vdash e \triangleright (\rho' \triangleright w)\) where \(\text{FLV}(e) \subseteq \text{dom}(\rho)\) and \(\rho[e]\) is **select-uniform** then \(\llbracket\rho[e]\rrbracket \triangleright \llbracket\rho'[e]\rrbracket\).

**Theorem 6.5** (Translation Soundness). If \(\vdash e : \tau \triangleright e'\) and \(\vdash e' \triangleright (\rho' \triangleright w)\) then \(e \triangleright \llbracket\rho'[e]\rrbracket\).
Acar et al. (2006b) proved that given a well-typed AFL program, change propagation updates the output consistently with an initial run. Using Theorems 6.1 and 6.5, this implies that change propagation is consistent with an initial run of the source program.

6.6 Cost of translated code

Our last main result extends Theorem 6.5, showing that the size $W(D)$ of the derivation of the target-language evaluation $\vdash e' \Downarrow (\rho \vdash w)$ is asymptotically the same as the size $W(D')$ of the derivation of the source-language evaluation $[[e']] \Downarrow [[\rho]w]$. To prove Theorem 6.14, the extended version of Theorem 6.5 we need a few definitions and intermediate results. The proof hinges on classifying keywords added by the translation, such as write, as “dirty”: a dirty keyword leads 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.

The omitted proofs can be found in Appendix C.

To extend the evaluation soundness result above (Theorem 6.4) 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 6.6. 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 6.7. Rules (TEvValue), (TEvPair), (TEvSumLeft), (TEvPrimop), (TEvCase), (TEvFst), and (TEvApply) are clean. Rule (TEvLet) is clean, since each let in the target expression becomes a let in the back-translation. The rules (TEvWrite), (TEvMod), (TEvRead) and (TEvSelect) are dirty.

Definition 6.8. 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.

Definition 6.9. The head cost $HC(e)$ of a term $e$ is defined in Figure 20.

---

As we mentioned in Section 6.5, the back-translation $[[e']]$ is not exactly the same as the source program $e$: it may be let-expanded. We are, therefore, relying on the property that let-expansion preserves asymptotic complexity (since the resulting evaluation will be larger by, at worst, a constant factor). Since we assume source programs are in A-normal form, however, we already need that property.
**Definition 6.10.** 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 \( \mathcal{D} \) is shallowly \( k \)-bounded if \( HC(\mathcal{D}) \leq k \), and deeply \( k \)-bounded if all its subderivations are shallowly \( k \)-bounded.

\[
\begin{align*}
HC(x) & = 0 \\
HC(x[\overline{a} = \overline{\delta}]) & = 1 \\
HC(\{ select \{ \overline{a}_i = \overline{\delta}_i \Rightarrow e_i \} \}[\overline{a} = \overline{\delta}]) & = 1 + \max_i(HC(e_i)) \\
HC(\{ select \{ \overline{a}_i = \overline{\delta}_i \Rightarrow e_i \} \}) & = 0 \\
HC((e_1, e_2)) & = 0 \\
HC(\text{inl} e) & = 0 \\
HC(\text{fun}^x f(x) = e^x) & = 0 \\
HC(\text{add}(e_1, e_2)) & = 0 \\
HC(\text{nat} e) & = 0 \\
HC(\text{apply}^x (e_1, e_2)) & = 0 \\
HC(\text{case} e \in \{ x_1 \Rightarrow e_1, x_2 \Rightarrow e_2 \}) & = 0 \\
HC(\text{let} x = e^x \in e_2) & = 0 \\
HC(\text{mod} e^C) & = 1 + HC(e^C) \\
HC(\text{read} e_1 \text{ as } \text{in } e^C_2) & = \\
1 + HC(e_1) + HC(e^C_2) & \quad \text{if (for } y \text{ not free in } e_3, e_4): \\
& \quad \text{\( e^C_2 \) has the form } \text{apply}^y(y, e_3) \\
& \quad \text{or case } y \text{ of } \{ x_1 \Rightarrow e_3, x_2 \Rightarrow e_4 \} \\
& \quad \text{or let } r = \text{add}(e_3, y) \text{ in } \text{write}(r) \\
& \quad \text{or read } e_4 \text{ as } \text{in } e^C_2 \text{ in } \text{write}(r) \\
& \quad \text{let } r = \text{add}(y, y_2) \text{ in } \text{write}(r) \\
& \quad \text{otherwise}
\end{align*}
\]

**Fig. 20.** Definition of the “head cost” \( HC(e) \) of a target expression \( e \).

**Theorem 6.11.** If \( \text{trans} (e, \varepsilon) = e' \) then \( e' \) is deeply 1-bounded.

**Theorem 6.12** (Cost Result). Given \( \mathcal{D} :: \rho \vdash e' \Downarrow (p^1 \vdash w) \) where for every subderivation \( \mathcal{D}^* :: \rho^*_1 \vdash e^* \Downarrow (p^*_2 \vdash w^*) \) of \( \mathcal{D} \) (including \( \mathcal{D} \)), \( HC(\mathcal{D}^*) \leq k \), then the number of dirty rule applications in \( \mathcal{D} \) is at most \( \frac{k+1}{k+1} W(\mathcal{D}) \).

The extended soundness result, Theorem 6.14 below, will follow from Theorem 6.13 which generalizes Theorem 6.12. The parts that differ from the uncosted result (Theorem 6.4) are shaded.

**Theorem 6.13** (Costed Evaluation Soundness). If \( \mathcal{D} :: \rho \vdash e \Downarrow (p^1 \vdash w) \) where FLV(\( e \)) \( \subseteq \text{dom}(\rho) \) and \( [\rho] e \) is select-uniform and \( [\rho] e \) is deeply \( k \)-bounded then \( \mathcal{D}' :: [\rho][e] \Downarrow ([\rho][w]) \)

and \( [\rho'][w] \) is deeply \( k \)-bounded

and for every subderivation \( \mathcal{D}^* :: \rho^*_1 \vdash e^* \Downarrow (p^*_2 \vdash w^*) \) of \( \mathcal{D} \) (including \( \mathcal{D} \)).
\[ HC(D^*) \leq HC(e^*) \leq k, \]
and the number of clean rule applications in \( D \) equals \( W(D) \).

**Theorem 6.14.** If \( \text{trans}((e, \varepsilon)) = e' \) and \( D :: \vdash e' \Downarrow (p' \vdash w) \), then \( D :: [e'] \Downarrow v \) where \( W(D') = \Theta(W(D)) \).

### 7 Related work

**Incremental computation.** Self-adjusting computation builds on incremental computation (Ramalingam & Reps 1993). Here we briefly review some techniques. Dependence-graph techniques (Demers et al. 1981) enable a change-propagation algorithm to update the computation. Self-adjusting computation performs a generalized form of this dependence tracking for changeable data. Memoization, an idea that dates back to the late 1950s (Bellman 1957), was first used for incremental computation by Pugh & Teitelbaum (1989) and then by many others (e.g., Abadi et al. 1996). Self-adjusting computation uses a form of memoization that allows reuse of computations that themselves can be incrementally updated, also within an imperative computation model.

Programming-language 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, Ley-Wild et al. 2008, Hammer et al. 2009). DITTO (Shankar & Bodik 2007) shows the benefits of eliminating user annotations in self-adjusting computation and similar incremental computation techniques. By customizing the computation graph data structures for invariant checking programs, they implemented a fully automatic incremental invariant checker that can speed up invariant checks by an order of magnitude. DITTO, however, is domain-specific, only works for certain programs (e.g., functions cannot return arbitrary values) and is unsound in general.

Another approach to incremental computation is partial evaluation (Sundaresh & Hudak 1991, Field & Teitelbaum 1990). Similar to implicit self-adjusting computation, the input is statically partitioned into a fixed portion known at compile time, and a dynamic portion. The partial evaluator will specialize the program with the fixed input, so this part of the input can never change in the runtime. In contrast, in self-adjusting computation, the stable input, although it cannot be changed via change propagation, can still take different values for different initial runs. Although partial evaluation speeds up responses when the dynamic input is modified, the lack of runtime dependency tracking means that the update time may not be as efficient as self-adjusting computation.

Finally, attribute grammars can be viewed as a simple declarative functional language, where programs specify sets of attributes that relate data items whose interdependencies are defined by a tree structure (e.g., the context-sensitive attributes, such as typing information, that decorate an abstract syntax tree). These attributes can be evaluated incrementally. When the attributed tree is changed, the system can sometimes update the affected attributes in optimal time (Reps 1982a, b, Reps & Teitelbaum 1989, Efremidis et al. 1993). The definition of optimality is input-sensitive: it is based on counting of the minimum number of attributes that must be updated after a tree edit occurs; in general this is not known until such an incremental reevaluation is completed. In this sense, the change propagation
algorithm used in these systems is similar to that of self-adjusting computation, but in a less general setting.

**Information flow and constraint-based type inference.** A number of information flow type systems have been developed to check security properties, including the SLam calculus (Heintze & Riecke 1998), JFlow (Myers 1999) and a monadic system (Crary et al. 2005). Our type system uses many ideas from Potthier & 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 2005; 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 & Peyton Jones 1995) and parallel languages (Spoonhower et al. 2008) where it is especially difficult to relate execution time to the source code, as well as in self-adjusting computation (Ley-Wild et al. 2009).

**Functional reactive programming.** Elliott & Hudak (1997) introduced functional reactive programming (FRP), which provides powerful primitives for operating on continuously changing values, called behaviors, and values that change at certain points in time, called discrete events. The approach proposed by Elliott and Hudak, which is known as classical FRP, turned out to be difficult to realize in practice, because it allows expressing computations that depend on future values and because its implementations were prone to so-called time and space leaks. Since its publication, the classical FRP paper started a lively line of research, leading to much work that continues to this day. Due to space limitations, we are able to discuss a relatively small subset of this work. The interested reader can find more details on the FRP literature in recent papers on this topic (Jeffrey 2013; Czaplicki & Chong 2013; Krishnaswami et al. 2012).

Real-time FRP (Wan et al. 2001) proposed techniques for eliminating time and space leaks by introducing signals as a uniform representation of behaviours and events by presenting a restricted language for operating on signals. By further restricting behaviors to change only at events (Wan et al. 2002), event-driven FRP offered a way to reduce redundant recomputation by requiring updates only when an event takes place. The restrictions, however, led to a loss of expressiveness, which subsequent work on arrowized FRP tried to recover (Liu & Hudak 2007; Liu et al. 2009). The work on arrowized FRP shows that much of the expressiveness of classical FRP may be regained while avoiding time and space leaks and while also preserving causality.

