1-1-2012

Dependent Interoperability

Peter-Michael Osera  
*University of Pennsylvania, posera@cis.upenn.edu*

Vilhelm Sjoberg  
*University of Pennsylvania, vilhelm@cis.upenn.edu*

Stephan A. Zdancewic  
*University of Pennsylvania, stevez@cis.upenn.edu*

Follow this and additional works at: [http://repository.upenn.edu/cis_reports](http://repository.upenn.edu/cis_reports)

Part of the [Engineering Commons](http://repository.upenn.edu/cis_reports)

Recommended Citation

Abstract
In this paper we study the problem of interoperability – combining constructs from two separate programming languages within one program – in the case where one of the two languages is dependently typed and the other is simply typed. We present a core calculus called SD, which combines dependently- and simply-typed sub-languages and supports user-defined (dependent) datatypes, among other standard features. SD has “boundary terms” that mediate the interaction between the two sub-languages. The operational semantics of SD demonstrates how the necessary dynamic checks, which must be done when passing a value from the simply-typed world to the dependently typed world, can be extracted from the dependent type constructors themselves, modulo user-defined functions for marshaling values across the boundary. We establish type-safety and other meta-theoretic properties of SD, and contrast this approach to others in the literature.

Disciplines
Engineering

Comments

This technical report is available at ScholarlyCommons: http://repository.upenn.edu/cis_reports/969
Dependent Interoperability (Technical Report)

Peter-Michael Osera
posera@cis.upenn.edu

Vilhelm Sjöberg
vilhelm@cis.upenn.edu

Steve Zdancewic
stevez@cis.upenn.edu

March 29, 2012

Abstract

In this paper we study the problem of interoperability—combining constructs from two separate programming languages within one program—in the case where one of the two languages is dependently typed and the other is simply typed. We present a core calculus called SD, which combines dependently- and simply-typed sub-languages and supports user-defined (dependent) datatypes, among other standard features. SD has “boundary terms” that mediate the interaction between the two sub-languages. The operational semantics of SD demonstrates how the necessary dynamic checks, which must be done when passing a value from the simply-typed world to the dependently typed world, can be extracted from the dependently typed type constructors themselves, modulo user-defined functions for marshaling values across the boundary. We establish type-safety and other meta-theoretic properties of SD, and contrast this approach to others in the literature.

1 Introduction

Dependently-typed languages allow programmers to specify a rich set of properties about their programs that are verifiable during type-checking. This comes at the price of complexity — it is at best extremely time-consuming and at worse infeasible to use dependently-typed languages in large software developments. A natural way to mitigate this weakness is to use a dependently-typed language to provide specifications for critical components while the rest of the system is written in a mainstream programming language. However, care must be taken to ensure that the specifications of the dependently-typed language are respected by “weaker” programming language. In this paper, we study the problem of interoperability between a language with dependent types and a language with simple types, focusing on the key meta-theoretic issues that arise in this setting.

Prior work on interoperability initially focused on the implementation of such interoperability systems. Many languages provide an escape hatch into C, such as Java’s JNI [16], or OCaml’s [14] and Haskell’s [18] FFI. Other work considers how to achieve interoperability by developing a lingua franca for languages to talk to each other. Proposals include C [3], the Java virtual machine [17], COM [26], or the .NET framework [30]. More recently, the focus has shifted to understanding the relationship between dynamic and typed languages with contracts [8], blame [33], and the integration of scripting and typed languages [34].

In these systems, dynamic checks ensure that the static guarantees of the typed language are respected by the untyped language. The dynamic check amounts to a simple type tag check, e.g., verifying that \texttt{typeof}(\lambda x: S.s) is indeed a function. However, the same concerns arise if we consider languages with richer type systems, namely those with dependent types. A simply-typed language will be able to enforce only some of a dependently-typed language’s static guarantees during type-checking; the difference must again be made up with dynamic checks. However these dynamic checks must now perform non-trivial computation rather than simply checking type tags.

For example, suppose that your dependently-typed language provides a certified library that you would
like to use in your application. For simplicity’s sake, let’s consider a List datatype that contains Ints.

\[
\begin{align*}
\text{List : Int} & \Rightarrow * \\
\text{Nil : (y : Unit)} & \rightarrow \text{List } y \\
\text{Cons : (y1 : Int)} & \rightarrow (y2 : \text{Int}) \rightarrow \text{List } y1 \rightarrow \text{List } y1 + 1
\end{align*}
\]

List is indexed by an integer that represents its length, and that invariant is maintained by its two constructors Nil and Cons. Suppose that our library also has a dependently-typed function \text{PrettyPrintList5 : List5} \rightarrow \text{Unit} that prints out lists of length five in a special way, but instead of giving it a dependently-typed List, we’d like to provide it our standard simply-typed List instead. Our interoperability layer must not only marshal the List value between languages, but also ensure that the simply-typed List has length five.

1.1 Contributions and Outline

How do we craft an interoperability layer that can generate such dynamic checks? How does such an interoperability layer affect the meta-theoretic properties of the languages involved? In order to answer these questions, we propose a calculus in the style of Matthews and Findler [20] that combines two languages together — in our case, a simply-typed and dependently-typed language — via boundary terms.

Our work on dependent interoperability contributes the following:

1. A core calculus called SD that combines a simply-typed and dependently-typed lambda calculus extended with user-defined datatypes. While we are aware of previous efforts to combine simply-typed and dependently-typed programming, to our knowledge, this is the first work that looks at the problem from the perspective of language interoperability with the corresponding aim of modifying the languages as little as possible when integrating them.

2. Analysis of the meta-theoretic properties of SD, in particular, a proof of type safety for the language.

3. Exploration of the design space of dependent interoperability, including changes to the design to guarantee termination in the presence of recursive functions and alternatives to directly translating data.

4. A comparison of our system to real world systems such as Coq and Agda that provide limited forms of language interoperability. Such comparisons strengthen our claim that our model faithfully captures dependent interoperability, but also suggests how these real world systems can improve in this area.

We open in Section 2 by expanding on the benefits of dependent interoperability. In Section 3, we describe the syntax and semantics of SD. We discuss the metatheory of SD in Section 4. Next we describe additional interesting properties of SD in Section 5. In Section 6 we compare SD to real world dependently-typed systems that offer interoperability facilities. Finally we discuss related and future work in Section 7 and close in Section 8. In this technical report, we also give a full account of the language in Appendix A and complete proofs of SD’s type safety in Appendix B.

2 Motivation

Before we discuss SD proper, we first motivate further why dependent interoperability is a useful idea by discussing three use cases in more detail. Along the way we will foreshadow the potential difficulties in creating an interoperability layer that we will solve in Section 3.

1. **Using a simply-typed library in a dependently-typed context.** While our dependently-typed language may be safer to use, it will typically not have all the functionality we would like. For example, we may wish to use a simply-typed library that provides network access, e.g., a function \text{sendData : Packet} \rightarrow \text{Unit}, from our dependently-typed program. It is a good bet (although not always true) that our dependent type system is strictly more powerful than the simple type system, so intuition tells us that we shouldn’t need any dynamic checks here. Therefore, our interop boundary needs only to
marshall the data from the dependently-typed language into the Packet that the simply-typed function expects to use.

2. Using a dependently-typed library in a simply-typed context. The dual of the previous use case is the desire to use dependently-typed code in a simply-typed context. In the introduction, we used the toy example of a List n. However, you can imagine wanting to use a verified library for a particular data structure or protocol from a simply-typed context and be assured that the simply-typed data you feed it does not break the properties the verified library enforces. Discovering and enforcing these properties is the primary challenge our interoperability boundary faces.

3. Verifying properties of simply-typed code. Finally, because we are working with a dependently-typed language, an interesting question arises. In addition to verifying properties of dependently-typed terms, can we do the same with simply-typed terms? That is, rather than implement a verified library in the dependently-typed language and translating simply-typed data into that library, we would like to verify properties of a simply-typed library directly. Ideally the dependently-typed language would be able to do this all during typechecking, but realistically, complete checking of a term across an interop boundary is impossible. We expect that the result is similar to a hybrid type system [9] where some properties are verified during compilation and the rest are “made up” with dynamic checks.

3 Language

Our language SD consists of a simply-typed and a dependently-typed lambda calculus joined together by boundary terms in the style of Matthews and Findler [20]. Throughout this paper, we use a meta-variable convention to distinguish terms of the simply-typed fragment ($\lambda^{\to}$) and the dependently-typed fragment ($\lambda^{=}$) outlined in Figure 1. In addition, there are several judgments that make up SD. In the interest of the brevity, we only present the salient features of each of these judgments. Appendices A and B contain the complete definitions of our system along with proofs.

3.1 Syntax

$\lambda^{\to}$ is a standard lambda calculus with simple types as defined in Figure 3. We augment the calculus with pairs $< s_1, s_2 >$, unit, an error term that will be raised if a boundary check fails, and user-defined data constructors $C$ with corresponding datatypes $A$. Constructors are modeled as taking only a single argument but this is not a limitation since multiple arguments can be combined using pairs. For example, the constructor $\text{Cons}^{\to}$ has type

$$\text{Cons}^{\to} : (\text{List } \ast \text{Int}) \rightarrow \text{List}.$$ 

In SD we presuppose a signature $\Psi_0$ containing the definitions of these constructors.

The notable addition to $\lambda^{\to}$ is the addition of the typed boundary term $SD^T_t$ which can be read as an interoperability boundary that translates the inner $\lambda^{=} t$ term of type $T$ to a $\lambda^{\to} t$ term of type $S$. Such boundaries are responsible for marshaling data from one side of the boundary to the other and checking that this marshaled data is appropriate for the context it will be used in. Our formulation focuses on
understanding the latter responsibility: what checks are necessary to ensure type-safety when moving across boundaries?

\(\lambda\sim\) is a standard dependently-typed lambda calculus inspired Jia et al’s system “Lambda-eek” [13]. The syntax of \(\lambda\sim\) as given in Figure 3 mirrors the syntactic forms found in \(\lambda\to\): it has dependent functions and pairs along with \texttt{unit} and \texttt{error}. The types of dependent functions and pairs are written \((y: T_1) \to T_2\) and \((y: T_1) \ast T_2\) reflecting the fact that \(T_2\) in both cases may contain the bound term variable \(y\). A datatype \(B\) is now a type-level function that, given a term \(t\), produces a type \(B\, t\). Consequently, we introduce kinds to classify such type-level functions \(T \Rightarrow \ast\), versus proper kinds \(\ast\).

Constructors in \(\lambda\sim\) also take single arguments. Combining multiple arguments using pairs is trickier because of dependent types, but still manageable. For example, the type of dependent constructor \(\texttt{Cons}\) is

\[
\texttt{Cons}\ (y_1: (y_2: \texttt{Int}) \ast (\texttt{List} \, y_2 \ast \texttt{Int})) \to \texttt{List} \,(y_1) + 1
\]

In effect, we use dependent pairs to introduce additional arguments and then project out the arguments when needed to compute the index of the datatype.

In the interest of simplifying the syntax, the introduction forms for the different constructs are shared
between $\lambda^\rightarrow$ and $\lambda^\equiv$. This is not problematic as we can look at a term’s sub-terms to determine which syntactic category it belongs to. In particular, the names of constructors $C$ are shared between the two calculi, with the implicit assumption that each constructor has $\lambda^\rightarrow$ and $\lambda^\equiv$ counterparts. This simplifies our reasoning when dealing with translating constructors, as we only need to worry about translating the arguments of the constructor.

We introduce a guard term $t_1 \triangleq t_2 \Rightarrow t_3$ that is the result of reducing a boundary term $DS^T_s$. This guard term makes explicit the equivalence check that must occur before we create the marshaled term $t$ from $s$. In our presentation of SD, the only check we need is an equivalence check $t_1 \cong t_2$ that determines whether two $\lambda^\equiv$ terms are indeed equivalent at runtime.

The attentive reader may notice that guards appear only on the $\lambda^\equiv$ side of the boundary. Intuitively this is because the types of $\lambda^\equiv$ make strictly stronger guarantees than $\lambda^\rightarrow$. When going from $\lambda^\equiv$ to $\lambda^\rightarrow$, no checks are necessary because the $\lambda^\equiv$ type system can verify all the properties that the $\lambda^\rightarrow$ type system tries to enforce. Conversely, $\lambda^\rightarrow$ cannot make such guarantees, so we make up the difference on the $\lambda^\equiv$ side with dynamic checks in the form of our guards.

In both $\lambda^\rightarrow$ and $\lambda^\equiv$ we introduce let forms as the standard syntactic sugar over abstraction binding.

$$\text{let } x = s_1 \text{ in } s_2 \triangleq (\lambda x; S_1, s_2) s_1$$
$$\text{let } y = t_1 \text{ in } t_2 \triangleq (\lambda y; T_1, t_2) t_1$$

However, in $\lambda^\rightarrow$ we also add the special let binding $\text{letd } y = t \text{ in } s$ that crosses from $\lambda^\rightarrow$ to $\lambda^\equiv$ to bind a $\lambda^\equiv$ term and then returns to evaluate $s$. This form is used in order to avoid duplication of side-effects during evaluation. We discuss $\text{letd}$ in more detail when we talk about the evaluation rules of SD.

### 3.2 Typing and well-formedness

The typing rules for the $\lambda^\rightarrow$ fragment are entirely standard, so we do not reproduce them in their entirety here. The only interesting addition is WF_STM_SD, which gives a type to our boundaries $SD^T_s t$. A boundary is well-typed if the contained $\lambda^\equiv$ term meets the type annotation on the boundary, and if the types on the boundary are compatible, written $S \leftrightarrow T$. Figure 4 gives these rules.

Our type compatibility relation ensures that we can translate between data of the given types. For compound types such as arrows and pairs, we can translate between them if we can translate between their component types. Translating between Unit types is trivial. And since datatypes $A$ and $B$ are user-defined, we appeal to user-defined translations between them represented by the meta-function $\text{corr}(A, B)$. As a concrete example, it is reasonable to expect that the List datatypes between the $\lambda^\rightarrow$ and $\lambda^\equiv$ fragments are convertible so that we have $\text{corr}(\text{List}^\rightarrow, \text{List}^\equiv)$. Note that $S \leftrightarrow T$ strips away the term-components of a dependent type—it compares types only up to the simply-typed “skeleton”. However, compatibility does require that the types of the indices of dependent data are first order, written $\text{FO}(T)$. Intuitively, $\text{FO}(T)$ means that the type $T$ does not contain any arrows. If we did allow arrows here, then when translating such datatypes we would be forced to compare equality of function values, which is a hard problem. This will become clear in Section 3.3 where we discuss the evaluation rules of SD. Note that the data that we are translating is allowed to contain functions, but the index of that datatype is not.