Citing difficulties in using arrow combinators and the relatively complex semantics model, other authors pursued research in at least two separate directions. Some research gave up the idea of trying to match the classical FRP semantics. Some work (e.g., Czaplicki & Chong 2013; Cooper & Krishnamurthi 2006) considered only discretely changing values, called signals, and restricts the use of signals to ensure efficient implementation. Other work developed semantics for classical FRP that guarantees causality (Jeffrey 2012; Krishnaswami et al. 2012; Krishnaswami & Benton 2011).
Even though functional reactive programming may be viewed as naturally amenable to incremental computation—it should be possible to incorporate time-varying values into a computation by performing an incremental update—most existing research does not employ incremental computation techniques, focusing instead on taming the time and space consumption of the “one-shot”, re-computation-based approach. Some recent work took steps in the direction of connecting functional programming and incremental computation (Cooper & Krishnamurthi 2006). In their setting, the compiler transparently lifts computations into the reactive domain, which is similar to marking every value as changeable in our implicit self-adjusting computation. Since this can lead to redundant signals in the runtime system, they develop an optimization technique, called “lowering”, which rewrites expressions that depend on non-time-varying values into pure computations. This optimization coarsens the dependency graph and eliminates many redundant “stable” signals. Both their system and our system aim to efficiently translate functional programs into a monadic language. The lowering technique starts with programs with all changeable data, and gradually lowers stable subcomputations. In contrast, we start with a pure source program and lift changeable data into modifiables.

8 Conclusion

This paper presents techniques for translating purely functional programs to programs that can automatically self-adjust in response to dynamic changes to their data. Our contributions include 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 JFP reviewers for their extensive and careful comments, as well as the anonymous ICFP reviewers, and Arthur Charguéraud, for their useful comments on earlier versions of this paper.

A Proof of translation type soundness

First, we need a few simple lemmas.
**Lemma A.1** (Translation of Outer Levels).

\[
[\phi]\tau \text{ O.C. } \text{ if and only if } \parallel \tau\parallel_\phi = \parallel \tau\parallel^C_\phi \mod; \\
[\phi]\tau \text{ O.S. } \text{ if and only if } \parallel \tau\parallel_\phi = \parallel \tau\parallel^C_\phi.
\]

**Proof**

Case analysis on \([\phi]\tau\), using the definitions of \(-\text{ O.S.}, -\text{ O.C.}\), \(-\parallel\phi\) and \(-\parallel\parallel_\phi^C\).

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

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

**Proof**

By induction on the given derivation.

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

1. If \(\tau''\) O.S. then \(\tau' = \tau''\).
2. If \(\tau''\) O.C. then either \(\tau' = \tau''\) or \(\tau' = \parallel \tau''\parallel^{\mathcal{S}}\).

**Proof**

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

- **Case** (subInt): \(\tau' = \text{int}^{\delta'}\) and \(\tau'' = \text{int}^{\delta''}\), where \(\delta' < \delta''\).
  1. If \(\tau''\) O.S. then \(\delta'' = \mathcal{S}\). So \(\tau' = \tau''\).
  2. If \(\tau''\) O.C. then \(\delta'' = \mathcal{C}\). If \(\delta' = \mathcal{S}\) then \(\parallel \tau''\parallel^{\mathcal{S}} = \text{int}^{\delta''} = \text{int}^{\delta'} = \tau'\); if \(\delta' = \mathcal{C}\) then \(\parallel \tau''\parallel^{\mathcal{C}} = \text{int}^{\delta''} = \tau'\).

- **Case** (subProd):
  1. By definition of \(\equiv\), \(\tau' = \tau''\).
  2. \(\tau''\) O.C. is impossible.

- **Case** (subSum):
  1. If \(\tau''\) O.S. then \(\tau'' = (\tau''_1 + \tau''_2)^{\bar{\delta}}\). By inversion on (subSum), \(\tau' = (\bar{\tau'}_1 + \bar{\tau'}_2)^{\bar{\delta}}\). By definition of \(\equiv\), \(\tau''_1 = \bar{\tau'}_1^{\bar{\delta}}\) and \(\tau''_2 = \bar{\tau'}_2^{\bar{\delta}}\). Therefore \(\tau' = \tau''\).
  2. If \(\tau''\) O.C. then \(\tau'' = (\tau''_1 + \tau''_2)^{\bar{\delta}}\). By inversion on (subSum), \(\tau' = (\bar{\tau'}_1 + \bar{\tau'}_2)^{\bar{\delta}}\). By definition of \(\equiv\), \(\tau''_1 = \bar{\tau'}_1^{\bar{\delta}}\) and \(\tau''_2 = \bar{\tau'}_2^{\bar{\delta}}\). If \(\bar{\delta} = \mathcal{S}\) then \(\parallel \tau''\parallel^{\mathcal{S}} = (\tau''_1 + \tau''_2)^{\bar{\delta}}\), which is equal to \(\tau'\). If \(\bar{\delta} = \mathcal{C}\) then \(\parallel \tau''\parallel^{\mathcal{C}} = (\tau''_1 + \tau''_2)^{\bar{\delta}} = (\tau'_1 + \tau'_2)^{\bar{\delta}} = \tau'\).

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

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

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

1. there exists \(e^{\mathcal{S}}\) such that \(\phi \Gamma \vdash e : [\phi]\tau \rightarrow e^{\mathcal{S}}\) and \(\vdash \parallel \parallel\phi\parallel\parallel S \vdash e^{\mathcal{S}} : \parallel \tau\parallel\phi\),
   and if \(e\) is a value, then \(e^{\mathcal{S}}\) is a value;
(2) there exists $e^C$ such that $[\phi] \Gamma \vdash e : [\phi] \tau \Rightarrow e^C$ and $\vdash :||\Gamma||_{\phi} e^C : ||\tau||_{\phi}^C$.

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 $S$ mode, typing in the $S$ mode, translation in the $C$ mode, and typing in the $C$ mode), and often arrive at some of them early, we indicate them with “$\leadsto$”.

“Part (1)” and “Part (2)” refer to the two parts of the conclusion: (1) “there exists $e^S \ldots$” and (2) “there exists $e^C \ldots$”. In some cases, it is convenient to prove these simultaneously, so we sometimes annotate the “$\leadsto$” symbol to clarify which part is being proved:

\[(1)\Rightarrow \vdash :||\Gamma||_{\phi} \vdash (\text{fun}^C f(x) = \cdot) : ||\tau||_{\phi}^C \text{ By (TFun)}\]

This information can also be read off from the turnstile: $\vdash_S$ means part (1), and $\vdash_C$ means part (2).

- **Case**

  $C; \Gamma \vdash e : \tau$ (SInt)

  Part (1): Let $e^S$ be $n$.

  $[\phi] \Gamma \vdash n : \text{int}^S \Rightarrow n$ By (Int)

  $\Rightarrow \vdash :||\Gamma||_{\phi} \vdash n : \text{int}^S \text{ By (TInt)}$

  $\Rightarrow \vdash :||\Gamma||_{\phi} \vdash n : \text{int}^S : ||\tau||_{\phi}^C$ By $\tau = \text{int}^S$

  Part (2): Let $e^C$ be let $r=n$ in write$(r)$.

  $[\phi] \Gamma \vdash n : \text{int}^C \Rightarrow n$ Above

  $[\phi] \Gamma \vdash n : \text{int}^C \Rightarrow \text{let } r=n \text{ in write}(r)$ By (Write)

  $\Rightarrow \vdash :||\Gamma||_{\phi} \vdash n : \text{int}^C \text{ By (TInt)}$

  $\Rightarrow \vdash :||\Gamma||_{\phi} \vdash r : \text{int}^C$ By (TVar)

  $\Rightarrow \vdash :||\Gamma||_{\phi} \vdash \text{write}(r) : \text{int}$ By (TWrite)

  $\Rightarrow \vdash :||\Gamma||_{\phi} \vdash \text{let } r=n \text{ in write}(r) : \text{int}$ By (TLet)

  $\Rightarrow \vdash :||\Gamma||_{\phi} \vdash e^C : \text{int}$ By def. of $e^C$

  $\Rightarrow \vdash :||\Gamma||_{\phi} \vdash e^C : ||\tau||_{\phi}^C$ By $\tau = \text{int}^C$

- **Case**

  $\Gamma(x) = \forall \bar{\alpha}(D). \tau_0$ $C \vdash \exists \bar{\beta}. [\bar{\beta} / \bar{\alpha}]D$

  $C \land D; \Gamma \vdash e : [\bar{\beta} / \bar{\alpha}]\tau_0$ (SVar)

  Part (1): Let $e^S$ be $x[\bar{\alpha} = \bar{\delta}]$. 

Implicit self-adjusting computation for purely functional programs

\( \Gamma(x) = \forall \bar{\alpha}[D], \tau_0 \)  

Premise

\((\phi|\Gamma)(x) = [\phi|\forall \bar{\alpha}[D], \tau_0] = \forall \bar{\alpha}[[\phi|D], \phi]\\) \(\tau_0\)  

By def. of substitution

\[\phi|\Gamma \vdash x: [\delta/\bar{\alpha}](\phi|\tau_0) \rightarrow \emptyset x[\bar{\alpha} = \delta] \]  

By (Var)

\[\phi|\Gamma \vdash x: [\phi][\delta/\bar{\alpha}]\tau_0 \rightarrow \emptyset x[\bar{\alpha} = \delta] \]  

\(\bar{\delta}\) closed and \(\bar{\alpha} \cap \text{dom}(\phi) = \emptyset\)

Intermediate subst.

\[\phi|\Gamma \vdash x: [\phi][(\beta/\bar{\alpha})\tau_0] \rightarrow \emptyset x[\bar{\alpha} = \delta] \]  

Intermediate subst.

\[\phi(\hat{\beta}) = \bar{\delta} \]

Part (2), subcase (a) where \([\phi]\tau\) O.S.: Let \(e^C = \text{let } r = x[\bar{\alpha} = \delta] \text{ in write}(r)\).

\[\phi|\Gamma \vdash x: [\phi]\tau \rightarrow x[\bar{\alpha} = \delta] \]  

Above

\[\phi|\Gamma \vdash x: [\phi]\tau \rightarrow \text{let } r = x[\bar{\alpha} = \delta] \text{ in write}(r) \]  

By (Write)

\[\phi|\Gamma \vdash e: [\phi]\tau \rightarrow e^C \]  

By \(e = x\) and def. of \(e^C\)

\[\phi|\Gamma \vdash \text{let } r = x[\bar{\alpha} = \delta] \text{ in write}(r): [\phi]\tau \rightarrow \]  

By (TVar)

\[\phi|\Gamma \vdash \text{write}(r): [\phi]\tau \rightarrow \]  

By (TWrite)

\[\phi|\Gamma \vdash \text{let } r = x[\bar{\alpha} = \delta] \text{ in write}(r): [\phi]\tau \rightarrow \]  

By (TVar)

\[\phi|\Gamma \vdash \text{let } r = x[\bar{\alpha} = \delta] \text{ in write}(r): [\phi]\tau \rightarrow \]  

By (TWrite)

\[\phi|\Gamma \vdash \text{let } r = x[\bar{\alpha} = \delta] \text{ in write}(r): [\phi]\tau \rightarrow \]  

By (TPV ar)

\[\phi|\Gamma \vdash \text{let } r = x[\bar{\alpha} = \delta] \text{ in write}(r): [\phi]\tau \rightarrow \]  

By (TPV ar)

Part (2), subcase (b) where \([\phi]\tau\) O.S.: Let \(e^C = \text{let } r = e^S \text{ in read } r \text{ as } r' \text{ in write}(r')\).

\[\phi|\Gamma \vdash x: [\phi]\tau \rightarrow e^C \]  

Above

\[\phi|\Gamma \vdash \text{let } r = e^S \text{ in read } r \text{ as } r' \text{ in write}(r'): [\phi]\tau \rightarrow \]  

By (ReadWrite)

\[\phi|\Gamma \vdash e^C: [\phi]\tau \rightarrow \]  

By (ReadWrite)

\[\phi|\Gamma \vdash \text{let } r = e^S \text{ in read } r \text{ as } r' \text{ in write}(r'): [\phi]\tau \rightarrow \]  

By (TPV ar)

\[\phi|\Gamma \vdash \text{let } r = e^S \text{ in read } r \text{ as } r' \text{ in write}(r'): [\phi]\tau \rightarrow \]  

By (TPV ar)

\[\phi|\Gamma \vdash \text{let } r = e^S \text{ in read } r \text{ as } r' \text{ in write}(r'): [\phi]\tau \rightarrow \]  

By (TPV ar)
\( \| \tau \|_\phi = \| \tau \|_\phi^C \mod \) By Lemma A.1

\[ \vdash \| \Gamma \|_\phi \vdash S e^S : \| \tau \|_\phi^C \mod \] By above eqn.

- Case

\( C; \Gamma \vdash e v_1 : \tau_1 \quad C; \Gamma \vdash e v_2 : \tau_2 \) \( \text{(SPair)} \) 

\( C; \Gamma \vdash (v_1, v_2) : (\tau_1 \times \tau_2)^S \) 

- Part (1), stable mode translation:

\( [\phi] \Gamma \vdash v_1 : [\phi] \tau_1 \xrightarrow{\phi} v_1 \) By i.h.

\[ \vdash \| \Gamma \|_\phi \vdash_S v_1 : \| \tau_1 \|_\phi \] "

\( [\phi] \Gamma \vdash v_2 : [\phi] \tau_2 \xrightarrow{\phi} v_2 \) By i.h.

\[ \vdash \| \Gamma \|_\phi \vdash_S v_2 : \| \tau_2 \|_\phi \] "

Let \( e^S = (v_1, v_2) \).

\[ [\phi] \Gamma \vdash e : [\phi]((\tau_1 \times \tau_2)^S) \xrightarrow{\phi} e^S \] and \( e^S \) is a value By def. of subst. and \( e^S = (v_1, v_2) \)

\[ \vdash \| \Gamma \|_\phi \vdash_S (v_1, v_2) : \| \tau_1 \|_\phi \times \| \tau_2 \|_\phi \] By (TPair)

\[ \vdash \| \Gamma \|_\phi \vdash_S e^S : \| (\tau_1 \times \tau_2)^S \|_\phi \] By def. of \( \| - \|_\phi \)

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

\[ [\phi] \Gamma \vdash e : [\phi] \tau \xrightarrow{\phi} e^S \] Above O.S. By definition of O.S.

\[ [\phi] \Gamma \vdash e : [\phi] \tau \xrightarrow{\phi} e^S \] let \( r = e^S \) in \( \text{write}(r) \) By (Write)

\[ \vdash \| \Gamma \|_\phi \vdash_S e^S : \| \tau \|_\phi \] Above

\[ \vdash \| \Gamma \|_\phi \vdash_S \| \tau \|_\phi \vdash_R r : \| \tau \|_\phi \] By (TPVar)

\[ \vdash \| \Gamma \|_\phi \vdash_S \| \tau \|_\phi \vdash_C \text{write}(r) : \| \tau \|_\phi \] By (TWrite)

\[ \| \tau \|_\phi = \| \tau \|_\phi^C \] By Lemma A.1

\[ \vdash \| \Gamma \|_\phi \vdash_C \text{write}(r) : \| \tau \|_\phi^C \] By above equality

**Case**

\[ C; \Gamma, x : \tau_1, f : (\tau_1 \xrightarrow{\phi} \tau_2)^S \vdash e f(x) : \tau_2 \] \( \text{(SFun)} \)

(a) Suppose \( [\phi] e = S \).
Implicit self-adjusting computation for purely functional programs

Let \( e^S \) be \( \text{fun}^S f(x) = e' \).

\( (1) \) Suppose \( \text{fun}^S f(x) = e' \) and \( e^S \) is a value.

\[ \vdash \|\Gamma\|_\phi, x: \|\Gamma\|_\phi, f: \|\Gamma\|_\phi \rightarrow \|\Gamma\|_\phi \vdash e': \|\Gamma\|_\phi \]  

Let \( e^C \) be \( \text{let} \quad r = e^S \quad \text{in} \quad \text{write}(r) \).

\( (2) \) Suppose \( \text{fun}^C f(x) = e' \).

\[ \vdash \|\Gamma\|_\phi, r: \|\Gamma\|_\phi \vdash \|\Gamma\|_\phi \]  

(b) Suppose \( \text{fun}^C f(x) = e' \) and \( e^S \) is a value.

\[ \vdash \|\Gamma\|_\phi, x: \|\Gamma\|_\phi, f: (\|\Gamma\|_\phi \rightarrow \|\Gamma\|_\phi \rightarrow \|\Gamma\|_\phi) \vdash e': \|\Gamma\|_\phi \]  

Let \( e^S \) be \( \text{fun}^S f(x) = e' \).

\[ \vdash \|\Gamma\|_\phi, \text{let} \quad r = e^S \quad \text{in} \quad \text{write}(r) \]  

\( (SSumLeft) \)

Part (1):

\[ \vdash C; \Gamma \vdash v: \tau ]  

Subderivation

\[ \vdash \|\Gamma\|_\phi \vdash v: \|\Gamma\|_\phi \]  

Let \( e^S = \text{inl} v \).

\[ \vdash \|\Gamma\|_\phi \vdash \text{inl} v: \|\Gamma\|_\phi \]  

By (SumLeft)

\[ \vdash C; \Gamma \vdash e: \tau ]  

By (SumLeft)

\[ \vdash \|\Gamma\|_\phi \vdash \tau ]  

By (TSumLeft)
Part (2): Similar to (SPair), using \((\tau_1 + \tau_2)^S\) O.S.

\[
\begin{array}{c}
\text{Case} \\
\begin{array}{c}
\text{C; } \Gamma \vdash e \cdot x : (\tau_1 \times \tau_2)^\delta \\
\text{C; } \Gamma \vdash \delta \leq \varepsilon
\end{array}
\end{array}
\]

(SFat)

— Suppose \([\phi]\delta = \varepsilon\).

Part (1):

\[
\begin{array}{c}
\text{C; } \Gamma \vdash e \cdot x : (\tau_1 \times \tau_2)^\delta \\
\text{Subderivation} \\
[\phi] \Gamma \vdash x : ([\phi] \tau_1 \times [\phi] \tau_2)^S \rightarrow \chi \\
\vdash [\chi] \phi \rightarrow S \vdash [\tau_1] \phi \times [\tau_2] \phi \\
\mapsto [\phi] \Gamma \vdash e : [\phi] \tau_1 \rightarrow \text{fst} \chi \\
\text{By (Fst)}
\end{array}
\]

Let \(e^\phi = \text{fst} \chi\).

\[
\begin{array}{c}
\vdash [\chi] \phi \rightarrow S \vdash \text{fst} \chi : [\tau_1] \phi \\
\text{By (TFst)}
\end{array}
\]

Part (2): Similar to (SVar):

— If \(\tau_1\) O.S., let \(e^C\) be \(\text{let } r = \text{fst} \chi \text{ in write}(r)\) and apply rule (Write).

— If \(\tau_1\) O.C., let \(e^C\) be \(\text{let } r = \text{fst} \chi \text{ in read as } r' \text{ in write}(r')\) and apply rule (ReadWrite).

— Suppose \([\phi]\delta = \chi\). 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 \(e^C\) be \(\text{read } \chi \text{ as } x'\) in \(r = \text{fst} x' \text{ in write}(r)\) and apply rule (Read) with (LFst).

\[
\begin{array}{c}
\ldots r : [\tau_1] \rightarrow S \vdash r : [\tau_1] \\
\text{By (TPVar)}
\end{array}
\]

\[
\begin{array}{c}
\ldots r : [\tau_1] \rightarrow C \text{ write}(r) : [\tau_1] \\
\text{By (TWrite)}
\end{array}
\]

\[
\begin{array}{c}
\ldots r : [\tau_1] \rightarrow C \text{ write}(r) : [\tau_1] \rightarrow C \\
\text{By i.h.}
\end{array}
\]

Let \(r = \text{fst } x' \text{ in write}(r)\) and apply rule (TWrite).

\[
\begin{array}{c}
\Gamma \vdash x' : ([\tau_1] \times [\tau_2])^C \\
\text{By def. of } \rightarrow \\
\Gamma \vdash x' : ([\tau_1] \times [\tau_2])^C \\
\text{By (TRead)}
\end{array}
\]

— If \(\tau_1\) O.C., then \([\tau_1] = \tau_1' \mod\) for some \(\tau_1'\).