For $\lambda^\equiv$ we present several of the kinding and typing rules in Figures 5 and 6 to remind the reader of the intricacies of dependent type systems and foreshadow the technical challenges of translating terms into these types during evaluation.

All programs are typed with respect to some fixed signature $\Psi_0$, which assigns types to constructors $C$ and kinds to datatypes $A$ and $B$. We assume that all the types and kinds in $\Psi_0$ are well-formed in the empty context. Because datatypes are type-level functions, we assign them kinds of the form $T_1 \Rightarrow \ast$, as shown in WF_DTY_DATA, while the remaining types have kind $\ast$, e.g., WF_DTY_ARR.

Rules WF_DTM_APP and WF_DTM_PAIR illustrate the dependent nature of abstraction and pairs in $\lambda^\equiv$. The second component $T_2$ of the types may contain free occurrences of $y$ of type $T_1$, so we must close $T_2$ by substituting for $y$. WF_DTM_CONV is the standard conversion rule that allows us to take advantage of indexed types by establishing equivalences between them (via the type-equivalence judgment $\Gamma \vdash T \equiv T'$.
Figure 4: Abridged $\lambda\to$ Typing Rules, Type Compatibility, and First-order Types
$\Gamma \vdash K$

\[
\frac{}{\Gamma \vdash \text{WF}_{\text{DKN}\_\text{PROPER}}} \quad \frac{}{\Gamma \vdash T : * \quad \Gamma \vdash T \Rightarrow * \quad \text{WF}_{\text{DKN}\_\text{ARR}}}
\]

$\Gamma \vdash T : K$

\[
\Gamma \vdash T_1 : * \\
\Gamma, y : T_1 \vdash T_2 : * \\
\Gamma \vdash (y : T_1) \rightarrow T_2 : * \quad \text{WF}_{\text{DTY}\_\text{ARR}} \\
B : T \Rightarrow * \in \Psi_0 \\
\Gamma \vdash B : T \Rightarrow * \quad \text{WF}_{\text{DTY}\_\text{DATA}}
\]

$\Gamma \vdash t : T$

\[
\begin{align*}
\Gamma & \vdash t_1 : (y : T_1) \rightarrow T_2 \\
\Gamma & \vdash t_2 : T_1 \\
\Gamma & \vdash [t_2/y]T_2 : * \\
\frac{}{\Gamma \vdash t_1 \ t_2 : [t_2/y]T_2} \quad \text{WF}_{\text{DTM}\_\text{APP}} \\
\Gamma & \vdash t_1 \ t_2 : (y : T_1) \rightarrow T_2 \\
\Gamma & \vdash t_1 : T_1 \\
\Gamma & \vdash t_2 : [t_1/y]T_2 \\
\Gamma & \vdash (y : T_1) * T_2 : * \\
\frac{}{\Gamma \vdash <t_1, t_2> : (y : T_1) * T_2} \quad \text{WF}_{\text{DTM}\_\text{PAIR}}
\end{align*}
\]

Figure 5: Abridged $\lambda^\approx$ Typing Rules

as discussed in the next section). With $\text{WF}_{\text{DTM}\_\text{CTOR}}$, we type a constructor $C$ at some datatype $B[t/y]T'$ where we substitute into the term the argument given to $C$. Note that the type of the argument to $C$ does not need to coincide with the type of the index of $B$. Finally when we type cases with $\text{WF}_{\text{DTM}\_\text{CASE}}$ in each branch we remember the refined type $B \ t_i'$ of the branch’s associated constructor.

Checking DS via $\text{WF}_{\text{DTM}\_\text{DS}}$ is analogous to SD boundaries: the inner term must typecheck and the type annotations must coincide. $\text{WF}_{\text{DTM}\_\text{GUARD}}$ typechecks guards by checking to see if the types involved in the equivalence check are well-typed. In addition, $t$ must be well-typed under the assumption that the check holds. Finally, we require that the types of the guard are first-order with the judgment $\text{FO}(T)$. The first-order judgment ensures that the types of guards are never arrows so that we do not have to determine the equivalence of functions.

The judgment $\text{FO}(T)$ ensures that the inhabitants of $T$ do not contain function values. In the case of $\text{FO}\_\text{DATA}$ we check that all constructors of $B$ take first-order arguments. We do not need to check that the type of $B$’s index term $t_i$ is first-order, since the index is not part of the values inhabiting $B$.

### 3.3 Evaluation

The evaluation rules of SD are of most interest to us because this is where we do the actual work of checking values and marshaling them across boundaries. Figures 7 and 8 give the syntax of our one-step evaluation contexts which define the standard call-by-value order for our language. In addition, Figures 7 and 8 give also lists the interesting evaluation rules for both languages.

The evaluation of the usual syntactic forms — abstractions, pairs, and constructors — are standard. The interesting rules arise from evaluation of boundary terms. In both languages, the evaluation of boundaries is directed by their type annotations, so there is one rule for each value that might be sent across a boundary.

When we translate lambdas, e.g., a $\lambda^{\Rightarrow}$ lambda to a $\lambda^\approx$ lambda as in $\text{EVAL}\_\text{STM}\_\text{DS}\_\text{ABS}$, the output must be a $\lambda^\approx$ lambda. Our translation is similar to Matthews’ and Findler’s. This new $\lambda^\approx$ lambda translates its argument $y$ to $\lambda^{\Rightarrow}$, supplies that translated argument to the $\lambda^{\Rightarrow}$ lambda, and translates the $\lambda^{\Rightarrow}$ result of the application back to $\lambda^\approx$.

In the DS case this is straightforward. However, if we look at the SD case as presented in $\text{EVAL}\_\text{DTM}\_\text{SD}\_\text{ABS}$, we note that $T_2$ may contain free occurrences of $y$ in the boundary. To fix this problem, we close $T_2$ with the
\[
\Gamma \vdash t : T
\]

\[
\frac{
\Gamma \vdash t : (y : T_1) \ast T_2 \\
\Gamma \vdash t.1 : T_1
}{
\Gamma \vdash t.1 : T_1}
\]

\[
\frac{
\Gamma \vdash t : (y : T_1) \ast T_2 \\
\Gamma \vdash [t.1/y]T_2 : * \\
\Gamma \vdash t.2 : [t.1/y]T_2
}{
\Gamma \vdash t.2 : [t.1/y]T_2}
\]

\[
\frac{
C : (y : T_1) \rightarrow B t' \in \Psi_0 \\
B \vdash * \in \Psi_0 \\
\Gamma \vdash t : T_1 \\
\Gamma \vdash B[t/y]t' : *
}{
\Gamma \vdash C t : B[t/y]t'}
\]

\[
\frac{
\Gamma \vdash s : S \\
\Gamma \vdash T : * \\
\Gamma \vdash \text{FO} (T_0)
}{
\Gamma \vdash T \equiv T' \in \Psi_0 \\
\Gamma \vdash t_0 \equiv t_0 \vdash t : T}
\]

\[
\frac{
\Gamma \vdash s : T \\
\Gamma \vdash \text{FO} (T_0)
}{
\Gamma \vdash DS^S_{T} s : T}
\]

\[
\frac{
\Gamma \vdash s : T \\
\Gamma \vdash \text{FO} (T_0)
}{
\Gamma \vdash t_0 \equiv t_0 \vdash t : T}
\]

\[
\frac{
\Gamma \vdash t : B t' \\
\Gamma \vdash T : * \\
\begin{align*}
\text{constrs } B &= \overline{C_i} \\
C_i : (y_i : T_i) &\rightarrow B t'_i \in \Psi_0
\end{align*}
}{
\Gamma \vdash \text{case } t \in \overline{C_i} y_i \rightarrow t_i : T}
\]

Figure 6: Abridged \( \lambda^\boxplus \) Typing Rules (cont.)

\[
\lambda \rightarrow \text{Values} \quad u ::= x \mid \lambda x : S x \mid <u_1, u_2> \mid C u
\]

\[
\lambda \rightarrow \text{Contexts} \quad \mathcal{E}_s ::= \square \mid \square s \mid u \square \mid <\square, \square > \mid <u, \square > \\
\mid \square.1 \mid \square.2 \mid C \square \mid \text{letd} y = \square \text{in } s
\]

\[
\lambda^\boxplus \text{ Values} \quad v ::= y \mid \lambda y : T.t \mid <v_1, v_2> \mid C v
\]

\[
\lambda^\boxplus \text{ Contexts} \quad \mathcal{E}_t ::= \square \mid \square t \mid v \square \mid <\square, t > \mid <v, \square > \\
\mid \square.1 \mid \square.2
\]

\[
\mid C \square \mid \text{case } \square \text{ of } C_i y_i \rightarrow t_i
\]

\[
\mid DS^S_{T} \square \mid \square \equiv t_2 \triangleright t \mid v \equiv \square \triangleright t
\]

Figure 7: SD Evaluation: Contexts and Rules
\[
\begin{align*}
C: S &\to A \in \Psi_0 \\
C: (y: T_1) &\to B \ t_1 \in \Psi_0 \\
\text{argToS}_C \ v &= u \\
\text{SD}_A^{(B \ t)} C \ v &\to C \ u & \text{EVAL\_STM\_SD\_CONSTR} \\
\end{align*}
\]

\[
\begin{align*}
\text{SD}_{(S_1 \to S_2)}^{(y: T_1) \to T_2} \lambda y: T_1. t &\to \lambda x: S_1. \text{letd} y' = \text{DS}_{S_1}^{T_1} x \text{ in } \text{SD}_{S_2}^{y'/y}((\lambda y: T_1. t) y') & \text{EVAL\_STM\_SD\_ABS} \\
\end{align*}
\]

\[
\begin{align*}
\text{SD}_{(S_1 + S_2)}^{(y: T_1) \to T_2} <v_1, v_2> &\to <\text{SD}_{S_1}^{T_1} v_1, \text{SD}_{S_2}^{y'/y}v_2> & \text{EVAL\_STM\_SD\_PAIR} \\
\end{align*}
\]

\[
\begin{align*}
\text{t} &\to t' \\
C: S &\to A \in \Psi_0 \\
C: (y: T_1) &\to B \ t_1 \in \Psi_0 \\
\text{argToD}_C \ v &= v \\
\text{DS}_A^{(B \ t)} (C \ u) &\to t \equiv [v/y] t_1 \triangleright (C \ v) & \text{EVAL\_DTM\_DS\_CONSTR} \\
\end{align*}
\]

\[
\begin{align*}
\text{DS}_{(S_1 + S_2)}^{(y: T_1) \to T_2} \lambda x: S_1'. s &\to \lambda y: T_1. \text{DS}_{S_2}^{T_2}((\lambda x: S_1'. s) (\text{SD}_{S_1}^{y} y)) & \text{EVAL\_DTM\_DS\_ABS} \\
\end{align*}
\]

\[
\begin{align*}
\text{DS}_{(S_1 + S_2)}^{(y: T_1) \to T_2} <u_1, u_2> &\to \text{let} y' = \text{DS}_{S_1}^{T_1} u_1 \text{ in } <y', \text{DS}_{S_2}^{y'/y}u_2> & \text{EVAL\_DTM\_DS\_PAIR} \\
\end{align*}
\]

\[
\begin{align*}
\text{v} &\equiv v \triangleright t & \text{EVAL\_DTM\_GUARD\_REFL} \\
\text{v} &\not\equiv v' \triangleright t & \text{EVAL\_DTM\_GUARD\_ERROR} \\
\end{align*}
\]

Figure 8: SD Evaluation: Contexts and Rules (cont.)
In general, what the translation should do is dependent on the datatypes we are translating. Of the List that the translation "respects" the property represented by the datatype's index. For example, in the case of the dependent datatype's properties. These conversions come as a pair of functions responsible for converting constructor arguments from one language to the other. At type-checking time, the arguments \( v \) and \( u \) could contain free variables making it unclear how to translate them, so we allow \( \text{argToS} \) and \( \text{argToD} \) to be partial functions. When they are undefined the corresponding boundary term is stuck. To ensure Progress, we require that they are always defined for closed well-typed values. We also require some additional conditions expressing that they are defined "naturally" in the argument that we discuss further in Section 4.3.

\( \text{argToS} \) and \( \text{argToD} \) can be viewed constructor-indexed user-level functions which, if \( C:S \rightarrow A \in \Psi_0, C:(y:T_1) \rightarrow B \in \Psi_0, \) and \( B:T_2 \Rightarrow * \in \Psi_0, \) have the types

\[
\begin{align*}
\text{argToS} : T_1 & \rightarrow S \\
\text{argToD} : S & \rightarrow T_1.
\end{align*}
\]

We distinguish them from user-level functions because as we have defined the calculus there is no way to form such mixed types. Also, in addition to their types, we intend that the functions are inverses. That is, the following equations should hold

\[
\begin{align*}
1. & \quad (\text{argToS} \circ \text{argToD})(u) = u \text{ with } u : S \\
2. & \quad (\text{argToD} \circ \text{argToS})(v) = v \text{ with } v : T_1.
\end{align*}
\]

This makes \( \text{argToS} \) and \( \text{argToD} \) an isomorphism over the constructor \( C \).

In \text{eval_stm_sd_constr}, we use \( \text{argToS} \) to convert the \( \lambda^\Xi \) argument \( v \). Intuitively, since we are going from \( \lambda^\Xi \) to \( \lambda^\rightarrow \), no checks are necessary because the type system of \( \lambda^\Xi \) enforces all the properties that \( \lambda^\rightarrow \) does and more.

Conversely, in \text{eval_dtm_ds_constr}, we must verify that the argument converted from \( \lambda^\rightarrow \) meets the specification demanded by the \( \lambda^\Xi \) datatype. To generate this check, we note that the type of the new
### 3.4 Equivalence

Equivalence checks are the core of a dependently-typed system. Figure 9 outlines the most important of these, equivalence over $\lambda \equiv$ terms. We elide $\lambda \equiv$ kind equivalence ($\Gamma \vdash K \equiv K'$) and $\lambda \equiv$ type equivalence ($\Gamma \vdash T \equiv T'$) as they are standard.