Let \(e^C\) be \(\text{read } \chi \text{ as } x'\) in \(r = \text{fst } x' \text{ in read as } r' \text{ in write}(r')\) and apply rule (Read) with (LFst).

\[
\begin{array}{c}
\ldots r' : [\tau_1'] \rightarrow C \text{ write}(r') : [\tau_1'] \\
\text{By (TPVar), (TWrite)}
\end{array}
\]

\[
\begin{array}{c}
\ldots r' : [\tau_1'] \rightarrow C \text{ write}(r') : [\tau_1] \rightarrow C \\
\text{By i.h.}
\end{array}
\]

The remaining steps are similar to the \(\tau_1\) O.S. subcase immediately above.
Case  
\[ C; \Gamma \vdash e_1 : \tau' \quad C; \Gamma, x : \tau'' \vdash e_2 : \tau \quad C \vdash \tau' <: \tau'' \]
\[ C; \Gamma \vdash e \text{ let } x = e_1 \text{ in } e_2 : \tau \quad (\text{SLetE}) \]

(a) Subcase for \([\phi]\tau'' \text{ O.C.}\)

\[ C; \Gamma \vdash e_1 : \tau' \quad \text{Subderivation} \]
\[ [\phi] \Gamma \vdash e_1 : [\phi] \tau' \xrightarrow{\beta} e^C \quad \text{By i.h.} \]
\[ \vdash [\Gamma]_{\phi} \vdash e^C : \| \tau' \|_{\phi}^C \quad n \]

\[ C \vdash \tau' <: \tau'' \quad \text{Premise} \]
\[ [\phi] \tau' <: [\phi] \tau'' \quad \text{By Lemma}[A.2] \]

\[ C \vdash \tau' \equiv \tau'' \quad \text{Premise} \]
\[ [\phi] \tau' \equiv [\phi] \tau'' \quad \text{By Lemma}[A.2] \]
\[ [\phi] \tau'' \text{ O.C.} \]
\[ [\phi] \tau' = [\phi] \tau'' \text{ or } [\phi] \tau' = \| [\phi] \tau'' \|^S \quad \text{By Lemma}[A.3](2) \]

If \([\phi] \tau' = [\phi] \tau'' \) then:
\[ [\phi] \Gamma \vdash e_1 : [\phi] \tau' \xrightarrow{\beta} \mod e^C \quad \text{By (Mod)} \]
\[ [\phi] \Gamma \vdash e_1 : [\phi] \tau'' \xrightarrow{\beta} \mod e^C \quad \text{By } [\phi] \tau' = [\phi] \tau'' \]

Otherwise, \([\phi] \tau'' \equiv [\phi] \tau'' \)
\[ [\phi] \Gamma \vdash e_1 : [\phi] \tau'' \xrightarrow{\beta} \mod e^C \quad \text{By (Lift)} \]

Now we have the same judgment no matter which equation Lemma\([A.3]\) gave us.

\[ \vdash [\Gamma]_{\phi} \vdash e^C : \| \tau' \|_{\phi}^C \quad \text{Above} \]
\[ \vdash [\Gamma]_{\phi} \vdash \mod e^C : \| \tau'' \|_{\phi}^C \quad \text{mod} \]

or \[ \vdash [\Gamma]_{\phi} \vdash \mod e^C : \| \tau'' \|_{\phi}^C \quad \text{mod} \]
\[ \vdash [\phi] \tau'' \text{ O.C.} \quad \text{By def. of } [\phi] \tau'' \text{ or copying} \]
\[ [\phi] \tau'' \text{ O.C.} \quad \text{Subcase (a) assumption} \]
\[ \| \tau'' \|_{\phi}^C = \| \tau'' \|_{\phi} \quad \text{mod} \quad \text{By Lemma}[A.1] \]

\[ \vdash [\Gamma]_{\phi} \vdash \mod e^C : \| \tau'' \|_{\phi} \quad \text{mod} \]

(b) Subcase for \([\phi]\tau'' \text{ O.S.}\)

\[ C; \Gamma \vdash e_1 : \tau' \quad \text{Subderivation} \]
\[ [\phi] \Gamma \vdash e_1 : [\phi] \tau' \xrightarrow{\beta} e^S \quad \text{By i.h.} \]
\[ \vdash [\Gamma]_{\phi} \vdash e^S : \| \tau' \|_{\phi} \quad n \]
\[ [\phi] \tau'' \text{ O.S.} \quad \text{Subcase (b) assumption} \]
\[ [\phi] \tau'' = [\phi] \tau' \quad \text{By Lemma}[A.3](1) \]
\[ \vdash [\Gamma]_{\phi} \vdash e^S : \| \tau'' \|_{\phi} \quad \text{By above equation} \]

For both subcases, we have:
C; Γ, x : τ’’ ⊢ e_2 : τ  
Subderivation

[φ]Γ, x : [φ]τ’’ ⊢ e_2 : [φ]τ’’ ⊢ e_2^S  
By i.h. and def. of subst.

::Γ[φ], x : ||τ’’||φ ⊢ e_2^S : ||τ’’||φ  
By i.h. and def. of ||−||φ

(1)•w  
[φ]Γ ⊢ e : [φ]τ ⊢ e^S in e_2^S  
By (LetE)

(1)•w  
::Γ[φ] ⊢ x = e^S in e_2^C : ||τ’’||φ  
By (TLet)

C; Γ, x : τ’’ ⊢ e_2 : τ  
Subderivation

[φ]Γ, x : [φ]τ’’ ⊢ e_2 : [φ]τ’’ ⊢ e_2^C  
By i.h. and def. of subst.

::Γ[φ], x : ||τ’’||φ ⊢ e_2^C : ||τ’’||φ^C  
By i.h. and def. of ||−||φ

(2)•w  
[φ]Γ ⊢ e : [φ]τ ⊢ e^C in e_2^C  
By (LetE)

(2)•w  
::Γ[φ] ⊢ x = e^S in e_2^C : ||τ’’||φ^C  
By (TLet)

\[ C; Γ, x : \forall \bar{\alpha}[D], \tau’’ ⊢ e_2 : \tau \quad C ⊢ τ’ < τ’’ \]

\[ C ∧ ∃\bar{\alpha}. D; Γ ⊢ x = v_1 in e_2 : τ \]  
(SLetV)

For all \( \bar{\delta}_i \) such that \( \bar{\alpha} = \bar{\delta}_i \models D \):

— (a) Suppose \([φ][\bar{\delta}_i/\bar{\alpha}][τ’’] O.S., that is, this \( i \)th monomorphic instance is outer-
stable, and will not need a \textbf{mod} in the target.

\[
C ∧ D; Γ ⊢ S v_1 : \tau' \\
\bar{\alpha} ∩ FV(C, Γ) = \emptyset \\
C ∧ D; [\bar{\delta}_i/\bar{\alpha}]Γ ⊢ S v_1 : [\bar{\delta}_i/\bar{\alpha}]τ' \\
[φ]([\bar{\delta}_i/\bar{\alpha}]Γ) ⊢ v_1 : [φ][[\bar{\delta}_i/\bar{\alpha}]τ'] ⊢ v_2  \\
\bar{\alpha} \text{ not free in } Γ \\
[φ]Γ ⊢ v_1 : [φ][[\bar{\delta}_i/\bar{\alpha}]τ'] ⊢ v_2  \\
::Γ[φ] ⊢ S v_1 : ||[\bar{\delta}_i/\bar{\alpha}]τ'||φ  
\]

Let \( e_2 \) be \( v_2 \).
Above:

(b) Suppose \( \phi \parallel \delta / \alpha \parallel \tau'' \) O.C., that is, this \( i \)th monomorphic instance is out-changeable, and therefore needs a \texttt{mod} in the target.

\[
C \mid D; \Gamma \vdash_{S} v_{1} : \tau' \quad \text{Subderivation}
\]
\[
\alpha \cap FV(C, \Gamma) = \emptyset \quad \text{Premise}
\]
\[
C \mid D; [\delta / \alpha \parallel \Gamma] \vdash_{S} v_{1} : [\delta / \alpha \parallel \tau'] \quad \text{By Lemma A.2}
\]
\[
[\phi](\delta / \alpha \parallel \Gamma) \vdash v_{1} : [\phi](\delta / \alpha \parallel \tau') \rightarrow e_{C} \quad \text{By i.h., using the lemma's guarantee about derivation height}
\]
\[
::\|\Gamma\|_{\phi} \vdash_{C} e_{C} : [\delta / \alpha \parallel \tau'] \rightarrow^{C} \text{By i.h. and def. of } \| - \|^{C}
\]
\[
[\phi](\delta / \alpha \parallel \tau') \rightarrow [\phi](\delta / \alpha \parallel \tau'')^{|S} \quad \text{or } \ldots = [\phi](\delta / \alpha \parallel \tau'' \quad \text{By Lemma A.3 (2))}
\]

If \([\phi](\delta / \alpha \parallel \tau') \rightarrow [\phi](\delta / \alpha \parallel \tau'')^{|S} \quad \text{then:}
\]
\[
[\phi](\delta / \alpha \parallel \Gamma) \vdash v_{1} : [\phi](\delta / \alpha \parallel \tau') \rightarrow e_{C} \quad \text{By } [\phi](\delta / \alpha \parallel \tau'')^{|S} = [\phi](\delta / \alpha \parallel \tau') \quad \text{By (Lift)}
\]
\[
[\phi](\delta / \alpha \parallel \Gamma) \vdash v_{1} : [\phi](\delta / \alpha \parallel \tau') \rightarrow e_{C} \quad \text{By } [\phi](\delta / \alpha \parallel \tau'')^{|S} = [\phi](\delta / \alpha \parallel \tau') \quad \text{mod } e_{C} \quad \text{By (Mod)}
\]

Otherwise, \([\phi](\delta / \alpha \parallel \tau') = [\phi](\delta / \alpha \parallel \tau'') \quad \text{or } \ldots = [\phi](\delta / \alpha \parallel \tau'' \quad \text{By Lemma A.3 (2))}
\]
\[
[\phi](\delta / \alpha \parallel \Gamma) \vdash v_{1} : [\phi](\delta / \alpha \parallel \tau') \rightarrow e_{C} \quad \text{By } [\phi](\delta / \alpha \parallel \tau'') = [\phi](\delta / \alpha \parallel \tau') \quad \text{mod } e_{C} \quad \text{By (Mod)}
\]

Now, through either (Lift) or (Mod), we have obtained the same judgment.

Let \( e_{2} \) be \texttt{mod} \( e_{C} \).
This ends the “for all \( \vec{y} \)” above. We now have translation judgments for each instance, and target typings for each \( e_i \) and associated variable \( y_i \).

\[
C; \Gamma, x: \forall \alpha[D]. \tau'' \vdash e_2 : \tau \quad \text{Subderivation}
\]
\[
[\phi] \Gamma, x: \forall \alpha[D]. \tau'' \vdash e_2 : [\phi] \tau \rightarrow e_2^\delta \quad \text{By i.h. and def. of substitution}
\]
\[
[\phi] \Gamma, x: \forall \alpha[D]. \tau'' \vdash e_2 : [\phi] \tau \rightarrow e_2^\delta'' \quad \text{"}
\]
\[
\vdash [\Gamma]_\phi, \Gamma, x: \forall \alpha[D]. [\phi] \tau'' \vdash e_2^\delta : \| \tau \|_\phi \quad \text{By i.h. and def. of } - \| \phi \|
\]
\[
\vdash [\Gamma]_\phi, \Gamma, x: \forall \alpha[D]. [\phi] \tau'' \vdash e_2^\delta : \| \tau \|_{- \phi} \quad \text{"}
\]

Let \( e_0^\delta \) be let \( x = \text{select } \{ \vec{y}_i = e_i \} \), in \( e_2^\delta \), and let \( e_0^\epsilon \) be let \( x = \text{select } \{ \vec{y}_i = e_i \} \), in \( e_2^\epsilon \).

Case

\[
C; \Gamma \vdash_S x_1 : (\tau_1 \rightarrow e^\delta_0) \quad C; \Gamma \vdash_S x_2 : \tau_1 \quad C \vdash e' = \epsilon \\
C; \Gamma \vdash_S \text{apply}(x_1, x_2) : \tau \quad \text{(SApp)}
\]

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

— **Subcase “S-S”** for \([\phi]e' = S, [\phi]\delta = S\).

Part (1):

\[
C; \Gamma \vdash_S x_2 : \tau_1 \quad \text{Subderivation}
\]
\[
[\phi] \Gamma \vdash x_2 : [\phi] \tau_1 \rightarrow x_2 \quad \text{By i.h.}
\]
\[
\vdash [\Gamma]_\phi, \Gamma \vdash x_2 : [\tau_1]_\phi \quad "
\]
\[
C; \Gamma \vdash_S x_1 : (\tau_1 \rightarrow e^\delta_0) \quad \text{Subderivation}
\]
Implicit self-adjusting computation for purely functional programs

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

\[
\begin{align*}
\phi \Gamma & \vdash x_1 : [\phi] \tau \xrightarrow{S} x_1 & \text{By i.h.} \\
\vdash \Gamma \| \vdash x_1 : \| (\tau_1 \xrightarrow{S} \tau) \| \phi & \text{By def. of } \| \| \phi \text{ and substitution} \\
\vdash \Gamma \| \vdash x_1 : \| ([\phi] \tau_1 \xrightarrow{\phi \delta} \phi) \| & \text{Subcase S-S assumption} \\
\vdash \Gamma \| \vdash x_1 : \| \tau_1 \| \phi & \text{By def. of } \| \| \\
\end{align*}
\]

Part (2):

(a) Suppose \([\phi] \tau \text{ O.S.}\)

\[
\begin{align*}
\phi \Gamma & \vdash e : [\phi] \tau \xrightarrow{\phi} \text{let } r = e^S \text{ in write}(r) & \text{By (Write)} \\
\vdash \Gamma \| \phi, r : \| \tau \| \phi & \text{By (TPVar)} \\
\vdash \Gamma \| \phi, r : \| \tau \| \phi \vdash \phi \tau \text{ O.S.} & \text{Subcase (a) assumption} \\
\vdash \Gamma \| \phi, r : \| \tau \| \phi & \text{By Lemma A.1} \\
\end{align*}
\]

(b) Suppose \([\phi] \tau \text{ O.C.}\)

\[
\begin{align*}
\phi \Gamma & \vdash e : [\phi] \tau \xrightarrow{\phi} \text{let } r = e^S \text{ in read } r \text{ as } r' \text{ in write}(r') & \text{By (ReadWrite)} \\
\vdash \Gamma \| \phi, r : \| \tau \| \phi \vdash \phi \tau \text{ O.C.} & \text{Subcase (b) assumption} \\
\vdash \Gamma \| \phi, r : \| \tau \| \phi \vdash \phi \tau \text{ O.C.} & \text{By Lemma A.1} \\
\vdash \Gamma \| \phi, r : \| \tau \| \phi \vdash \phi \tau \text{ O.C.} & \text{By (TPVar)} \\
\vdash \Gamma \| \phi, r : \| \tau \| \phi \vdash \phi \tau \text{ O.C.} & \text{By (TWrite)} \\
\vdash \Gamma \| \phi, r : \| \tau \| \phi \vdash \phi \tau \text{ O.C.} & \text{By (TRead)} \\
\vdash \Gamma \| \phi, r : \| \tau \| \phi \vdash \phi \tau \text{ O.C.} & \text{By (TLet)} \\
\end{align*}
\]

Subcase “\( \text{C-S} \)” where \([\phi] e' = \text{C} \) and \([\phi] \delta = S \).

Part (2):

\[
\begin{align*}
[\phi] \Gamma & \vdash x_1 : [\phi] \tau \xrightarrow{S} x_1 \quad \text{From subcase S-S above} \\
[\phi] \Gamma & \vdash x_2 : [\phi] \tau \xrightarrow{S} x_2 \quad \text{From subcase S-S above} \\
\text{Let } e^C = \text{apply}^C(x_1, x_2). \\
\end{align*}
\]
\[ [\phi] \vdash e : [\phi] \tau \rightarrow \text{apply}^C(x_1, x_2) \quad \text{By (App)} \]
\[ [\phi] \vdash e : [\phi] \tau \rightarrow e^C \quad \text{By i.h.} \]
\[ [\phi] \vdash e : [\phi] \tau \rightarrow [\phi] \tau^\delta \quad \text{By def. of } ||-||^C \]
\[ [\phi] \vdash e : [\phi] \tau \rightarrow [\phi] \tau^\delta \quad \text{By subcase } C-S \text{ assumption} \]
\[ [\phi] \vdash e : [\phi] \tau \rightarrow [\phi] \tau^\delta \quad \text{By def. of } ||-||^C \]
\[ [\phi] \vdash e : [\phi] \tau \rightarrow [\phi] \tau^\delta \quad \text{From subcase } S-S \text{ above} \]

\[ [\phi] \vdash e \rightarrow e^C : [\tau]_{\phi}^C \quad \text{By (TApp)} \]

Part (1):
\[ [\phi] \vdash O.C. \quad \text{By } [\phi] e' = C \text{ and barring } (\tau'_1 \rightarrow \tau'_2)^\delta \text{ where } \tau'_2 \text{ O.S.} \]

\[ [\phi] \vdash e : [\phi] \tau \rightarrow e^C \quad \text{Above} \]
\[ [\phi] \vdash e : [\phi] \tau \rightarrow \text{mod } e^C \quad \text{By (Mod)} \]
\[ [\phi] \vdash e : [\phi] \tau \rightarrow e^C : [\tau]_{\phi}^C \quad \text{Above} \]
\[ [\phi] \vdash \text{mod } e^C : [\tau]_{\phi}^C \quad \text{By (TMod)} \]
\[ [\phi] \vdash O.C. \quad \text{Above} \]
\[ [\phi] \vdash \text{mod } e^C : [\tau]_{\phi}^C \quad \text{By Lemma A.1} \]

Subcase “C-C” where \([\phi] e' = C \text{ and } [\phi] \delta = C:\)

Part (2):
\[ (\Gamma, \lambda') : (\tau_1 \rightarrow \tau)^{\delta}(\lambda') = \forall \alpha[\text{true}].(\tau_1 \rightarrow \tau)^{\delta} \quad \text{By def. of } \Gamma \]
\[ C \vdash \exists \alpha. \text{true} \quad \text{By def. of } ||-|| \]
\[ C ; \Gamma, \lambda' : (\tau_1 \rightarrow \tau)^{\delta} \vdash \lambda' : (\tau_1 \rightarrow \tau)^{\delta} \quad \text{By (SVar)} \]
\[ [\phi] \vdash \lambda' : (\tau_1 \rightarrow \tau)^{\delta} \vdash \lambda' : (\tau_1 \rightarrow \tau)^{\delta} \quad \text{By (Var)} \]
\[ [\phi] \vdash \lambda' : (\tau_1 \rightarrow \tau)^{\delta} \vdash \lambda' : (\tau_1 \rightarrow \tau)^{\delta} \quad \text{By extending } \Gamma \]
\[ [\phi] \vdash \lambda' : (\tau_1 \rightarrow \tau)^{\delta} \vdash \text{apply}(\lambda', \lambda) : [\phi] \tau \rightarrow \text{apply}^C(\lambda', \lambda) \quad \text{By (App)} \]
\[ [\phi] \vdash \lambda' : (\tau_1 \rightarrow \tau)^{\delta} \vdash e : [\phi] \tau \rightarrow \text{apply}^C(\lambda', \lambda) \quad \text{By def. of subst., } ||-||^{\delta} \]
\[ [\phi] \vdash e \rightarrow (x_1 \gg \lambda' : ([\phi] \tau_1 \rightarrow [\phi] \tau)^{\delta} \vdash \text{apply}(\lambda', \lambda)) \quad \text{By (LApply)} \]
\[ [\phi] \vdash \lambda' : [\phi] \tau \rightarrow e^C \quad \text{O.C.} \quad \text{By def. of O.C.} \]
\[ C ; \Gamma \vdash \lambda' : (\tau_1 \rightarrow \tau)^{\delta} \quad \text{Subderivation} \]
\[ C ; \Gamma \vdash \lambda' : (\tau_1 \rightarrow \tau)^{\delta} \quad \text{By i.h.} \]
\[ [\phi] \vdash e : [\phi] \tau \rightarrow \text{read } x_1 \text{ as } \lambda' \text{ in } \text{apply}^C(\lambda', \lambda) \quad \text{By (Read)} \]