Our term-level equivalence is reflexive, transitive, and symmetric by the $\text{EQ\_DTM\_REFL}$, $\text{EQ\_DTM\_SYM}$, and $\text{EQ\_DTM\_TRANS}$ rules. The most interesting of these rules is $\text{EQ\_DTM\_STEP}$ which allows us to use reduction of $t$ in our equivalence relation. This rule is good because we do not need an explicit notion of $\lambda \to$ equivalence, which would be unnatural. That is, in a real system, the $\lambda \equiv$ will only have available to it the ability to evaluate $\lambda \to$ terms rather than have access to the internals of the entire $\lambda \to$ program.

One subtlety that sets us apart from dependent languages like Coq and Agda is that our $\text{EQ\_STM\_STEP}$ rule is restricted to call-by-value reduction. Pure, strongly normalizing languages have the luxury of allowing arbitrary $\beta$-reductions when comparing types because any order of evaluation gives the same answer. In our language that is not the case because of run-time errors, e.g. $\lambda y : \text{Unit}. \text{error}$ evaluates to $\text{error}$ under CBV but to $\text{unit}$ under CBN. This problem would get even worse if the language included more interesting side-effects.

For this reason, the type equivalence judgment is defined in terms of the evaluation relation $\rightarrow$ which is explicitly CBV. Even so, we do want to allow reduction of open terms. For example to typecheck the usual append function we want $\text{List} (0 + y) \equiv \text{List} y$. Therefore, our definition of values includes variables. To make that choice work, we are careful to only substitute values for variables. In particular, we need an extra premise in $\text{WF\_DTM\_APP}$ to check that the type $[t_2/y]T_2$ is well-kindred. It might not be, since the well-kindness of $(y : T_1) \to T_2$ may depend on $y$ being a value.
3.5 Examples

To get a better understanding of how our system works, let’s expand on the List example we’ve used so far.

The complete set of definitions for our List datatype are

\[
\begin{align*}
\text{List} & : \text{Int} \Rightarrow \ast \\
\text{Nil} & : \text{Unit} \rightarrow \text{List} \\
\text{Nil} : (y : \text{Unit}) & \rightarrow \text{List}\{\} \\
\text{Cons} : (\text{List} \ast \text{Int}) & \rightarrow \text{List} \\
\text{Cons} : (y_1 : (y_2 : \text{Int}) \ast (\text{List} y_2 \ast \text{Int})) & \rightarrow \text{List}\{y_1, 1\} + 1.
\end{align*}
\]

So the types of our argument conversion functions are

\[
\begin{align*}
\text{argToSNil} & : \text{Unit} \rightarrow \text{Unit} \\
\text{argToDNil} & : \text{Unit} \rightarrow \text{Unit} \\
\text{argToSCons} : (y_1 : (y_2 : \text{Int}) \ast (\text{List} y_2 \ast \text{Int})) & \rightarrow (\text{List} \ast \text{Int}) \\
\text{argToDCons} : (\text{List} \ast \text{Int}) & \rightarrow (y_1 : (y_2 : \text{Int}) \ast (\text{List} y_2 \ast \text{Int})).
\end{align*}
\]

Note that the type of the arguments to \text{Cons}→ is a pair whereas \text{Cons}⇝ is a triple. This is because the extra \text{Int} carried by \text{Cons}⇝ is required to represent the size of the argument List.

Morally, a List\{y\} has length \(y\) so our conversions needs to respect that property. The conversions of the arguments to Nil are trivial.

\[
\begin{align*}
\text{argToSNil} \text{unit} & = \text{unit} \\
\text{argToDNil} \text{unit} & = \text{unit}
\end{align*}
\]

To convert from a \text{Cons}⇝ to a \text{Cons}→, we can simply drop the index argument. To convert in the other direction, we must regenerate it by requesting the List’s length.

\[
\begin{align*}
\text{argToSCons}(k, l, v) & = (l, v) \\
\text{argToDCons}(l, v) & = \text{length}(l), (l, v)
\end{align*}
\]

This is reminiscent of McBride’s work on ornamental types [21] where he also makes the observation that the difference between a simply-typed list and a standard dependently-typed list is the “ornamental” length data.

Matthews and Amhed demonstrate how nested boundaries can enforce specifications over the behavior of the weakly-typed language while being written in a strongly-typed language [19]. In their system, they are only able to express simple type specifications, e.g., that a Scheme function performs at type \text{Int} → \text{Int}. As expected with our dependently-typed language, we are able to express more powerful constraints via this method. For example consider a function \text{pop} over simply-typed Lists.

\[
\begin{align*}
\text{pop} : \text{List} \rightarrow \text{List}
\end{align*}
\]

Given this function, we can write a safe variant of \text{pop} in \(\lambda^\times\) that simply calls \text{pop} to do the heavy lifting:

\[
\begin{align*}
\text{safePop} : (n : \text{Int}) & \rightarrow \text{List} n \rightarrow \text{List} (n - 1) \\
\text{safePop} = \lambda n : \text{Int}. \lambda y : \text{List} n. \text{DS}_{\text{List}}^{\text{List}} n - 1 \text{pop}(\text{SD}_{\text{List}}^{\text{List}} n, y))
\end{align*}
\]

Now, this function will verify via dynamic checks that — provided the length of the subject list \(n\) — \text{pop} does the right thing for that list.

Providing this length argument explicitly is annoying, so we can write one more wrapper around this method that is callable directly from \(\lambda^\times\) and has the signature we want. The difference between this and the original \text{pop} is that now the function will check to see if \text{pop} produces the correct value:

\[
\begin{align*}
\text{verifiedPop} : \text{List} \rightarrow \text{List} \\
\text{verifiedPop} = \lambda y : \text{List}. \\
\text{let} \ l = \text{length} y \ \text{in} \\
\text{SD}_{\text{List}}^{\text{List}} \text{DS}_{\text{List}}^{\text{List}} n - 1 ( \\
\text{safePop} (\text{DS}_{\text{Int}}^{\text{Int}} l) (\text{DS}_{\text{List}}^{\text{List}} n, y))
\end{align*}
\]
Property 1 (Types of argToD/argToS). Suppose $C : S \rightarrow A \in \Psi_0$ and $C(y : T_1) \rightarrow B \in \Psi_0$.
If $\Gamma \vdash u : S$, then $\Gamma \vdash \text{argToD}_C u : T_1$ (if it is defined).
If $\Gamma \vdash v : T_1$, then $\Gamma \vdash \text{argToS}_C v : S$ (if it is defined).

Property 2 (Correctness of $\text{corr}(A, B)$). If $\text{corr}(A, B)$, then $A$ and $B$ have the same constructors $C_i$.

Property 3 (argToD/argToS respect substitution). If $\text{argToD}_C u$ and $\text{argToS}_C v$ are defined, then
$\text{argToD}_C([u_1/x_1]u) = [u_1/x_1](\text{argToD}_C u)$
$\text{argToD}_C([v_1/y_1]u) = [v_1/y_1](\text{argToD}_C u)$
$\text{argToS}_C([u_1/x_1]v) = [u_1/x_1](\text{argToS}_C v)$
$\text{argToS}_C([v_1/y_1]v) = [v_1/y_1](\text{argToS}_C v)$

Property 4 (argToD/argToS respect $\rightarrow_p$).
If $u \rightarrow_p u'$, then $\text{argToD}_C u \rightarrow_p \text{argToD}_C u'$.
If $v \rightarrow_p v'$, then $\text{argToS}_C v \rightarrow_p \text{argToS}_C v'$.

Property 5. $\text{argToD}$ and $\text{argToS}$ are defined for closed values.

Figure 10: Requirements on the conversion functions

verifiedPop is a good example of the power of dependent interoperability. We are able to take a simply-typed piece of code and then inject dynamic checks to verify its behavior against a dependently-typed specification.

4 Metatheory

Our technical contribution is a proof of type safety for SD: every well-typed term either goes to a value, diverges, or goes to $\text{error}$. We state this result in the usual way, via Preservation and Progress theorems.

The type-safety proof puts some requirements on the user-defined translation-functions $\text{argToD}$, $\text{argToS}$, and $\text{corr}(A, B)$. These are stated in figure 10, and we will point out where they are needed. Note that the round-tripping law is not one of the properties needed for type-safety. The term equivalence judgment does not axiomatize this property, so violating it does not lead to type errors. However, we still feel that requiring it rules out bad behavior.

4.1 Structural Lemmas

We begin by showing basic structural properties of the type system: Weakening, Substitution, and ignoring redundant assumptions.

Since the different syntactic categories of our language (simple and dependent terms, types and kinds) form a mutually recursive system, the proofs of these lemmas also need to be by mutual induction. The typing judgments call out to the type equivalence judgments, but the equivalence is defined without any reference to types, so the proofs about the equivalence judgments can be done first. For example, Weakening can be proved in two lemmas, each of which is proved using mutual induction.

Lemma 1 (Weakening for Equivalence).

1. If $\Gamma_1, \Gamma_3 \vdash t \equiv t'$, then $\Gamma_1, \Gamma_2, \Gamma_3 \vdash t \equiv t'$.
2. If $\Gamma_1, \Gamma_3 \vdash T \equiv T'$, then $\Gamma_1, \Gamma_2, \Gamma_3 \vdash T \equiv T'$.
3. If $\Gamma_1, \Gamma_3 \vdash K \equiv K'$, then $\Gamma_1, \Gamma_2, \Gamma_3 \vdash K \equiv K'$
Lemma 2 (Weakening).
1. If $\Gamma_1, \Gamma_3 \vdash t : T$ then $\Gamma_1, \Gamma_2, \Gamma_3 \vdash t : T$.
2. If $\Gamma_1, \Gamma_3 \vdash s : S$ then $\Gamma_1, \Gamma_2, \Gamma_3 \vdash s : S$.
3. If $\Gamma_1, \Gamma_3 \vdash T : *$ then $\Gamma_1, \Gamma_3, \Gamma_3 \vdash T : *$.
4. If $\vdash \Gamma_1, \Gamma_2$ then $\vdash \Gamma_1$

The other lemmas are proved by similar mutual inductions. To save space we abbreviate sets of statements like this to $\Gamma \vdash J$, where the $J$ stands for all the judgment forms in the type system (equivalence, typing, and kinding).

For the Preservation proof we need a substitution lemma. Somewhat unusually, it is restricted to substituting values into the judgments, not arbitrary terms. This is because our term equivalence is CBV, so substituting a non-value could block reductions and cause types to no longer be equivalent.

Lemma 3 (Substitution).
1. If $\Gamma, x:S_2, \Gamma' \vdash J$ and $\Gamma \vdash u_2 : S_2$ then $\Gamma, [u_2/x]\Gamma' \vdash [u_2/x]J$.
2. If $\Gamma, y:S_2, \Gamma' \vdash J$ and $\Gamma \vdash v_2 : T_2$ then $\Gamma, [v_2/y]\Gamma' \vdash [v_2/y]J$.

Because we present dependent pattern matching using explicit equality assumptions in the context, we also need a set of structural lemmas stating that we can omit redundant equations and swap equivalent ones. These lemmas are used when proving type preservation of case-expressions and guard expressions: when the scrutinee steps, the corresponding equation changes to a syntactically different but $\beta$-equivalent one.

Lemma 4 (Cut). If $\Gamma \vdash t_1 \equiv t_2$ and $\Gamma, t_1 \equiv t_2, \Gamma' \vdash J$, then $\Gamma, \Gamma' \vdash J$.

Lemma 5 (Context Equivalence). If $\Gamma \vdash t_1 \equiv t'_1$ and $\Gamma \vdash t_2 \equiv t'_2$ and $\Gamma, t_1 \equiv t_2, \Gamma' \vdash J$, then $\Gamma, t'_1 \equiv t'_2, \Gamma' \vdash J$.

Cut is proved like a substitution lemma: each use of the equality assumption is replaced by the explicit derivation of the equation. The Context Equivalence lemma follows as a corollary of Weakening and Cut.

4.2 Preservation

We prove preservation by mutual recursion on the simple typing, dependent typing, and kinding judgment.

Theorem 1 (Preservation).
1. If $\Gamma \vdash s : S$ and $s \rightarrow s'$ then $\Gamma \vdash s' : S$.
2. If $\Gamma \vdash [t/y]_0 : T$ and $t \rightarrow t'$ then $\Gamma \vdash [t'/y]_0 : T$.
3. If $\Gamma \vdash [t/y]_0 : K$ and $t \rightarrow t'$ then $\Gamma \vdash [t'/y]_0 : K$.

The statement for simple typing is standard but we have generalized the ones for dependent typing and kindling. The reason for this twist is again the CBV-style dependent type system: we need to know that the premise $\vdash [t_2/y]T_2 : *$ to the $\text{wf\_DTM\_APP}$ rule is preserved when $t_2$ steps. The generalization creates some extra congruence-like cases to deal with, but essentially this is still a standard Preservation proof.

The proof of this theorem informs the typing rules for the interoperability features. We highlight a few interesting cases.

First, the case when a SD-boundary for pairs steps is interesting because we substitute into the type on the SD boundary:

$$\text{SD}_{\langle y: T_1, v_1 \rangle < v_1, v_2 >} \rightarrow \text{SD}_{\langle y: T_1, v_1 \rangle < v_1, v_2 >}$$

This is different from prior work on non-dependent interoperability. We might worry that this would interfere with the compatibility check of the type. However, that is not the case, as we have the following lemma, which states that compatibility never looks at the terms embedded inside a type.
Lemma 6. \( S \leftrightarrow T \) iff \( S \leftrightarrow [t/y]T \).

Now, from the derivation of \( SD_{\langle y:T_1 \rangle \cdot T_2}^{S_1 \cdot S_2} <v_1, v_2> \) we get \( S_1 \cdot S_2 \leftrightarrow (y : T_1) \cdot T_2 \), so by inversion \( S_2 \leftrightarrow T_2 \) and hence \( S \leftrightarrow [v_1/y]T_2 \), which is the compatibility condition that we need for the term \( SD_{\langle v_1/y \rangle \cdot T_2}^{S_2} v_2 \) to be well-typed.

Next, consider the case when a DS-boundary for a data constructor steps. This is the case that motivates our handling of dynamic checks:

\[
DS_A^{(B \cdot t)}(c \cdot u) \rightarrow t \equiv [v/y] t_1 \vdash (C \cdot v) \text{ where } \argToC u = v
\]

when the signature contains declarations \( C : S \rightarrow A \) and \( C : (y : T_1) \rightarrow B \cdot t_1 \). By our requirements on \( \argToC \) we know that \( \Gamma \vdash v : T_1 \), so \( \Gamma \vdash C \cdot v : B \cdot [v/y] t_1 \). By the type conversion rules, that means \( \Gamma, t \equiv [v/y] t_1 \vdash C \cdot v : B \cdot t \). So we wrap the expression in a guard that enforces that equality assumption.

A final interesting case is when a guarded term steps. This motivates the structural lemmas Cut and Context Equivalence. The typing rule looks like

\[
\begin{align*}
\Gamma \vdash t_0 & : T_0 \\
\Gamma \vdash t_1 & : T_0 \\
\text{FO} (T_0) & \\
\Gamma, t_1 & \equiv t_0 \vdash t : T \\
\Gamma & \vdash t_1 \equiv t_0 \vdash t : T \text{ \emph{WF.DTM_GUARD}}
\end{align*}
\]

Consider how the term can step. If \( t_1 \rightarrow t'_1 \), then it suffices to show \( \Gamma, t'_1 \equiv t_0 \vdash t : T \). But by the rule EQ.DTM_STEP, \( \Gamma, t'_1 \equiv t_0 \) and \( \Gamma, t'_1 \equiv t_0 \) are equivalent contexts. Otherwise, if it steps by \( v \equiv v \vdash t \rightarrow t \), then by EQ.DTM_REFL the equation \( v \equiv v \) was redundant, so by Cut we can show \( \Gamma \vdash t : T \) as required.

Finally, it may step by \( v \equiv v' \vdash \text{error} \). Since \text{error} is always well-typed, preservation holds. Although the proof doesn’t illustrate it, the FO \((T_0)\) restriction means that we will never go to error unless it is absolutely necessary, when \( v \) and \( v' \) are unequal first-order values.

4.3 Progress

As it turns out, the interoperability features do not add much complication to the Progress part of the proof. However, as is common in languages with dependent pattern matching, we need to do a bit of work to rule out contradictory equalities.

To prove progress we first need to prove a canonical forms lemma.

Lemma 7 (Canonical Forms).

1. If \( \vdash v : (y : T_1) \rightarrow T_2 \) then \( v \) is \( \lambda y : T. t \).
2. If \( \vdash v : (y : T_1) \cdot T_2 \) then \( v \) is \( <v_1, v_2> \).
3. If \( \vdash v : \text{Unit} \) then \( v \) is \( \text{unit} \).
4. If \( \vdash v : B \cdot t \) then \( v \) is \( C \cdot v' \) and \( C : (y : T) \rightarrow B \cdot t' \in \Psi_0 \).

This does not follow immediately from inspecting the typing judgment, because of the rule EQ.DTY_INCON: if we could somehow in the empty context prove \( \vdash C_1 v_1 \equiv C_2 v_2 \) where \( C_1 \neq C_2 \), then we could assign any term any type. So we need to rule out such an inconsistent equation. However, the way we define the term equivalence judgment \( \Gamma \vdash t \equiv t' \) makes that difficult. The definition is succinct, but because it has an explicit transitivity rule it doesn’t give any leverage for doing induction on it.

Our solution is to define an auxiliary notion of parallel reduction, denoted \( \rightarrow_p \), in the style of Taka-hashi [31]. This relation contains the evaluation relation \( \rightarrow \), but it also allows reducing more than one
redex, and reducing inside the body of a lambda expression or other binder. For example, the two parallel reduction rules for applications are:

\[
\begin{align*}
  t_1 & \rightsquigarrow_p t'_1 \\
  t_2 & \rightsquigarrow_p t'_2 \\
  t_1 t_2 & \rightsquigarrow_p t'_1 t'_2 \\
  v & \rightsquigarrow_p v' \\
  (\lambda y : T . t_1) v & \rightsquigarrow_p [v'_2/y] t'_1
\end{align*}
\]

As a result, unlike evaluation, parallel reduction is closed under substitution: if \( v_1 \rightarrow_p v_2 \) and \( t_1 \rightarrow_p t_2 \) then \([v_1/y]t_1 \rightarrow_p [v_2/y]t_2 \) and \([t_1/y]t \rightarrow_p [t_2/y]t \). We also show that it is confluent. Together, these properties let us prove a useful characterization of term equivalence.

**Lemma 8** (Parallel reduction contains term equivalence). If \( \vdash t_1 \equiv t_2 \), then there exists some \( t' \) such that \( t_1 \rightarrow_p t' \) and \( t_2 \rightarrow_p t' \).

This lemma rules out the inconsistent equation we were worried about, since reducing a term can never change its constructor. We can then straightforwardly show Canonical Forms and Progress.

**Theorem 2** (Progress).

1. If \( \vdash t : T \) then either \( t \rightarrow t' \), \( t \) is a value, or \( t \) is error.
2. If \( \vdash s : S \) then either \( s \rightarrow s' \), \( s \) is a value, or \( s \) is error.

However, there is a difficulty. In order to prove substitution and confluence of parallel reduction, we need to assume these properties for the \( \text{argToD} \) and \( \text{argToS} \) functions, because the reduction relation is defined in terms of them. This yields properties 3 and 4 in figure 10.

We expect these requirements to be satisfied by any “natural” definition of \( \text{argToD} \) and \( \text{argToS} \). For example, one definition that would not respect parallel reduction would be to define

\[
\begin{align*}
  \text{argToS}_C(\lambda y : \text{Unit}.1 + 1) & = \text{true} \\
  \text{argToS}_C(\lambda y : \text{Unit}.2) & = \text{false}
\end{align*}
\]

But such a function, which examines the body of a \( \lambda \)-abstraction, could never be written by user code. In practice, we expect the translation functions to do pattern matching and to construct constructor applications and function calls, e.g. \( \text{argToD}_{\text{Cons}} \) in section 3.5. Such translation functions automatically satisfy these requirements, because they are just built up from \( \lambda \rightarrow \) and \( \lambda \equiv \) terms.

### 5 Additional Properties

Two important properties of SD that deserve special mention are the soundness of the dependently-typed fragment of the language and decidable typechecking.

#### 5.1 Soundness

Soundness of a dependently-typed language is important because a sound language can function as a proof system. Unfortunately, by introducing boundaries that produce errors and defer complete typechecking until runtime, we’ve removed soundness from \( \lambda \equiv \).

In the case of error we can simply consider the empty datatype \( \text{false} \) that should have no inhabitants. But due to \( \text{SD}_{\text{WF}}_{\text{DTM}}_{\text{ERROR}} \) we can ascribe error that type.

With respect to complete typechecking, consider the term

\[
\text{case } \text{DS}^{(\text{Foo})}_{\text{mkFoo}} \text{ unit of } \text{mkFoo } y \rightarrow t
\]

Where \( \text{Foo} : \text{Int} \Rightarrow * \) and \( \text{mkFoo} : (y : \text{Unit}) \rightarrow \text{Foo} 0 \). The boundary typechecks giving \( \text{DS}^{(\text{Foo})}_{\text{mkFoo}} s \) the type \( \text{Foo} 1 \), an uninhabited type. By \( \text{SD}_{\text{WF}}_{\text{DTM}}_{\text{CASE}} \), in the only case for \( \text{Foo} \) we arrive at the inequality \( 0 \equiv 1 \in \Gamma \) and can thus typecheck the case to \( \text{false} \).
Note that this is an unavoidable consequence of boundaries. We need to signal errors at runtime and our boundaries necessarily make claims (e.g., above that the boundary expects a Foo even though it is impossible) that can only be verified at runtime.

However, like Lambda-eek [13], we believe that while an interoperating calculus such as SD is not necessarily suitable as a proof system, it is interesting as a programming language in its own right.

5.2 Decidable Typechecking

A related question to the soundness of $\lambda^\leq$ is whether the typechecking of SD is decidable in the presence of term evaluation in types. With our current formulation of $\lambda^\rightarrow$ and $\lambda^\leq$, we believe (but do not prove) that SD is strongly normalizing and thus typechecking of SD is decidable. We believe that this is reasonable given that both $\lambda^\rightarrow$ and $\lambda^\leq$ appear to be strongly normalizing and the type-directed boundaries that we consider in SD themselves do not contribute any additional computational power to the language.

Irrespective of this, it is clear that we can make SD typechecking undecidable by giving $\lambda^\rightarrow$ recursive functions. This is because we determine the equivalence of $t_1 \cong t_2$ by $\beta$-reduction as per the EQ_DTM_STEP rule (Figure 9). With recursive functions in $\lambda^\rightarrow$, evaluation of a DS boundary could end up in an infinite loop.

Because our actual $\lambda^\rightarrow$ language will likely be a general-purpose functional language with recursion, how might we recover decidable typechecking in this scenario? One such approach is to introduce a purity check in $\lambda^\leq$ that restricts boundaries from being embedded in types. This is a clean way to regain decidable typechecking but at the cost of losing the ability to embed terminating boundary terms in types.

Finally, we may give up the ambition that the typechecker automatically decides term equivalence by evaluating terms, and instead require the programmer to add explicit annotations stating what should be evaluated for how many steps. An example of a language taking this approach is Guru [29].

5.3 Lumping and Non-termination

One tempting suggestion to alleviate the problem of decidable typechecking is to limit how we can compute with values across the boundary. Rather than marshaling values, perhaps we can treat data on the other side of the boundary as an opaque lump that we can carry around and give back, but otherwise not inspect its contents. We give the evaluation rules in Figure 11. While appealing at first glance, it turns out that this system admits non-termination.

In the lump variant of our rules, we introduce a type $L$ that represents an opaque lump value contained in a boundary. With lumps, boundaries no longer marshal values between languages or otherwise look at their structure. Instead, boundaries are “canceled out” when they meet each other as per EVALSTM_SD_LUMP and EVAL_DTM_DS_LUMP. The problem is that it turns out that you can write an infinite loop with these boundaries in a similar manner to type dynamic [1] where you use a pair of functions of type $L \rightarrow (L \rightarrow L)$ and $(L \rightarrow L) \rightarrow L$ to encode a term $\Omega$ that loops. The actual terms for these functions and $\Omega$ are the same as Matthews’ and Findler’s versions for their ML-in-ML calculus [20] but adapted to our boundaries.
Because of this, any interoperability boundary between simply- and dependently-typed languages using a lump style induces undecidable typechecking if boundaries can appear in dependent types and reduce.

6 Comparisons

Many real-world dependently-typed languages provide some facilities for interoperability with simply-typed languages. However we know of no language that provides the flexibility suggested by SD. Now that we’ve established SD and its properties, it is instructive to compare the techniques used by these dependently-typed languages with how SD establishes its interoperability boundaries for two reasons. First, if SD can accurately describe the interoperability features of these languages, then it builds confidence that SD is a good model for dependent interoperability in general. And second, the differences between the two suggests ways that the dependently-typed language can improve its interoperability support, or conversely, why it may be hard to do so.

6.1 ATS Data Translation

ATS [6] is built with interoperability with C in mind. Since the two languages share the same data representation, marshaling is relatively trivial. ATS values are typically exposed to C as wrapped structs, e.g., a C int has type \texttt{ats.int.type} in ATS. ATS functions can be exposed to C via \texttt{extern} declarations and C code can either be inline into ATS files or referenced as external values or types. In this sense, ATS closely mimics the two-way interoperability boundary of SD.

However, beyond basic type-checking, ATS interoperability makes no attempt at checking to see if dependent type properties are preserved when traveling in and out of C. This is because with arbitrary casts, C code can arbitrarily munge ATS values or otherwise break the type guarantees made by ATS.

6.2 Extraction in Coq

The theorem prover Coq [32] provides a mechanism, \texttt{Extraction}, that extracts functional programs written in OCaml (or other functional languages such as Haskell) from proofs of specifications [15]. Coq distinguishes between computationally relevant types (\texttt{Sets}) and computationally irrelevant types (\texttt{Props}) and uses that information to guide \texttt{Extraction}. Datatypes extracted from Coq are translated into comparable datatypes in ML. Alternatively, Coq provides a mechanism for the user to map a Coq datatype and its associated constructors into a ML datatype and its constructors.

For our purposes, \texttt{Extraction} is a form of one-way interoperability where ML code can use verified Coq code. If we imagine the extracted program as living in $\lambda \rightarrow $ and the ML code living in $\lambda \Rightarrow $, then this amounts to only allowing the user to call $\lambda \Rightarrow $ code via a SD boundary.

However, there are several limitations to the one-way interoperability model offered by \texttt{Extraction}:

1. \textbf{Extracted code does not enforce the properties of datatypes.} By design the extracted code is correct up to the verification done in Coq. However, because of erasure, the extracted code cannot verify that ML data passed to it meets the pre-conditions (if any) to use that code. For example, our \texttt{List} example datatype would be erased to a simple \texttt{List} in ML. If the extracted code depends on receiving a non-empty \texttt{List} then it must trust the user to give it a non-empty \texttt{List} rather than enforcing that pre-condition itself.

2. \textbf{User-defined translation of datatypes is simple macro replacement.} In SD, the user-defined translation function \texttt{argToS} is any function from the arguments of the $\lambda \Rightarrow $ constructor to the $\lambda \rightarrow $ constructor that respects the properties we outlined in the previous sections. In Coq, the analogous \texttt{Extract Inductive} command performs a macro-replacement of the occurrences of the datatype and its constructors with the strings specified with the commands. The resulting ML code is not even checked for well-formedness.
6.3 Agda Data Translation

Agda [23] provides a foreign-function interface that allows Agda to call into Haskell code. As part of the FFI, the user specifies Haskell functions to call from Agda with the {{-# COMPILED #-}} pragma. The user can also specify translations from Agda datatypes to Haskell datatypes via the {{-# COMPILED_DATA ... #-}} pragma.

Like Coq Extraction, the Agda FFI is a one-way interoperability layer. The difference is that the FFI allows Agda, the dependently-typed language, to invoke Haskell code, the simply-typed language. Translation occurs when Agda invokes a Haskell function. The arguments are converted to Haskell and the return value converted back to Agda according to the FFI’s built in rules to translate Agda types coupled with the declared COMPILED_DATA pragmas.

Agda’s FFI suffers from problems similar to Coq Extraction due to the restrictive nature of Agda’s translation function. Agda erases terms in types down to unit so the translation has no way of preserving or even checking to see if the properties of dependent types are preserved. Unlike Coq Extraction’s macro-based datatype compatibility declarations, Agda’s compatibility declarations are type-directed. However, they are still less flexible than SD as you can only map constructors of the same number of arguments and types.

6.4 Coq’s Program Tactic

Coq’s Program tactic [28] offers a different flavor of interoperability than Extraction. Program allows the user to write dependently-typed code in the form of predicate subtyping [27] over terms, but using a simply-typed language instead. This simply-typed language is a relaxed version of Coq’s term language, but could very well be OCaml or Haskell instead.