Let \(e^C\) be \(\text{read } x_1\) as \(x'\) in \(\text{apply}^C(\lambda', \lambda)\).
Implicit self-adjusting computation for purely functional programs

\[ \vdash \Gamma \vdash \text{read } \varphi \text{ as } \chi' \text{ in apply}^C(\chi', \chi_2) : \| \tau \|_{\Gamma} \]

-- Subcase "\(S-C\)" where \(\varphi') = S\) and \(\varphi)\delta = C\):

Part (2):

\[
\begin{align*}
\varphi) & \Gamma, \chi' : (\varphi) \tau \vdash \text{apply}(\chi', \chi_2) : (\varphi) \tau \vdash e_0^C \quad \text{Above with } \chi' \text{ for } \chi_1 \\
\varphi) & \Gamma, \chi' : (\varphi) \tau \vdash [\chi'/\chi_1] e : (\varphi) \tau \vdash e_0^C \\
\varphi) & \Gamma \vdash \chi_1 : (\varphi) \tau \vdash \chi_2^C \quad \text{By i.h.} \\
\varphi) & \Gamma \vdash e : (\varphi) \tau \vdash \text{read } \chi_1 \text{ as } \chi' \text{ in } e_0^C \quad \text{By (Read)}
\end{align*}
\]

Let \(e^C = \text{read } \chi_1 \text{ as } \chi' \text{ in } e_0^C\):

\[
\begin{align*}
\vdash & \Gamma \vdash e^C : \| \tau \|_{\Gamma} \\
\vdash & \Gamma, \chi' : (\varphi) \tau \vdash \chi_1^C : \| \tau \|_{\Gamma} \\
\vdash & \Gamma, \chi' : (\varphi) \tau \vdash \chi_2^C : \| \tau \|_{\Gamma} \\
\vdash & \Gamma \vdash \chi_1 \text{ as } \chi' \text{ in } e_0^C \quad \text{By (TRead)}
\end{align*}
\]

Part (1): Similar to Part (1) of subcase \(C-C\).

Case

\[
\begin{align*}
C, \Gamma & \vdash \chi_1 : \text{int}^\delta_1 \\
C, \Gamma & \vdash \chi_2 : \text{int}^\delta_2 \\
C & \vdash \delta_1 = \delta_2 \\
\vdash & \oplus : \text{int} \times \text{int} \rightarrow \text{int} \\
C, \Gamma & \vdash e \oplus (\chi_1, \chi_2) : \text{int}^\delta_1 \\
\text{(SPrim)}
\end{align*}
\]

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

Part (1):

\[
\begin{align*}
C, \Gamma & \vdash \chi_1 : \text{int}^\delta_1 \\
\varphi) & \Gamma \vdash \chi_1 : \text{int}^\delta_1 \rightarrow \chi_1^C \quad \text{By i.h.} \\
\vdash & \Gamma \vdash \chi_1 : \text{int}^\delta_1 \\
\vdash & \Gamma \vdash \chi_1 : \text{int} \\
\vdash & \Gamma \vdash \chi_1 \text{ as } \chi' \text{ in } e_0^C \quad \text{By [\varphi)\delta_1 = S \text{ and def. of } ||||} \\
\varphi) & \Gamma \vdash \chi_2 : \text{int}^\delta_2 \rightarrow \chi_2^C \\
\vdash & \Gamma \vdash \chi_2 : \text{int} \\
\vdash & \Gamma \vdash e : \text{int}^\delta_2 \oplus (\chi_1, \chi_2) \quad \text{By (Prim)} \\
\varphi) & \Gamma \vdash e : (\varphi)(\text{int}^\delta_1) \rightarrow \oplus (\chi_1, \chi_2) \quad \text{By [\varphi)\delta_1 = S} \\
\text{Let } e^S = \oplus (\chi_1, \chi_2).
\end{align*}
\]
\[ \Gamma \vdash \oplus : \text{int} \to \text{int} \quad \text{Premise} \]
\[ \vdash [\delta] \phi \Gamma \vdash \ominus (x_1, x_2) : \text{int} \quad \text{By (TPrim)} \]
\[ \forall \phi : [\Gamma] \phi \vdash \ominus (x_1, x_2) : \| [\text{int}^h] \phi \| \quad \text{By } [\phi] \delta = \mathbb{S} \text{ and def. of } \| \| \]

Part (2): Similar to (SPair), where the outer level is stable \((\tau = \text{int}^h = \text{int}^g)\).

If \([\phi] \delta = [\phi] \delta_2 = \mathbb{C}\) then:

Part (2):
\[ [\phi] \Gamma, y_1 : \text{int}^h, y_2 : \text{int}^\delta \vdash \ominus (y_1, y_2) : \text{int}^C \twoheadrightarrow \ominus (y_1, y_2) \quad \text{By (Var), (Var), (Prim)} \]
\[ [\phi] \Gamma, \ldots \vdash \ominus (y_1, y_2) : \text{int}^C \twoheadrightarrow \text{let } r = \ominus (y_1, y_2) \text{ in write}(r) \quad \text{By (Write)} \]
\[ [\phi] \Gamma, y_1 : \text{int}^h \vdash \ominus (y_1, y_2) : \text{int}^C \twoheadrightarrow \text{read } x_2 \text{ as } y_2 \text{ in} \]
\[ \quad \text{let } r = \ominus (y_1, y_2) \text{ in write}(r) \quad \text{then (Read)} \]

By (LPrimop2)
\[ [\phi] \Gamma \vdash \ominus (y_1, y_2) : \text{int}^C \twoheadrightarrow \text{read } x_1 \text{ as } y_1 \text{ in read } x_2 \text{ as } y_2 \text{ in} \]
\[ \quad \text{let } r = \ominus (y_1, y_2) \text{ in write}(r) \quad \text{then (Read)} \]

By (LPrimop1)
\[ [\phi] \Gamma \vdash r : \text{int} \vdash \text{write}(r) : \text{int} \quad \text{By (TVar) then (TWrite)} \]
\[ [\phi] \Gamma \vdash r : \text{int} \vdash \text{write}(r) : \text{int} \quad \text{By (TVar) and (TVar), then (TPrim)} \]
\[ [\phi] \Gamma \vdash r : \text{int} \vdash \text{write}(r) : \text{int} \quad \text{By (TLet)} \]
\[ \vdash [\phi] \Gamma \vdash r = \ominus (y_1, y_2) \text{ in write}(r) : \text{int} \quad \text{By (TRead)} \]

By def. of \([\| \| - \mathbb{C}]\) and \([\phi] \delta_1 = \mathbb{C}\)

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

<table>
<thead>
<tr>
<th>Case</th>
<th>C; \Gamma \vdash \epsilon ; (\tau_1 \oplus \tau_2)^\delta</th>
<th>C; \Gamma, x_1 : \tau_1 \vdash e_1 : \tau</th>
<th>C \vdash \delta \leq \epsilon</th>
<th>C; \Gamma, x_2 : \tau_2 \vdash e_2 : \tau</th>
<th>C \vdash \delta &lt; \tau</th>
<th>(SCase)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[ C; \Gamma \vdash x : (\tau_1 \oplus \tau_2)^\delta ]</td>
<td>[ C; \Gamma, x_1 : \tau_1 \vdash e_1 : \tau ]</td>
<td>[ C \vdash \delta \leq \epsilon ]</td>
<td>[ C; \Gamma, x_2 : \tau_2 \vdash e_2 : \tau ]</td>
<td>[ C \vdash \delta &lt; \tau ]</td>
<td>(SCase)</td>
</tr>
</tbody>
</table>

(a) Suppose \([\phi] \delta = \mathbb{S}\).
\[ \vdash [\phi] \delta \quad \text{Subderivation} \]
\[ C; \Gamma \vdash \vdash \va : (\tau_1 \oplus \tau_2)^\delta \quad \text{By i.h.} \]
\[ \vdash [\phi] \delta \quad \text{Subderivation} \]
\[ \vdash [\phi] \delta \quad \text{By i.h.} \]
\[ \vdash [\phi] \delta \quad \text{By i.h.} \]
\[ \vdash [\phi] \delta \quad \text{By i.h.} \]
\[ \vdash [\phi] \delta \quad \text{By i.h.} \]
\[ \vdash [\phi] \delta \quad \text{By i.h.} \]
\[ \vdash [\phi] \delta \quad \text{By i.h.} \]
\[ \vdash [\phi] \delta \quad \text{By i.h.} \]
By induction on the given derivation. All cases are straightforward.

**Proof**

By induction on the given derivation. All cases are straightforward.

**Lemma B.1** (Stores Are Monotonic). If $\rho_1 \vdash e \Downarrow (\rho_2 \vdash v)$ then there exists $\rho'$ such that $\rho_2 = \rho_1, \rho'$.

**Proof**

By induction on the given derivation. All cases are straightforward.

**Lemma B.2** (Commuting). If $e_1$ and $e$ are target expressions, then $\llbracket e_1 / x \rrbracket e = \llbracket e \rrbracket / x \llbracket e_1 \rrbracket$.

**Proof**

By induction on $e_1$, using the definitions of back-translation and substitution.

**Lemma B.3.** For all closed target values $w$, the back-translation $\llbracket w \rrbracket$ is a (source) value.

**Proof**

By induction on $w$. □
Lemma B.4. The following equivalences hold:

(i) \((\text{let } x = e_0 \text{ in } x) \sim e'_0\), if \(e_0 \sim e'_0\)

(ii) \((\text{let } x' = x_1 \text{ in } \text{apply}(x', x_2)) \sim \text{apply}(x_1, x_2)\)

(iii) \((\text{let } x = x_1 \text{ in } \oplus(x', x_2)) \sim \oplus(x_1, x_2)\)

(iv) \((\text{let } x = x_1 \text{ in } \oplus(x_1, x')) \sim \oplus(x_1, x_2)\)

(v) \((\text{let } x = x \text{ in } \text{fst } x') \sim \text{fst } x\)

(vi) \((\text{let } x = x \text{ in } \text{case } x' \text{ of } \{ x_1 \Rightarrow e_1, x_2 \Rightarrow e_2 \}) \sim \text{case } x \text{ of } \{ x_1 \Rightarrow e_1, x_2 \Rightarrow e_2 \}\)

Proof
Straightforward, using inversion on the given source evaluation derivation, and applying the appropriate evaluation rules.