The workflow of Program occurs in two steps:

1. The user writes a program in the simply-typed fragment. This includes predicates over types written in the refinement style \{x \mid P\}. The user does not need to write any proofs during this step.

2. Coq elaborates the program into Coq terms and then generates a series of proof obligations that the user must discharge. The result is a complete Coq term that is the program that meets the specifications outlined via the predicates of the program.

Program is an example of a dependently-typed system utilizing the power of a simply typed system to do interesting work. We can view the elaboration step from the simply-typed fragment to Coq as a translation from \(\lambda \rightarrow\) to \(\lambda \cong\) where we are interested in using \(\lambda \cong\) to prove properties of the \(\lambda \rightarrow\) program.

7 Prior Work

We believe our work is the first to directly address the technical challenges involved with interoperating between a dependently-typed and simply-typed programming language. However, there has been considerable effort in related areas that we highlight here.

Interoperability Implementation Since different programming languages typically operate under different runtime environments, much of the early work in interoperability research focuses how to reconcile those environments. Frequently the analysis takes specific pairs of languages, usually C, with other languages such as Java [7], ML [4], and Haskell [5], but sometimes also with other language pairs such as Python to Scheme [25] or SML to Java [22]. Other approaches attempt to develop a lingua franca by which two languages can communicate such as C [3], the Java virtual machine, COM [26], or the .NET framework [30].
Interoperability Semantics  There has been comparatively less work in understanding the semantics of interoperating languages. We extend Matthews's and Findler's original work [20] that showed that even with simple language pairs — untyped and simply-typed lambda calculi — interoperability leads to some surprising results. Their latest work in this area focuses on adding polymorphism to a interoperability setting while preserving parametricity [19].

Mixing Dependency with Dynamic  A different thread of related research comes from analyses of dependently-typed languages intermixed with type dynamic [1]. Ou et al [24] introduce simple and dependent constructs in which dynamically-typed and dependently-typed, respectively, exists. They allow for nesting of such constructs (e.g., simple{dynamic{...}}) and provide rules for how simple blocks dynamically enforce constraints imposed by dependent blocks. Gronski et al [12] extend this approach to a pure-type system without explicit, separate constructs for dynamic and dependent types. Instead, they include dynamic as a base type and assume the rest of the world is dependent.

Refinement Types and Contracts  The underlying framework for many of these systems is the theory of refinement types [10] and higher-order contracts [8]. Recently, the study of contracts has gone in many directions, for example assigning blame [33]. Directly relevant to our work is the study of dependent contracts, e.g., the systems studied by Greenberg et al [11].

8 Future Work and Conclusion

We tackle the problem of making dependently-typed programming more accessible from the viewpoint of interoperability. Can we author an interoperability boundary between a dependently-typed language and a simply-typed language that preserves the properties enforced by the dependently-typed language? Our solution, the language SD, is able to meet design goals we set forth for such an interoperability layer: using code from one language from within the other language and verifying properties of simply-typed code with the dependently-typed language.

In the future, we would like to apply the ideas in this paper to improve the interop support of real-world languages like Coq and Agda, e.g., adding true “two-way” interoperability. Theoretically, there is also room for more careful analysis: proofs of strong normalization and a theorem characterizing when boundaries can be inserted without changing program behavior in harmful ways.

There are also more design variations for SD worth exploring. In particular, we restrict datatype indices at boundaries to be first-order. While this is not a serious limitation, it would be interesting to adapt ideas from the contracts literature and decompose equality checks of functions into checks at their use sites during type conversion. Finally, we can move beyond the pairing of dependent and simple types are explore other combinations such as dependent and dynamic types and pairings involving linear types.

References


A The Full Language

Figures 12 through 28 gives the full syntax and semantics of SD.
\begin{align*}
\lambda \rightarrow \text{Types} \quad S &::= S_1 \to S_2 \mid S_1 \ast S_2 \mid \text{Unit} \mid A \\
\lambda \rightarrow \text{Terms} \quad s &::= x \mid \lambda x : S . s \mid s_1 . s_2 \\
&\quad \mid <s_1, s_2> \mid s . 1 \mid s . 2 \\
&\quad \mid C . s \mid \text{case } s \text{ of } C_i . x_i \to s_i^i \\
&\quad \mid \text{unit} \mid \text{error} \mid \text{let } d y = t \text{ in } s \mid SD^S_T t
\end{align*}

\begin{align*}
\lambda \Rightarrow \text{Kinds} \quad K &::= * \mid T \Rightarrow *
\\
\lambda \Rightarrow \text{Types} \quad T &::= (y : T_1) \to T_2 \mid T . t \\
&\quad \mid (y : T_1) \ast T_2 \mid \text{Unit} \mid B \\
\lambda \Rightarrow \text{Terms} \quad t &::= y \mid \lambda y : T . t \mid t_1 . t_2 \\
&\quad \mid <t_1, t_2> \mid t . 1 \mid t . 2 \\
&\quad \mid C . t \mid \text{case } t \text{ of } C_i . y_i \to t_i^i \\
&\quad \mid \text{unit} \mid \text{error} \\
&\quad \mid DS^T_S s \mid t_1 \triangleq t_2 \triangleright t_3
\end{align*}

Figure 12: SD Syntax
\( \Gamma \vdash s : S \)

\( \vdash \Gamma \)
\( x : S \in \Gamma \quad \text{WF}_\text{STM}_\text{VAR} \)
\( \vdash x : S \)

\( \vdash \lambda x : S_1, s : S_2 \rightarrow S \quad \text{WF}_\text{STM}_\text{ABS} \)

\( \Gamma \vdash s_1 : S_1 \rightarrow S_2 \)
\( \Gamma \vdash s_2 : S_1 \quad \text{WF}_\text{STM}_\text{APP} \)
\( \Gamma \vdash s_1 \cdot s_2 : S_2 \)

\( \Gamma \vdash s : S_1 \rightarrow S_2 \)
\( \Gamma \vdash s_1 : S_1 \quad \Gamma \vdash s_2 : S_2 \quad \text{WF}_\text{STM}_\text{PAIR} \)
\( \Gamma \vdash s : S_1 \ast S_2 \)

\( \Gamma \vdash s.i : S_i \quad \text{WF}_\text{STM}_\text{PROJ1} \)
\( \Gamma \vdash s.2 : S_2 \quad \text{WF}_\text{STM}_\text{PROJ2} \)

\( \Gamma \vdash s : A \quad \text{constrs } A = C_i^i \)
\( \Gamma, x_i : S_i^i \vdash s_i : S_i^i \quad \text{WF}_\text{STM}_\text{CTOR} \)
\( \Gamma \vdash \text{case } s \text{ of } C_i^i x_i \rightarrow s_i^i : S \quad \text{WF}_\text{STM}_\text{CASE} \)

\( \vdash \Gamma \quad \Gamma \vdash t : T \quad \Gamma, y : T \vdash s : S \quad \text{WF}_\text{STM}_\text{UNIT} \quad \text{WF}_\text{STM}_\text{LETD} \)
\( \vdash \Gamma \quad \Gamma \vdash \text{letd } y = t \text{ in } s : S \quad \text{WF}_\text{STM}_\text{LETD} \)

\( \Gamma \vdash t : T \)
\( S \leftrightarrow T \quad \text{WF}_\text{STM}_\text{SD} \)
\( \Gamma \vdash S D_T^T : t : S \quad \vdash \Gamma \quad \Gamma \vdash \text{error} : S \quad \text{WF}_\text{STM}_\text{ERROR} \)

Figure 13: \( \lambda \rightarrow \) Typing
\[ \Gamma \vdash K \]

\[ \frac{\Gamma \vdash \star}{\Gamma \vdash T \Rightarrow \star} \quad \text{WF\_DKN\_PROP} \]

\[ \frac{\Gamma \vdash T : \star}{\Gamma \vdash \star \Rightarrow \star} \quad \text{WF\_DKN\_ARR} \]

\[ \Gamma \vdash T : K \]

\[ \frac{\Gamma, y : T_1 \vdash T_2 : \star \quad \text{WF\_DTY\_ARR}}{\Gamma \vdash (y : T_1) \rightarrow T_2 : \star} \]

\[ \frac{\Gamma \vdash t : T_1 \quad \Gamma \vdash T : T_1 \Rightarrow \star}{\Gamma \vdash T \star \Rightarrow \star} \quad \text{WF\_DTY\_APP} \]

\[ \frac{\Gamma \vdash t_1 : \star \quad \Gamma \vdash t_2 : \star \quad \text{WF\_DTY\_PAIR}}{\Gamma \vdash (y : T_1) \star T_2 : \star} \]

\[ \frac{\Gamma \vdash \text{Unit} : \star \quad \text{WF\_DTY\_UNIT}}{\Gamma \vdash \text{Unit} : \star} \]

\[ \frac{B : T \Rightarrow \star \in \Psi_0}{\Gamma \vdash B : T \Rightarrow \star} \quad \text{WF\_DTY\_DATA} \]

Figure 14: \( \lambda^\infty \) Kinding
\( \text{Figure 15: } \lambda^n \text{ Typing} \)
\[ \vdash \Psi \]

\[ \vdash \Psi \]
\[ \text{WF_SIG_EMPTY} \]
\[ \vdash \Psi \]
\[ A \in \Psi \]
\[ \text{WF_SIG_SCTOR} \]
\[ \vdash \Psi, C : S \rightarrow A \]
\[ \vdash \Psi \]
\[ A \notin \Psi \]
\[ \text{WF_SIG_STYCTOR} \]
\[ \vdash \Psi, A \]

\[ \vdash \Psi \]
\[ \vdash \Psi \]
\[ \cdot \vdash (y : T_2) \rightarrow B \ t : * \]
\[ \text{WF_SIG_DCTOR} \]
\[ \vdash \Psi, C : (y : T_2) \rightarrow B \ t \]
\[ \vdash \Psi \]
\[ \cdot \vdash T : * \]
\[ \text{WF_SIG_DTYCTOR} \]
\[ \vdash \Psi, B : T \Rightarrow * \]

\[ \vdash \Gamma \]
\[ \text{WF_CTX_EMPTY} \]
\[ \vdash \Gamma \]
\[ \cdot \vdash \Gamma, x : S \]
\[ \text{WF_CTX_CONS} \]
\[ \vdash \Gamma \]
\[ \vdash \Gamma \]
\[ \cdot \vdash \Gamma \]
\[ \Gamma \vdash T : * \]
\[ \Gamma \vdash t : T \]
\[ \text{WF_CTX_DCONS} \]
\[ \vdash \Gamma, y : T \]
\[ \Gamma \vdash t' : T' \]
\[ \vdash \Gamma, t \equiv t' \]
\[ \text{WF_CTX_EQUIV} \]

Figure 16: Auxiliary definitions
Figure 17: Auxiliary definitions (cont.)
\[ \Gamma \vdash K \equiv K' \]

\[ \Gamma \vdash * \equiv * \quad \text{EQ_DKN_REFL} \]
\[ \Gamma \vdash T \equiv T' \quad \text{EQ_DKN_PI} \]
\[ \Gamma \vdash T \Rightarrow * \equiv T' \Rightarrow * \]

Figure 18: \(\lambda^{=\approx}\) Kind Equivalence

\[ \Gamma \vdash T \equiv T' \]

\[ \frac{B : K \in \Psi_0}{\Gamma \vdash B \equiv B} \quad \text{EQ_DTY_TREFL} \]
\[ \frac{\Gamma \vdash T_1 \equiv T'_1 \quad \Gamma \vdash T_2 \equiv T'_2}{\Gamma \vdash (y : T_1) \to T_2 \equiv (y : T'_1) \to T'_2} \quad \text{EQ_DTY_PI} \]
\[ \frac{\Gamma \vdash T \equiv T' \quad C \neq C'}{\Gamma \vdash C \equiv C'} \quad \text{EQ_DTY_INCON} \]
\[ \frac{\Gamma \vdash T_1 \equiv T'_1 \quad \Gamma \vdash T_2 \equiv T'_2}{\Gamma \vdash (y : T_1) \ast T_2 \equiv (y : T'_1) \ast T'_2} \quad \text{EQ_DTY_SIGMA} \]
\[ \frac{\Gamma \vdash T \equiv T' \quad \Gamma \vdash t \equiv t'}{\Gamma \vdash \text{Unit} \equiv \text{Unit} \quad \text{EQ_DTY_UREFL}} \]
\[ \frac{\Gamma \vdash t \equiv t'}{\Gamma \vdash T \equiv T' \quad \text{EQ_DTY_App}} \]

Figure 19: \(\lambda^{=\approx}\) Type Equivalence
\[ \Gamma \vdash t \equiv t' \]

\[
\begin{align*}
& t \equiv t' \in \Gamma \\
\ & \Gamma \vdash t \equiv t' \quad \text{EQ\_DTM\_ASSUMPTION} \\
& t \rightarrow t' \\
\ & \Gamma \vdash t \equiv t' \quad \text{EQ\_DTM\_STEP} \\
\end{align*}
\]

\[
\begin{align*}
\ & \Gamma \vdash t \equiv t' \quad \text{EQ\_DTM\_REFL} \\
\ & \Gamma \vdash t \equiv t' \quad \text{EQ\_DTM\_SYM} \\
\ & \Gamma \vdash t \equiv t' \quad \text{EQ\_DTM\_TRANS} \\
\end{align*}
\]

\[
\begin{align*}
& y \not\in \text{dom}(\Gamma) \\
\ & \Gamma \vdash t \equiv t' \\
\ & \Gamma \vdash [t/y]t \equiv [t'/y]t \quad \text{EQ\_DTM\_SUBST} \\
\ & \Gamma \vdash [v/y]t \equiv [v/y]t' \quad \text{EQ\_DTM\_SUBST\_VAL} \\
\end{align*}
\]

\[
\begin{align*}
& x \not\in \text{dom}(\Gamma) \\
\ & \Gamma \vdash [u/x]t \equiv [u/x]t' \quad \text{EQ\_DTM\_SSUBST\_VAL} \\
\end{align*}
\]

Figure 20: \( \lambda^= \) Term Equivalence

\[
\begin{align*}
\lambda \to \text{Contexts} \quad \mathcal{E}_s & : = \quad \square \mid \square s \mid u \square \mid \langle \square , s \rangle \mid \langle u , \square \rangle \\
& \mid \quad \square .1 \mid \square .2 \mid C \square \\
& \mid \quad \text{case}\quad \square \text{of} \quad C : i \rightarrow s_i \mid \text{letd}\ y = \square \text{in} \ s \mid \text{SD}_T \square \\
\end{align*}
\]

\[
\begin{align*}
\lambda^= \text{Contexts} \quad \mathcal{E}_t & : = \quad \square \mid \square t \mid v \square \mid \langle \square , t \rangle \mid \langle v , \square \rangle \\
& \mid \quad \square .1 \mid \square .2 \mid C \square \\
& \mid \quad \text{case}\quad \square \text{of} \quad C : i \rightarrow t_i \mid \text{DS}_T \square \mid \square \equiv t_1 \triangleright t \mid v_0 \equiv \square \triangleright t \\
\end{align*}
\]

Figure 21: Evaluation contexts
Figure 22: $\lambda \rightarrow$ Evaluation
Figure 23: $\lambda^n$ Evaluation
Figure 24: Parallel reduction (simple terms)
Figure 25: Parallel reduction (simple terms, cont.)
Figure 26: Parallel reduction (dependent terms)
\[
\begin{array}{c}
t \rightarrow_p t' \\
t_i \rightarrow_p t_i'
\end{array}
\]
\[\text{PAR_EVAL_DTM_CASE}\]

\[
\begin{array}{c}
v \rightarrow_p v' \\
t_i \rightarrow_p t_i'
\end{array}
\]
\[\text{PAR_EVAL_DTM_CASE_BETA}\]

case \(C_i\) of \(C_i\) 
\[
\begin{array}{c}
t \rightarrow_p t' \\
t_i \rightarrow_p t_i'
\end{array}
\]
\[\text{PAR_EVAL_DTM_CASE}\]

case \(C_i\) of \(C_i\) 
\[
\begin{array}{c}
v \rightarrow_p v' \\
t_i \rightarrow_p t_i'
\end{array}
\]
\[\text{PAR_EVAL_DTM_CASE_BETA}\]

\[
\begin{array}{c}
T \rightarrow_p T' \\
S \rightarrow_p S'
\end{array}
\]
\[\text{PAR_EVAL_DTM_DS}\]

\[
\begin{array}{c}
DS_s^T s \rightarrow_p DS_{S'}^T s'
\end{array}
\]
\[\text{PAR_EVAL_DTM_DS}\]

\[
\begin{array}{c}
T_1 \rightarrow_p T'_1 \\
S_1 \rightarrow_p S'_1 \\
S_3 \rightarrow_p S'_3
\end{array}
\]
\[\text{PAR_EVAL_DTM_DS_ABS}\]

\[
\begin{array}{c}
DS_{(S_1 \rightarrow S_2)} (\lambda x: S_3.s) \rightarrow_p \lambda y: T_1'.DS_{S_2'}^{T_2'}((\lambda x: S_3'.s')(SD_{S_1'}^{T_1'})y)
\end{array}
\]
\[\text{PAR_EVAL_DTM_DS_ABS}\]

\[
\begin{array}{c}
T_1 \rightarrow_p T'_1 \\
S_1 \rightarrow_p S'_1 \\
u_1 \rightarrow_p u'_1
\end{array}
\]
\[\text{PAR_EVAL_DTM_DS_PAIR}\]

\[
\begin{array}{c}
(T_1 \rightarrow_p T'_1) \cdot (S_2 \rightarrow_p S'_2)
\end{array}
\]
\[\text{PAR_EVAL_DTM_DS_PAIR}\]

\[
\begin{array}{c}
DS_{A}^{(B T_1)} (C u) \rightarrow_p t' \equiv [v/y] t_1 \triangleright (C v)
\end{array}
\]
\[\text{PAR_EVAL_DTM_DS_CONSTR}\]

\[
\begin{array}{c}
t_1 \rightarrow_p t_1' \\
t_2 \rightarrow_p t_2'
\end{array}
\]
\[\text{PAR_EVAL_DTM_GUARD}\]

\[
\begin{array}{c}
t \rightarrow_p t'
\end{array}
\]
\[\text{PAR_EVAL_DTM_GUARD_REFL}\]

\[
\begin{array}{c}
t_1 \rightarrow_p v \\
t_2 \rightarrow_p v
\end{array}
\]
\[\text{PAR_EVAL_DTM_GUARD_REFL}\]

\[
\begin{array}{c}
v \equiv v \triangleright t \rightarrow_p t
\end{array}
\]
\[\text{PAR_EVAL_DTM_GUARD_REFL}\]

\[
\begin{array}{c}
DS_{Unit} Unit \rightarrow_p Unit
\end{array}
\]
\[\text{PAR_EVAL_DTM_DS_UNIT}\]

Figure 27: Parallel reduction (dependent terms, cont.)
Figure 28: Parallel reduction (simple and dependent types)
B Proofs

B.1 Structural Properties

Lemma 9. Free variables in typing judgments

1. If $\Gamma \vdash t : T$ then $\text{fv}(t) \subseteq \text{dom}(\Gamma)$ and $\text{fv}(T) \subseteq \text{dom}(\Gamma)$.

2. If $\Gamma \vdash T : K$ then $\text{fv}(T) \subseteq \text{dom}(\Gamma)$ and $\text{fv}(K) \subseteq \text{dom}(\Gamma)$.

3. If $\Gamma \vdash K$ then $\text{fv}(K) \subseteq \text{dom}(\Gamma)$.

4. If $\Gamma \vdash s : S$ then $\text{fv}(s) \subseteq \text{dom}(\Gamma)$ and $\text{fv}(S) \subseteq \text{dom}(\Gamma)$.

Lemma 10. Weakening for Equivalence

1. If $\Gamma_1, \Gamma_3 \vdash t \equiv t'$. then $\Gamma_1, \Gamma_2, \Gamma_3 \vdash t \equiv t'$.

2. If $\Gamma_1, \Gamma_3 \vdash T \equiv T'$. then $\Gamma_1, \Gamma_2, \Gamma_3 \vdash T \equiv T'$.

3. If $\Gamma_1, \Gamma_3 \vdash K \equiv K'$. then $\Gamma_1, \Gamma_2, \Gamma_3 \vdash K \equiv K'$.

Proof. Proof by mutual induction on the typing derivations.

Lemma 11. Weakening

1. If $\Gamma_1, \Gamma_3 \vdash t : T$ and $\vdash \Gamma_1, \Gamma_2, \Gamma_3$ then $\Gamma_1, \Gamma_2, \Gamma_3 \vdash t : T$.

2. If $\Gamma_1, \Gamma_3 \vdash s : S$ and $\vdash \Gamma_1, \Gamma_2, \Gamma_3$ then $\Gamma_1, \Gamma_2, \Gamma_3 \vdash s : S$.

3. If $\Gamma_1, \Gamma_3 \vdash T : K$ and $\vdash \Gamma_1, \Gamma_2, \Gamma_3$ then $\Gamma_1, \Gamma_3, \Gamma_3 \vdash T : K$.

4. If $\Gamma_1, \Gamma_3 \vdash K : T$ and $\vdash \Gamma_1, \Gamma_2, \Gamma_3$ then $\Gamma_1, \Gamma_3, \Gamma_3 \vdash K : T$.

5. If $\vdash \Gamma_1, \Gamma_2$ then $\vdash \Gamma_1$

Proof. Proof by mutual induction on the typing derivations.

Lemma 12 (Values are closed under substitution). For any values $v_1$, $v_2$, $u_1$, $u_2$, the substituted terms $[v_1/y]u_2$, $[u_1/x]v_2$, $[v_1/y]u_2$, and $[u_1/x]u_2$ are also values.

Proof. Simple induction on the structure of values.

Lemma 13 (Substitution of us for Equivalence).

1. $\Gamma_1, x_2:S_2, \Gamma_2 \vdash T \equiv T'$ and $\Gamma_1 \vdash u_2 : S_2$ then $\Gamma_1, [u_2/x_2]\Gamma_2 \vdash [u_2/x_2]T \equiv [u_2/x_2]T'$.

2. $\Gamma_1, x_2:S_2, \Gamma_2 \vdash K \equiv K'$ and $\Gamma_1 \vdash u_2 : S_2$ then $\Gamma_1, [u_2/x_2]\Gamma_2 \vdash [u_2/x_2]K \equiv [u_2/x_2]K'$.

3. $\Gamma_1, x_2:S_2, \Gamma_2 \vdash t \equiv t'$ and $\Gamma_1 \vdash u_2 : S_2$ then $\Gamma_1, [u_2/x_2]\Gamma_2 \vdash [u_2/x_2]t \equiv [u_2/x_2]t'$.

Proof. By mutual induction on the three derivations. The cases for $\Gamma, x_2:S_2, \Gamma_2 \vdash T \equiv T'$ are:

Case $\text{eq_dty_incon}$: The rule looks like

$$
\Gamma \vdash C \equiv C' \quad \Gamma \vdash T \equiv T' \\
\frac{}{\text{EQ_DTY_INCON}}
$$

By the mutual IH we get $\Gamma_2, [u_2/x]\Gamma_2 \vdash [u_2/x](C \equiv C'(C \equiv C'))$. Since $[u_2/x](C \equiv C') = C [u_2/x]v$ this is still a contradiction and we can re-apply $\text{EQ_DTY_INCON}$. 

38
Case **eq_dty_urefl**: The rule looks like

\[ \Gamma \vdash \text{Unit} \equiv \text{Unit}^{\text{EQ_DTY_UREFL}} \]

We must show \( \Gamma_1, [u_2/x_2] \Gamma_2 \vdash [u_2/x] \text{Unit} \equiv [u_2/x] \text{Unit} \). But \( [u_2/x] \text{Unit} = \text{Unit} \), so we can just apply \text{EQ_DTY_UREFL} again.

Case **eq_dty_trefl**: Similar to the case for \text{EQ_DTY_UREFL}.

Case **eq_dty_pi**: The rule looks like

\[ \begin{align*}
\Gamma & \vdash T_1 \equiv T_1' \\
\Gamma & \vdash T_2 \equiv T_2' \\
\Gamma & \vdash (y: T_1) \to T_2 \equiv (y: T_1') \to T_2' \quad \text{EQ_DTY_PI}
\end{align*} \]

We must show \( \Gamma_1, [u_2/x_2] \Gamma_2 \vdash [u_2/x_2] (y: T_1) \to T_2 \equiv [u_2/x_2] (y: T_1') \to T_2' \). Since \( y \) is a bound variable we can pick it fresh, so this is the same as showing \( \Gamma_1, [u_2/x_2] \Gamma_2 \vdash (y: [u_2/x_2] T_1) \to [u_2/x_2] T_2 \equiv (y: [u_2/x_2] T_1') \to [u_2/x_2] T_2' \). By the IH we get \( \Gamma_1, [u_2/x_2] \Gamma_2 \vdash [u_2/x_2] T_1 \equiv [u_2/x_2] T_1' \) and \( \Gamma_1, [u_2/x_2] \Gamma_2 \vdash [u_2/x_2] T_2 \equiv [u_2/x_2] T_2' \), then re-apply \text{EQ_DTY_PI}.

Case **eq_dty_sigma**: Similar to \text{EQ_DTY_PI}.

Case **eq_dty_app**: The rule looks like

\[ \begin{align*}
\Gamma & \vdash T \equiv T' \\
\Gamma & \vdash t \equiv t' \\
\Gamma & \vdash T t \equiv T' t' \quad \text{EQ_DTY_APP}.
\end{align*} \]

We get \( \Gamma_1, [u_2/x] \Gamma_2 \vdash [u_2/x] T \equiv [u_2/x] T' \) by IH, and \( \Gamma_1, [u_2/x_2] \Gamma_2 \vdash [u_2/x_2] t \equiv [u_2/x_2] t' \) by the mutual IH. Then we can re-apply \text{EQ_DTY_APP}.

The cases for \( \Gamma_1, x_2:S_2, \Gamma_2 \vdash K \equiv K' \) are:

Case **eq_dkn_refl**: Similar to \text{EQ_DTY_UREFL}.

Case **eq_dkn_pi**: Similar to \text{EQ_DTY_PI}.

The cases for \( \Gamma_1, x_2:S_2, \Gamma_2 \vdash t \equiv t' \) are:

Case **eq_dtm_assumption**: We have \( t \equiv t' \in \Gamma_1, x_2:S_2, \Gamma_2 \) as a premise to the rule. There are two cases: either \( t \equiv t' \in \Gamma_1 \) or \( t \equiv t' \in \Gamma_2 \). If \( t \equiv t' \in \Gamma_1 \), then we also have \( t \equiv t' \in \Gamma_1, [u_2/x_2] \Gamma_2 \). So the conclusion follows by \text{EQ_DTM_ASSUMPTION} followed by \text{EQ_DTM_SUBST}. If \( t \equiv t' \in \Gamma_2 \) then \( [u_2/x_2] t \equiv [u_2/x_2] t' \in \Gamma_1, [u_2/x_2] \Gamma_2 \), so the conclusion follows by just \text{EQ_DTM_ASSUMPTION}.

Case **eq_dtm_step**: By \text{EQ_DTM_STEP} followed by \text{EQ_DTM_SUBST}.

Case **eq_dtm_refl, eq_dtm_sym, eq_dtm_trans**: These all go directly by IH.

Case **eq_dtm_subst**: The rule looks like

\[ \begin{align*}
\Gamma & \vdash t_1 \equiv t_1' \\
y & \notin \text{dom} (\Gamma) \\
\Gamma & \vdash [t_1/y] t \equiv [t_1'/y] t \quad \text{EQ_DTM_SUBST}
\end{align*} \]

By the IH (instantiated with \( u_2 \)) we get \( \Gamma_1, [u_2/x_2] \Gamma_2 \vdash [u_2/x_2] t_1 \equiv [u_2/x_2] t_1' \).

So by \text{EQ_DTM_SUBST}, taking \([u_2/x] t\) as the template, we get

\[ \Gamma_1, [u_2/x] \Gamma_2 \vdash [[u_2/x_2] t_1/y] [u_2/x_2] t \equiv [[u_2/x_2] t_1'/y] [u_2/x_2] t. \]
Now by the assumption \( \Gamma \vdash u_2 : S_2 \), lemma 9 and the premise \( y \notin \text{dom}(\Gamma_1, x_2 : S_2, \Gamma_2) \) we know that \( y \) is not free in \( u_2 \). So we can commute the substitution to get
\[
\Gamma_1, [u_2 / x] \Gamma_2 \vdash [u_2 / x_2][t_1 / y]t \equiv [u_2 / x_2][t'_1 / y]t,
\]
which is what we needed to show.