Lemma B.5. If \(\Gamma \vdash e : \tau \Rightarrow e'\) then \[^e' \sim e\].

Proof
By induction on the given derivation.

For (Apply), and other rules for constructs at which substitution happens during evaluation, we use Lemma [B.2].

The other interesting cases are those in which \(e\) cannot be exactly \[^e'\]: (Read), (Write), and (ReadWrite).

For (Write), \[^e'] = \[[\text{let } r = e^S \text{ in } \text{write}(r)]\] = \[[\text{let } r = e^S \text{ in } \text{write}(r)]\] = \[[\text{let } r = e^S \text{ in } r, \text{but we only have } [e^S] \sim e' \text{ (by i.h.), so we use Lemma [B.4]}(i).\]

Rule (ReadWrite) creates two \text{lets}, so we use the lemma twice.

For (Read), we use Lemma [B.4]. If the rule from Figure 17 used to derive the first premise was (LApply), we use part (ii) of the lemma; if (LPrimop1), part (iii); if (LPrimop2), part (iv); if (LFst), part (v); if (LCase), part (vi).

Roughly, we want to show that, if a target expression \(e'\) evaluates to some target value \(w\), that the back-translation \[^e'\], a source expression, evaluates to the back-translation of \(w\) (after replacing locations \(\ell\) in \(w\) with their corresponding values). This does not hold in general: the back-translation of \text{select} uses only the first arm, under the assumption that all the arms are “essentially” the same. That is, the back-translation assumes the arms differ only in their use of modifiables, and in how they instantiate polymorphic variables. Fortunately, this condition does hold for all target expressions produced by our translation. We call this condition \textit{select-uniformity}.

Definition B.6 (Select Uniformity). A target expression \(e'\) is \textit{select-uniform} if and only if, for all subexpressions of \(e'\) of the form \text{select} \(\{ (\vec{\alpha}=\vec{\delta}_1) \Rightarrow e_1, \ldots, (\vec{\alpha}=\vec{\delta}_n) \Rightarrow e_n \}\), all the arms have equivalent back-translations:

\[ [e_1] \sim [e_2] \sim \ldots \sim [e_n] \]

Lemma B.7. If \(\Gamma \vdash e : \tau \Rightarrow e'\) then \(e'\) is \textit{select-uniform}.

Proof
By induction on the given derivation. All cases are completely straightforward, except the case for (LetV), where we use Lemma [B.5].
**Theorem 6.4** (Evaluation Soundness).
If \( \rho \vdash e \downarrow (\rho' \vdash w) \) where \( \text{FLV}(e) \subseteq \text{dom}(\rho) \) and \( [\rho]e \) is select-uniform
then \( [\rho]e \downarrow [\rho']w \).

**Proof**
By induction on the given derivation. Wherever we apply the induction hypothesis, it is easy to show the condition of select-uniformity; in what follows, we omit this reasoning.

- **Case** \( \rho \vdash w \downarrow (\rho \vdash w) \) (TEvValue)

Stores only contain values, so \([\rho]w\) is a value. By Lemma B.3 \([\rho]w\) is some source value \(v\). By (SEvValue), \([\rho]w \downarrow [\rho]w\), which was to be shown.

\[
\begin{align*}
\rho \vdash e_1 \downarrow (\rho_1 \vdash \text{fun}^f f(x) = e_0) \\
\rho_1 \vdash e_2 \downarrow (\rho_2 \vdash w_2) \\
\rho_2 \vdash ([\text{fun}^f f(x) = e_0]/f)[w_2/x]e_0 \downarrow (\rho' \vdash w) \\
\rho \vdash \text{apply}^e(e_1, e_2) \downarrow (\rho' \vdash w) \tag{TEvApply}
\end{align*}
\]

**Case** \( \rho \vdash e_1 \downarrow (\rho_1 \vdash \text{fun}^f f(x) = e_0) \)

Subd.

\[
\begin{align*}
[[\rho]e_1] & \downarrow [[\rho_1]\text{fun}^f f(x) = e_0] & \text{By i.h.} \\
[[\rho]e_1] & \downarrow [[\rho_1]e_0] & \text{By definition of \([-]\)} \\
[[\rho]e_1] & \downarrow \text{fun} f(x) = [[\rho_1]e_0] & \text{By definition of \([-]} \\
[[\rho]e_1] & \downarrow \text{fun} f(x) = [[\rho']e_0] & \text{Monotonicity}
\end{align*}
\]

\[
\begin{align*}
\rho_1 \vdash e_2 \downarrow (\rho_2 \vdash w_2) \\
[[\rho_1]e_2] & \downarrow [[\rho_2]w_2] & \text{By i.h.} \\
[[\rho]e_2] & \downarrow [[\rho']w_2] & \text{FLV}(e_2) \subseteq \text{dom}(\rho) \text{ and monotonicity}
\end{align*}
\]

\[
\begin{align*}
\rho_2 \vdash ([\text{fun}^f f(x) = e_0]/f)[w_2/x]e_0 \downarrow (\rho' \vdash w) & \text{Subd.} \\
[[\rho_2]\text{fun}^f f(x) = e_0]/f[w_2/x]e_0 & \downarrow [[\rho']w] & \text{By i.h.} \\
[[\rho']\text{fun}^f f(x) = e_0]/f[w_2/x]e_0 & \downarrow [[\rho']w] & \text{Monotonicity}
\end{align*}
\]

\[
[[\text{fun} f(x) = [[\rho']e_0]/f] [[\rho']w_2]/x] [[\rho']e_0] \downarrow [[\rho']w] \tag{Properties of substitution, \([-\), \([-]}
\]

\[
\begin{align*}
\text{apply}([[\rho]e_1], [[\rho]e_2]) & \downarrow [[\rho']w] & \text{By (SEvApply)}
\end{align*}
\]

- **Cases** (TEvPair), (TEvSumLeft), (TEvPrimop), (TEvFst), (TEvCaseLeft): By similar reasoning as in the (TEvApply) case, but simpler.

- **Case** TEvLet: By similar reasoning to the (TEvApply) case, but slightly simpler.

\[
\begin{align*}
\rho \vdash e^C \downarrow (\rho'_0 \vdash w) \\
\rho \vdash \text{mod} e^C \downarrow (\rho'_0, \ell \mapsto w) \vdash \ell) \tag{TEvMod}
\end{align*}
\]
\[\rho \vdash e^C \Downarrow (\rho' \vdash w)\] Subd.
\[\left[\rho\right]e^C \Downarrow \left[\rho'\right]w\] By i.h.
\[\left[\rho\right]e^C \Downarrow \left[\rho'\right]e^C \Downarrow \left[\rho'\right]w\] By def. of subst.
\[\mod \left(\left[\rho\right]e^C\right) \Downarrow \left[\rho'\right]e^C \Downarrow \left[\rho'\right]w\] By def. of \([-\).

\[\rho \vdash e_1 \Downarrow (\rho_1 \vdash \ell)\] Subd.
\[\left[\rho\right]e_1 \Downarrow \left[\rho_1\right]\ell\] By i.h.
\[\rho_1 \vdash [p_1(\ell)/x']e^C \Downarrow (\rho' \vdash w)\] Subd.
\[\left[p_1\right]p_1(\ell)/x' \left[e^C\right] \Downarrow \left[p'\right]w\] By i.h.
\[\left[p_1\right]p_1(\ell)/x' \left[e^C\right] \Downarrow \left[p'\right]w\] By def. of subst.
\[\left[p_1\right]p_1(\ell)/x' \left[e^C\right] \Downarrow \left[p'\right]w\] By FLV(e^C) \subseteq \text{dom}(\rho) and Lemma [B.1]
\[\text{let } x' = \left[p\right]e_1 \text{ in } \left[p\right]e_1 \Downarrow \left[p\right]w\] By Lemma [B.2]
\[\rho \vdash \text{read } e_1 \text{ as } x' \text{ in } e^C \Downarrow \left[p'\right]w\] By def. of \([-\).

\[\rho \vdash e_0 \Downarrow (\rho' \vdash w)\] Subd.
\[\left[p\right]e_0 \Downarrow \left[p'\right]w\] By def. of subst.
\[\rho \vdash \text{write } e_0 (\rho' \vdash w)\] (TEvWrite)

\[\rho \vdash e_i \Downarrow (\rho' \vdash w)\] Subd.
\[\left[p\right]e_i \Downarrow \left[p'\right]w\] By i.h.
\[\left[p\right]e_i \Downarrow \left[p'\right]w\] By select-uniformity
\[\left[p\right]e_i \Downarrow \left[p'\right]w\] By def. of \(\sim\)

\[\rho \vdash (\rho' \vdash w)\] (TEvSelect)

\[\rho \vdash e \vdash e' \Downarrow (\rho' \vdash w)\] and \(\vdash e' \Downarrow \left[p'\right]w\) then \(e \Downarrow \left[p'\right]w\).

\[\text{Proof}\]

By Lemma [B.7] \(e'\) is select-uniform. The empty store \(\cdot\) is trivially select-uniform. By Theorem [6.4] \([\cdot]e' \Downarrow \left[p'\right]w\). Since the empty store acts as an identity substitution,

\[e' \Downarrow \left[p'\right]w\]
Proof of costed soundness

Theorem 6.11. If trans $(e, ε) = e'$ then $e'$ is deeply 1-bounded.

Proof

By lexicographic induction on $e$ and $ε$, with $S$ considered smaller than $C$.

- If $e ∈ \{n, x, (v_1, v_2), \text{fun} \ldots, \text{inl} \; v\}$ then:
  - If $ε = S$ then $\text{trans}$ uses one of its first 5 cases, and the result follows by induction. ($HC(e') = 0$ except for (Var) where $HC(e') = 1$ is possible.)
  - If $ε = C$ then, for $n/(v_1, v_2)/\text{fun/inl} \; v$, $\text{trans}$ uses its last case and applies (Write). A let has head cost 0 (the let appears in the back-translation), so $HC(e') = 0$; however, the head cost of the write subterm is 1, so the term is deeply 1-bounded. For $x$, $\text{trans}$ uses either (Write) or (ReadWrite); in both cases, $e'$ is deeply 1-bounded.