Case \text{eq_dtm_subst_val}: The typing rule looks like
\[
\Gamma \vdash t \equiv t' \\
y \notin \text{dom}(\Gamma) \\
\Gamma \vdash [v / y]t \equiv [v / y]t' \quad \text{EQ_DTM_SUBST_VAL}
\]

By the IH we have \( \Gamma, [u_2 / x] \Gamma_2 \vdash [u_2 / x]t \equiv [u_2 / x]t \). Values are closed under substitution of values (lemma 12), so \([u_2 / x]v \) is a value. Applying EQ_DTM_SUBST_VAL we get
\[
\Gamma, [u_2 / x] \Gamma_2 \vdash [[u_2 / x_2]v / y][u_2 / x_2]t \equiv [[u_2 / x_2]v / y][u_2 / x_2]t'
\]
By the assumption \( \Gamma \vdash u_2 : S_2 \), lemma 9, and the premise \( y \notin \text{dom}(\Gamma_1, x_2 : S_2, \Gamma_2) \) we know that \( y \) is not free in \( u_2 \), so we can commute the substitutions and get
\[
\Gamma_1, [u_2 / x] \Gamma_2 \vdash [u_2 / x_2][v / y]t \equiv [u_2 / x_2][v / y]t'
\]
which is what we needed to show.

Case \text{eq_dtm_ssubst_val}: Similar to the previous case.

\[\square\]

Lemma 14 (Substitution of vs for Equivalence).

1. If \( \Gamma_1, y_2 : T_2, \Gamma_2 \vdash T \equiv T' \) and \( \Gamma_1 \vdash v_2 : T_2 \) then \( \Gamma_1, [v_2 / y_2] \Gamma_2 \vdash [v_2 / y_2] T \equiv [v_2 / y_2] T' \).

2. If \( \Gamma_1, y_2 : T_2, \Gamma_2 \vdash K \equiv K' \) and \( \Gamma_1 \vdash v_2 : T_2 \) then \( \Gamma_1, [v_2 / y_2] \Gamma_2 \vdash [v_2 / y_2] K \equiv [v_2 / y_2] K' \).

3. If \( \Gamma_1, y_2 : T_2, \Gamma_2 \vdash t \equiv t' \) and \( \Gamma_1 \vdash v_2 : T_2 \) then \( \Gamma_1, [v_2 / y_2] \Gamma_2 \vdash [v_2 / y_2] t \equiv [v_2 / y_2] t' \).

Proof: Similar to the previous lemma.

\[\square\]

Lemma 15 (Substitution of us).  

1. If \( \Gamma_1, x_2 : S_2, \Gamma_2 \vdash t_1 : T_1 \) and \( \Gamma_1 \vdash u_2 : S_2 \) then \( \Gamma_1, [u_2 / x_2] \Gamma_2 \vdash [u_2 / x_2] t_1 : [u_2 / x_2] T_1 \).

2. If \( \Gamma_1, x_2 : S_2, \Gamma_2 \vdash s_1 : S_1 \) and \( \Gamma_1 \vdash u_2 : S_2 \) then \( \Gamma_1, [u_2 / x_2] \Gamma_2 \vdash [u_2 / x_2] s_1 : [u_2 / x_2] S_1 \).

3. If \( \Gamma_1, x_2 : S_2, \Gamma_2 \vdash T : K \) and \( \Gamma_1 \vdash u_2 : S_2 \) then \( \Gamma_1, [u_2 / x_2] \Gamma_2 \vdash [u_2 / x_2] T : [u_2 / x_2] K \).

4. If \( \Gamma_1, x_2 : S_2, \Gamma_2 \vdash K \) and \( \Gamma_1 \vdash u_2 : S_2 \) then \( \Gamma_1, [u_2 / x_2] \Gamma_2 \vdash [u_2 / x_2] K \).

5. If \( \vdash \Gamma_1, x_2 : S_2, \Gamma_2 \) and \( \Gamma_1 \vdash u_2 : S_2 \) then \( \vdash \Gamma_1, [u_2 / x_2] \Gamma_2 \).

Proof: Mutual induction on all the judgments. In the VAR cases we splice in the provided typing derivation. In the WD_DTM_CONV case we appeal to lemma 13.

\[\square\]

Lemma 16 (Substitution of vs).  

1. If \( \Gamma_1, y_2 : T_2, \Gamma_2 \vdash t_1 : T_1 \) and \( \Gamma_1 \vdash v_2 : T_2 \) then \( \Gamma_1, [v_2 / y_2] \Gamma_2 \vdash [v_2 / y_2] t_1 : [v_2 / y_2] T_1 \).

2. If \( \Gamma_1, y_2 : T_2, \Gamma_2 \vdash s_1 : S_1 \) and \( \Gamma_1 \vdash v_2 : T_2 \) then \( \Gamma_1, [v_2 / y_2] \Gamma_2 \vdash [v_2 / y_2] s_1 : [v_2 / y_2] S_1 \).
3. If $\Gamma_1, y_2 : T_2, \Gamma_2 \vdash T : K$ and $\Gamma_1 \vdash v_2 : T_2$ then $\Gamma_1, [v_2/y_2] \Gamma_2 \vdash [v_2/y_2] T : [v_2/y_2] K$.

4. If $\Gamma_1, y_2 : T_2, \Gamma_2 \vdash K$ and $\Gamma_1 \vdash v_2 : T_2$ then $\Gamma_1, [v_2/y_2] \Gamma_2 \vdash [v_2/y_2] K$.

5. If $\not\vdash \Gamma_1, y_2 : T_2, \Gamma_2$ and $\not\vdash v_2 : T_2$ then $\not\vdash \Gamma_1, [v_2/y_2] \Gamma_2$.

Proof. Similar to the previous lemma.

Lemma 17 (Equivalence Cut). Suppose $\Gamma \vdash t_1 \equiv t_2$. Then:

1. If $\Gamma, t_1 \equiv t_2, \Gamma' \vdash t \equiv t'$, then $\Gamma, \Gamma' \vdash t \equiv t'$.

2. If $\Gamma, t_1 \equiv t_2, \Gamma' \vdash T \equiv T'$, then $\Gamma, \Gamma' \vdash T \equiv T'$.

3. If $\Gamma, t_1 \equiv t_2, \Gamma' \vdash K \equiv K'$, then $\Gamma, \Gamma' \vdash K \equiv K'$.

Proof. Mutual induction on the derivations. The only case that doesn’t go directly by the IH is EQ_DTM_ASSUMPTION, where we splice in the provided derivation.

Lemma 18 (Typing Cut). Suppose $\Gamma \vdash t_1 \equiv t_2$. Then:

1. If $\Gamma, t_1 \equiv t_2, \Gamma' \vdash t : T$, then $\Gamma, \Gamma' \vdash t : T$.

2. If $\Gamma, t_1 \equiv t_2, \Gamma' \vdash s : S$, then $\Gamma, \Gamma' \vdash s : S$.

3. If $\Gamma, t_1 \equiv t_2, \Gamma' \vdash T : K$, then $\Gamma, \Gamma' \vdash T : K$.

4. If $\Gamma, t_1 \equiv t_2, \Gamma' \vdash K$, then $\Gamma, \Gamma' \vdash K$.

5. If $\not\vdash \Gamma, t_1 \equiv t_2, \Gamma'$, then $\not\vdash \Gamma, \Gamma'$.

Proof. Mutual induction on the derivations. The only case that doesn’t go directly by IH is WF_SIG_CONV, where we appeal to lemma 17.

Lemma 19 (Substitution through types). If $\Gamma \vdash T_1 : K$ and $\Gamma \vdash t_2 \equiv t'_2$ and $y_2 \not\in \text{dom}(\Gamma)$, then $\Gamma \vdash [t_2/y_2] T_1 \equiv [t'_2/y_2] T_1$.

Proof. Induction on the derivation of $\Gamma, y : T_2 \vdash T_1 : K$. The cases are

Case \texttt{wf\_dty\_arr}: The rule looks like

$$
\Gamma \vdash T_1 : *
\quad
\Gamma, y : T_1 \vdash T_2 : *
\quad
\Gamma \vdash (y : T_1) \rightarrow T_2 : * \quad \text{WF\_DTY\_ARR}
$$

Since $y$ is a bound variable we can pick it to be different from $y_2$ and push the substitution in, so we must show $\Gamma \vdash (y : [t_2/y_2] T_1) \rightarrow [t_2/y_2] T_2 \equiv (y : [t'_2/y_2] T_1) \rightarrow [t'_2/y_2] T_2$. By EQ\_DTY\_PI it suffices to show $\Gamma_1, y : T_2 \vdash [t_2/y_2] T_1 \equiv [t'_2/y_2] T_1$ and $\Gamma_1 \vdash [t_2/y_2] T_2 \equiv [t'_2/y_2] T_2$, both of which follow by IH (noting again that $y_2 \neq y$).

Case \texttt{wf\_dty\_pair}: Similar to the previous case.

Case \texttt{wf\_dty\_data}: We must show $\Gamma \vdash [t_2/y_2] B \equiv [t'_2/y_2] B$, that is to say, $\Gamma \vdash B \equiv B$. This follows by EQ\_DTY\_TREFL.

Case \texttt{wf\_dty\_unit}: Similar to the previous case.
Case \textbf{wf\_dty\_app}: The rule looks like
\[
\frac{\Gamma \vdash T : T_1 \Rightarrow \ast \quad \Gamma \vdash t : T_1}{\Gamma \vdash T . t : \ast} \text{WF\_DTY\_APP}
\]

By distributing the substitution and using \textsc{eq\_dtm\_app}, it suffices to show \(\Gamma \vdash [t_2 / y_2] T \equiv [t_2' / y_2] T\) (which is direct by IH) and \(\Gamma \vdash [t_2 / y_2] t \equiv [t_2' / y_2] t\) (which is by \textsc{eq\_dtm\_subst}).

\begin{proof}
\end{proof}

\begin{lemma}[Context conversion (types)]. Suppose \(\Gamma \vdash T_1 \equiv T_2\) and \(\Gamma \vdash T_2 : \ast\). Then:
\begin{enumerate}
\item If \(\Gamma, y_1; T_1, \Gamma' \vdash t : T\), then \(\Gamma, y_1; T_2, \Gamma' \vdash t : T\).
\item If \(\Gamma, y_1; T_1, \Gamma' \vdash s : S\), then \(\Gamma, y_1; T_2, \Gamma' \vdash s : S\).
\item If \(\Gamma, y_1; T_1, \Gamma' \vdash T : K\), then \(\Gamma, y_1; T_2, \Gamma' \vdash T : K\).
\item If \(\Gamma, y_1; T_1, \Gamma' \vdash K\), then \(\Gamma, y_1; T_2, \Gamma' \vdash K\).
\item If \(\Gamma \vdash \Gamma, \Gamma'\), then \(\Gamma \vdash \Gamma, \Gamma'\).
\end{enumerate}
\end{lemma}

\begin{proof}
Mutual induction on all the judgments. The only case that doesn’t go immediately by IH is \textsc{wf\_dtm\_var}, where we splice in a use of \textsc{wf\_dtm\_conv}.
\end{proof}

\begin{lemma}[Context conversion (equations)]. If \(\Gamma, t_1 \equiv t_2, \Gamma' \vdash J\) and \(\Gamma \vdash t_1 \equiv t'_1\) and \(\Gamma \vdash t_2 \equiv t'_2\), then \(\Gamma, t'_1 \equiv t'_2, \Gamma' \vdash J\).
\end{lemma}

\begin{proof}
The proof can be carried out completely generically for all the judgment forms, using the Weakening and Cut properties.

By weakening (lemmas 10 and 11) on the second two assumptions we have \(\Gamma, t'_1 \equiv t'_2 \vdash t_1 \equiv t'_1\) and \(\Gamma, t'_1 \equiv t'_2 \vdash t_2 \equiv t'_2\). So by \textsc{eq\_dtm\_sym} and \textsc{eq\_dtm\_trans} we know \(\Gamma, t'_1 \equiv t'_2 \vdash t_1 \equiv t_2\).

By weakening on the first assumption, we have \(\Gamma, t'_1 \equiv t'_2, t_1 \equiv t_2, \Gamma' \vdash J\). But then by Cut (lemmas 17 and 18) we have \(\Gamma, t'_1 \equiv t'_2, \Gamma' \vdash J\) as we claimed.
\end{proof}

\subsection{Preservation}

\begin{lemma}[Regularity].
\begin{enumerate}
\item If \(\Gamma \vdash \Gamma\) and \(y : T \in \Gamma\) then \(\Gamma \vdash T : \ast\).
\item If \(\Gamma \vdash s : S\) then \(\vdash \Gamma\).
\item If \(\Gamma \vdash T\) then \(\Gamma \vdash T : \ast\) and \(\vdash \Gamma\).
\end{enumerate}
\end{lemma}

\begin{proof}
Claim (1) is by induction on \(\vdash \Gamma\), using weakening (lemma 11). Claim (2) is an easy induction on \(\Gamma \vdash s : S\) (using inversion on \(\vdash \Gamma\) in the cases that extend the context.) Claim (3) is by induction on \(\Gamma \vdash T : T\). In the \textsc{wf\_dtm\_app}, \textsc{wf\_dtm\_proj2} and \textsc{wf\_dtm\_ctor} we have the needed well-formedness directly as a premise to the rule.
\end{proof}

\begin{lemma}[Type equivalence inversion].
\begin{enumerate}
\item If \(\Gamma \vdash (y : T_1) \rightarrow T_2 \equiv (y : T'_1) \rightarrow T'_2\), then \(\Gamma \vdash T_1 \equiv T'_1\) and \(\Gamma \vdash T_2 \equiv T'_2\).
\item If \(\Gamma \vdash (y : T_1) \ast T_2 \equiv (y : T'_1) \ast T'_2\), then \(\Gamma \vdash T_1 \equiv T'_1\) and \(\Gamma \vdash T_2 \equiv T'_2\).
\item If \(\Gamma \vdash T t \equiv T' t'\), then \(\Gamma \vdash T \equiv T'\) and \(\Gamma \vdash t \equiv t'\).
\end{enumerate}
\end{lemma}

\begin{proof}
\end{proof}
Proof. By inversion on the judgment. The three claims are similar, so we only show (1).