- If $e$ has the form $\text{let } x = e_1 \text{ in } e_2$, then $HC(e') = 0$; by induction, $e'_1$ and $e'_2$ are deeply 1-bounded, so $e'$ is deeply 1-bounded.

- If $e = \oplus(x_1, x_2)$, then: For the stable case, $e'$ is a $\oplus$ so $HC(e') = 0$. For the changeable case, $\text{trans}$ applies (Var), (Var), (Prim), (Write), (Read) with (LPrimop2), and (Read) with (LPrimop1), producing

$$e' = \text{read } x_1 \text{ as } y_1 \text{ in read } x_2 \text{ as } y_2 \text{ in let } r = \oplus(y_1, y_2) \text{ in write}(r)$$

so (assuming $HC(x_1), HC(x_2) ≤ 1$) we have $HC(e') = 0$ and all inner head costs bounded by 1.

- If $e$ is an apply, then:
  - Case ($S, S, S$): Here $e'$ is an apply$^S$, so $HC(e') = 0$.
  - Case ($C, S, C$): Here $e'$ is an apply$^C$, so $HC(e') = 0$.
  - Case ($S, S, C$): Either (Write), or (ReadWrite), after switching to S mode, meaning one of the (−, −, $S$) cases—which each generate a subterm whose $HC$ is 0. For (Write), the write subterm of $e'$ has head cost 1, and likewise for (ReadWrite). The rules (LApply) and (LCase) guarantee that the read has the correct form for $HC(e')$ to be defined.
  - Case ($e', C, C$): Applies (Read) after devolving to ($e', S, C$) which returns a term with $HC(e') ≤ 1$ (zero if $e' = C$, and 1 if $e' = S$). Applying (Read) yields a term whose $HC$ is 0, and which is deeply 1-bounded. Note that $HC(e')$ is defined for the same reason as in the ($S, S, C$) subcase.
  - Case ($S, S, S$): Devolves to the ($C, S, C$) case, yielding a subterm with $HC$ of 0; the algorithm then uses (Mod), yielding $HC(e') = 1 + 0 = 1$.
  - Case ($e', C, S$): Devolves to the ($e', C, C$) case, where $HC = 0$, then applies (Mod), yielding $HC(e') ≤ 1$.

(Note: We do not use the induction hypothesis as we “devolve”; we are merely reasoning by cases.)
• If \( e = \text{fst} \, x \) where \( x : (\tau_1 \times \tau_2)^\delta \), then:
  
  — Case \((\mathcal{S}, \mathcal{S})\): We use (Fst), yielding \( HC(e') = 0 \).
  
  — Case \((\mathcal{S}, \mathcal{C})\): If \( \tau_1 \text{ O.S. then } HC(e') = 0 \) (Write). If \( \tau_1 \text{ O.C. then we use (Read-Write), which has } HC \text{ of 0.}
  
  — Case \((\mathcal{C}, \mathcal{C})\): We use (Read) with (LFst) and go to the \((\mathcal{S}, \mathcal{C})\) case with a new variable \( x' \). The \( HC \) for the \((\mathcal{S}, \mathcal{C})\) case is 0. Using (Read) in this case also has head cost 0.

• If \( e \) is a case on a variable \( x : \tau \), then:
  
  — If \( \tau \) is outer stable, the proof is straightforward.
  
  — If \( \tau \) is outer changeable, the algorithm applies rule (Read), recursing with \( x : [\tau]^\mathcal{S} \), which will apply rule (Case). A case has \( HC \) of 0, so (Read) produces \( e' \) where \( HC(e') = 0 \) and \( e' \) is deeply 1-bounded.

  \[ \square \]

In the following proofs, we assume that in any target evaluation \( \rho \vdash e' \downarrow (\rho' \vdash w) \), the target expression \( e' \) is closed (that is, it has no free program variables \( x \), though of course it may contain store locations \( \ell \in \text{dom}(\rho) \)).

**Theorem 6.12** (Cost Result). Given \( \mathcal{D} :: \rho \vdash e' \downarrow (\rho' \vdash w) \) where for every subderivation \( \mathcal{D}^* :: \rho_1^* \vdash e' \downarrow (\rho_2^* \vdash w^*) \) of \( \mathcal{D} \) (including \( \mathcal{D} \)), \( HC(\mathcal{D}^*) \leq k \), then the number of dirty rule applications in \( \mathcal{D} \) is at most \( \frac{k}{k+1} W(\mathcal{D}) \).

**Proof**

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

\[ \square \]

**Theorem 6.13** (Costed Stable Evaluation).

If \( \mathcal{D} :: \rho \vdash e \downarrow (\rho' \vdash w) \) where \( \text{FV}(e) \subseteq \text{dom}(\rho) \) and \( [\rho]e \) is select-uniform and \( [\rho]e \) is deeply \( k \)-bounded then \( \mathcal{D}' :: [[\rho]e] \downarrow [[[\rho']w]] \) and \( [\rho']w \) is deeply \( k \)-bounded and for every subderivation \( \mathcal{D}'^* :: \rho_1^* \vdash e^* \downarrow (\rho_2^* \vdash w^*) \) of \( \mathcal{D} \) (including \( \mathcal{D} \)), \( HC(\mathcal{D}'^*) \leq HC(e^*) \leq k \), and the number of clean rule applications in \( \mathcal{D} \) equals \( W(\mathcal{D}') \).

**Proof**

The differences from Theorem 6.4 require additional reasoning:

• The 7 cases for the “clean” rules (TEvValue), (TEvPair), (TEvSumLeft), (TEvPrimop), (TEvFst), (TEvCaseLeft), and (TEvApply) are straightforward: the induction hypothesis shows that the \( HC \) condition holds for proper subderivations of \( \mathcal{D} \), and \( HC(\mathcal{D}) = 0 \) by definition of \( HC(\mathcal{D}) \), which is certainly not greater than \( HC(e^*) \).

Finally, each one of these cases generates a single application of an SEv* rule,
Implicit self-adjusting computation for purely functional programs

which together with the i.h. satisfies the last condition (that the number of clean rule applications in \(D\) equals \(W(D')\).

For (TEvCaseLeft) and (TEvApply), observe that we are substituting closed values; for all closed 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. (The target expression \(x[\alpha = \delta]\) is not closed, so we need not consider it here.)

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

\(\bullet\) (TEvWrite): We have \(D :: \rho \vdash \text{write}(e'_0) \downarrow (\rho' \vdash w)\) with subderivation \(\mathcal{D}_0 :: \rho \vdash e'_0 \downarrow \ldots\). By i.h., \(HC(D_0) \leq HC(\text{write}(e'_0))\). Therefore \(HC(D_0) + 1 \leq HC(e'_0)\). By the definitions of \(HC\) we have \(HC(D) = HC(D_0) + 1\) and \(HC(\text{write}(e'_0)) = 1 + HC(e'_0)\), so our inequality becomes \(HC(D) \leq HC(\text{write}(e'_0))\), which was to be shown. Lastly, the \(\ldots = W(D')\) condition from the i.h. is exactly what we need, because the \(D'\) is the same and (TEvWrite) is not clean.

\(\bullet\) (TEvMod): Similar to the (TEvWrite) case.

\(\bullet\) (TEvLet): According to our definition, \(HC(D) = 0\), and we proceed as with the first 7 cases. Every (TEvLet) in \(D\) corresponds to a (SEvLet) in \(D'\), even if the let was created by translation: the theorem concerns the reverse translation \([\rho][e]\), not the original source program (which probably has fewer lets). (We already assume implicitly that let-expansion preserves asymptotic complexity, because we assume that source programs are in A-normal form, and our goal is to prove an asymptotic equivalence in Theorem 6.14.)

\(\bullet\) (TEvRead): For \(HC(\text{read} \ldots)\) to be defined, the variable bound is used exactly once and contributes to the \(HC\) of the term accordingly, justifying the equation

\[HC([p_1(\ell)/x']e^C) = HC(e^C) + HC(p_1(\ell))\]

\(\bullet\) (TEvSelect):

\[
\begin{align*}
HC(D_1) & \leq HC(e_1) & \text{i.h.} \\
(\text{L}) & 1 + HC(D_1) \leq 1 + HC(e_1) & +1 \text{ each side} \\
(\text{R}) & 1 + HC(e_1) \leq HC(\text{select} \{ \ldots \}[\ldots]) & \text{By def. of } HC(e_1); \text{ property of max.} \\
& 1 + HC(D_1) \leq HC(e') & \text{By (L), (R), transitivity, } e' = (\text{select} \{ \ldots \}[\ldots] \\
\iff & HC(D) \leq HC(e') & \text{By def. of } HC(D)
\end{align*}
\]

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 (TEvValue) it follows from the assumption that \(e' = w\) is bounded. For any rule whose conclusion has the same \(w\) as one of its premises—(TEvLet), (TEvCaseLeft), (TEvApply), (TEvWrite), (TEvRead), (TEvSelect)—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 (TEvSumLeft) 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.

\(\Box\)
**Theorem 6.14** If $\text{trans}(e, \varepsilon) = e'$ and $\mathcal{D}' :: \cdot \vdash e' \downarrow (\rho' \downarrow w)$, then $\mathcal{D} :: [e'] \downarrow v$ where $W(\mathcal{D'}) = \Theta(W(\mathcal{D}))$.

**Proof**

By Theorem 6.11, $e'$ is deeply 1-bounded.

The algorithm $\text{trans}$ merely applies the translation rules, so $\cdot \vdash e : \tau \Rightarrow e'$. By Theorem 6.13, $\mathcal{D} :: [e'] \downarrow v$, and the given derivation $\mathcal{D}'$ and all its subderivations have $HC$ bounded by $k$.

By Theorem 6.12, the number of dirty rule applications in $\mathcal{D}'$ is at most $\frac{k}{k+1} W(\mathcal{D'})$. Each rule application is either clean or dirty, so $W(\mathcal{D'}) \leq (k+1) \cdot W(\mathcal{D})$, where $k = 1$.

By inspecting the evaluation rules, it is clear that $W(\mathcal{D'}) \geq W(\mathcal{D})$. Therefore, $W(\mathcal{D'}) = \Theta(W(\mathcal{D}))$. 

**References**