For the claim (1), two rules can match the conclusion, namely \texttt{EQ\_DTY\_PI} and \texttt{EQ\_DTY\_INCON}. If the derivation ended with \texttt{EQ\_DTY\_PI} we have \( \Gamma \vdash T_1 \equiv T_1' \) and \( \Gamma \vdash T_2 \equiv T_2' \) as premises to the rule. If it ended with \texttt{EQ\_DTY\_INCON} we have an inconsistent premise \( \Gamma \vdash C v \equiv C' v' \), so we can derive \( \Gamma \vdash T_1 \equiv T_1' \) and \( \Gamma \vdash T_2 \equiv T_2' \) by applying \texttt{EQ\_DTY\_INCON}.

**Lemma 24** (Type equivalence is an equivalence relation).

1. For any \( T \), we have \( \Gamma \vdash T \equiv T \).
2. If \( \Gamma \vdash T \equiv T' \) then \( \Gamma \vdash T' \equiv T \).
3. If \( \Gamma \vdash T \equiv T' \) and \( \Gamma \vdash T' \equiv T'' \), then \( \Gamma \vdash T \equiv T'' \).

Proof. Claim (1) is by induction on the structure of \( T \). For each syntactic form (arrow, type application, pair, Unit, and \( B \)) there is a corresponding equivalence rule (\texttt{EQ\_DTY\_PI}, \texttt{EQ\_DTY\_APP}, \texttt{EQ\_DTY\_SIGMA}, \texttt{EQ\_DTY\_UREFL}, \texttt{EQ\_DTY\_TREFL}). In the type application case we use \texttt{EQ\_DTM\_REFL}.

Claim (2) is an easy induction on \( \Gamma \vdash T \equiv T' \).

Claim (3) is by a double induction on \( \Gamma \vdash T \equiv T' \) and \( \Gamma \vdash T' \equiv T'' \). The cases for \( \Gamma \vdash T \equiv T' \) and \( \Gamma \vdash T' \equiv T'' \) are:

\texttt{eq\_dtym\_incon} and anything, anything and \texttt{eq\_dtym\_incon}: Here we can directly show \( \Gamma \vdash T \equiv T'' \) using the inconsistent equality premise.

Both derivations are \texttt{eq\_dtym\_urefl}: Then \( T = T' = T'' = \text{Unit} \).

Both derivations are \texttt{eq\_dtym\_trefl}: Similar.

Both derivations are \texttt{eq\_dtym\_pi}: We apply the IH to the sub-derivations.

Both derivations are \texttt{eq\_dtym\_sigma}: Similar.

Both derivations are \texttt{eq\_dtym\_app}: As premises to the two rules we have

1. \( \Gamma \vdash T \equiv T' \)
2. \( \Gamma \vdash t \equiv t' \)
3. \( \Gamma \vdash T' \equiv T'' \)
4. \( \Gamma \vdash t' \equiv t'' \).

From the IH applied to (1) and (3) we get \( \Gamma \vdash T \equiv T'' \). From \texttt{EQ\_DTM\_TRANS} applied to (2) and (4) we get \( \Gamma \vdash t \equiv t' \). Then apply \texttt{EQ\_DTM\_APP} again.

**Other combinations**: Cannot happen, since the top-level structure of the “middle” term would not match up.

**□**

**Lemma 25** (Kinding inversion).

1. If \( \Gamma \vdash B t : * \) and \( B : T_0 \Rightarrow * \in \Psi_0 \), then \( \Gamma \vdash t : T_0 \).

Proof. Directly by inversion on the judgment we see that the derivation must have been by \texttt{WF\_DTY\_APP} and \texttt{WF\_DTY\_DATA}. So we must have \( B : T \Rightarrow * \in \Psi_0 \) and \( \Gamma \vdash t : T \). Since there are no duplicate declarations in \( \Psi_0 \), \( T \) must be \( T_0 \).

**□**

**Lemma 26** (Typing inversion).

1. If \( \Gamma \vdash (\lambda y : T_1. t) : T' \), then \( \Gamma, y : T_1 \vdash t : T_2 \), and \( \Gamma \vdash (y : T_1) \rightarrow T_2 \equiv T' \).

43
2. If $\Gamma \vdash <t_1, t_2>: T'$, then $\Gamma \vdash t_1 : T_1$ and $\Gamma \vdash t_2 : [t_1/y]T'_2$ and $\Gamma \vdash (y:T_1)*T_2 \equiv T'$.

3. If $\Gamma \vdash C t : T'$, then $C:(y:T_1) \rightarrow B t_1 \in \Psi_0$ and and $\Gamma \vdash t : T_1$ and $\Gamma \vdash B[t/y]t_1 \equiv T'$.

Proof. Induction on the typing $\Gamma \vdash t : T'$. The cases are:

Cases $\text{wf_dtm_var, app, proj1, proj2, case, ds, guard, error}$: In these rules the shape of the term does not match the ones mentioned in the lemma.

Case $\text{wf_dtm_abs}$: The typing rule looks like

$$\frac{\Gamma, y:T_1 \vdash t : T_2}{\Gamma \vdash \lambda y:T_1.t : (y:T_1) \rightarrow T_2} \text{WF_DTM_ABS}$$

So we get $\Gamma, y:T_1 \vdash t : T_2$ as an assumption to the rule. By reflexivity (lemma 24) we have $\Gamma \vdash (y:T_1) \rightarrow T_2 \equiv (y:T_1) \rightarrow T_2$ as required.

Case $\text{wf_dtm_pair, wf_dtm_unit}$: Similar to the abs case.

Case $\text{wf_dtm_ctor}$: The typing rule looks like

$$\frac{C(y:T_1) \rightarrow B t' \in \Psi_0}{\frac{B:T_2 \Rightarrow * \in \Psi_0}{\frac{\Gamma \vdash t : T_1}{\Gamma \vdash B[t/y]t' : *}}} \text{WF_DTMCTOR}$$

We have $C:(y:T_1) \rightarrow B \in \Psi_0$ as a premise, and $\Gamma \vdash [t/y]t' \equiv [t/y]t$ by $\text{EQ_DTM_REFL}$.

Case $\text{wf_dtm_conv}$: The typing rule looks like

$$\frac{\Gamma \vdash t : T}{\frac{\Gamma \vdash T \equiv T' \quad \Gamma \vdash T' : *}{\Gamma \vdash t : T'}} \text{WF_DTM_CONV}$$

For (1) we get $\Gamma, y:T_1 \vdash t : T_2$ and $\Gamma \vdash (y:T_1) \rightarrow T_2 \equiv T$ by the IH, so by transitivity (lemma 24) we have $\Gamma \vdash (y:T_1) \rightarrow T_2 \equiv T'$ as required. (2) and (3) are similar.

$\square$

Lemma 27 ($\Leftrightarrow$ ignores terms in types). $S \Leftrightarrow T$ iff $S \Leftrightarrow [t/y]T$.

Proof. We show the left-to-right direction only, as the reverse direction is similar. We proceed by induction on $S \Leftrightarrow T$. The cases are:

Case $\text{compat_arr}$: The case looks like

$$\frac{S_1 \Leftrightarrow T_1 \quad S_2 \Leftrightarrow T_1}{S_1 \rightarrow S_2 \Leftrightarrow (y':T_1) \rightarrow T_2} \text{COMPAT_ARR}$$

Since $y'$ is a bound variable we can pick it fresh, so that $[t/y]((y':T_1) \rightarrow T_2) = (y:[t/y]T_1) \rightarrow [t/y]T_2$. Then we get $S_1 \Leftrightarrow [t/y]T_1$ and $S_2 \Leftrightarrow [t/y]T_2$ by IH. So re-applying the rule we get $S_1 \rightarrow S_2 \Leftrightarrow (y':[t/y]T_1) \rightarrow [t/y]T_2$ as required.

Case $\text{compat_pair, compat_unit}$: Similar to $\text{COMPAT_ARR}$.  

44
Case **compat_data**: The case looks like

\[
B : T_0 \Rightarrow * \in \Psi_0 \\
\text{FO (}T_0\text{)} \\
\text{corr (}A,B\text{)} \\
A \leftrightarrow B \Gamma \text{COMPAT_DATA}
\]

The substitution doesn’t affect the premises of the rule. 

**Lemma 28** (Convenient derivable typing rules). The following rules are derivable:

\[
\begin{align*}
\Gamma & \vdash \sigma \in \Psi_0 \\
\text{prop} \ 	ext{(Generalized Preservation)} \\
\text{comp} \ 	ext{(Convenient derivable typing rules)} \\
\end{align*}
\]

**Proof.** **WF DTM APPVAL:** By regularity (lemma 22) we have \(\Gamma \vdash (y:T_1) \rightarrow T_2\). By inversion on the kinding relation, that means that \(\Gamma, y:T_1 \vdash T_2 : *\). So by substitution (lemma 16) we get \(\Gamma \vdash [v_2/y]T_2 : *\). Then we conclude by **WF DTM APP**.

**WF DTM LET:** Expanding the syntactic sugar, what we need to show is

\[
\Gamma \vdash (\lambda y : T_1. t_2) T_1 : T_2
\]

By **WD DTM ABS** we know \(\Gamma \vdash (\lambda y : T_1. t_2) : (y : T_1) \rightarrow T_2\). From the premise \(\Gamma \vdash T_2 : *\) and lemma 9 we know that \(y \notin \text{fv}(T_2)\), so \([t_2/y]T_2 = T_2\). So the same kinding premise also tells us \(\Gamma \vdash [t_2/y]T_2 : *\). Then the application is well-formed, so \(\Gamma \vdash (\lambda y : T_1. t_2) t_1 : [t_1/y]T_2\), which is syntactically equal to the type we want. 

**Lemma 29.** If \(B : T_0 \Rightarrow * \in \Psi_0\) and constrs \(B = \mathcal{C}^{i}_T\) and \(C : (y:T_1) \rightarrow B \) \(t_j \in \Psi_0\), then \(\cdot, y_j : T_j \vdash t_j : T_0\).

**Proof.** By inversion on the judgment \(\vdash \Psi_0\) we get \(\cdot \vdash (y_j : T_j) \rightarrow B \) \(t_j : *\). Then use inversion on the kinding judgment. 

**Property 6.** If \(C : S \rightarrow A \in \Psi_0\) and \(C : (y : T_1) \rightarrow B t_1 \in \Psi_0\) \(\Gamma \vdash u : S\), then \(\Gamma \vdash \text{argToD}_C u : T_1\) (if it is defined).

**Property 7.** If \(C : S \rightarrow A \in \Psi_0\) and \(C : (y : T_1) \rightarrow B t_1 \in \Psi_0\) \(\Gamma \vdash v : T_1\), then \(\Gamma \vdash \text{argToS}_C v : S\) (if it is defined).

**Theorem 3** (Generalized Preservation). Let \(y_0\) be fresh for \(\Gamma, T, S, K\). Then

1. If \(\Gamma \vdash s : S\) and \(s \rightarrow s’\) then \(\Gamma \vdash s : S\).
2. If \(\Gamma \vdash [t_0/y_0] t : T\) and \(t_0 \rightarrow t_0’\) then \(\Gamma \vdash [t_0'/y_0] t : T\).
3. If \(\Gamma \vdash [t_0/y_0] s : S\) and \(t_0 \rightarrow t_0’\) then \(\Gamma \vdash [t_0'/y_0] s : S\).
4. If \(\Gamma \vdash [t_0/y_0] T : K\) and \(t_0 \rightarrow t_0’\), then \(\Gamma \vdash [t_0'/y_0] T : K\).

**Proof.** We proceed by mutual induction on the judgments \(\Gamma \vdash s : S\), \(\Gamma \vdash [t_0/y_0] s : S\), \(\Gamma \vdash [t_0/y_0] t : T\), and \(\Gamma \vdash [t_0/y_0] T : K\).

The cases for \(\Gamma \vdash s : S\) are mostly routine, but we show the two cases which involve novel language features, namely SD-boundaries and letd-expressions.
Case **sd_stm_sd**: The rule looks like

\[
\begin{align*}
  & \Gamma \vdash t : T \\
  & S \iff T \\
  & \Gamma \vdash SD_T^S t : S
\end{align*}
\]

The expression reduces either by the context \(SD_T^S \Box\) or by one of the DS stepping rules.

- Suppose it was by congruence so \(t \rightarrow t'\). Then by IH \(\Gamma \vdash t' : T\) and thus \(\Gamma \vdash SD_T^S t' : S\).
- Suppose it was by \(\text{eval}_{\text{STM}_{\text{SD}}}\). So the step looks like

\[
SD_{((y:T_1) \rightarrow T_2)}^{(S_1 \rightarrow S_2)} \lambda y:T_1. t \rightarrow \lambda x:S_1 . \text{letd} y' = DS_{S_1}^{T_1} x \in SD_{(v'/y:T_2)}^{S_2}((\lambda y:T_1^t) y') \quad \text{\text{eval}_{\text{STM}_{\text{SD}}}}
\]

The variable \(y'\) is bound, so we rename it to \(y\) to reduce clutter. We must show \(\Gamma \vdash \lambda x:S_1 . \text{letd} y = DS_{S_1}^{T_1} x \in SD_{(v'/y:T_2)}^{S_2}((\lambda y:T_1^t) y) : S_1 \rightarrow S_2\), while we have the fact \(\Gamma \vdash (\lambda y:T_1^t) : (y:T_1) \rightarrow T_2\) available as a premise to the typing rule. By inversion on the judgment \(S_1 \rightarrow S_2 \iff (y:T_1) \rightarrow T_2\) we get \(S_1 \iff T_1\) and \(S_2 \iff T_2\).

By Weakening (lemma 11) and \(\text{WF}_{\text{DTM}_{\text{APPVAL}}}\) (lemma 28) we get \(\Gamma, x:S_1, y:T_1 \vdash (\lambda y:T_1^t) y : T_2\). So by \(\text{WF}_{\text{STM}_{\text{SD}}}\) we have

\[
\Gamma, x:S_1, y:T_1 \vdash SD_{S_1}^{T_1} x \in SD_{(v'/y:T_2)}^{S_2}((\lambda y:T_1^t) y) : S_2.
\]

Also, by \(\text{WF}_{\text{DTM}_{\text{DS}}}\) we immediately get immediately get \(\Gamma, x:S_1 \vdash SD_{S_1}^{T_1} x : T_1\). So by \(\text{WF}_{\text{STM}_{\text{LETD}}}\) (lemma 28) we have

\[
\Gamma, x:S_1 \vdash \text{letd} y = DS_{S_1}^{T_1} x \in SD_{(v'/y:T_2)}^{S_2}((\lambda y:T_1^t) y) : S_2.
\]

We conclude by applying \(\text{WF}_{\text{STM}_{\text{AB}}}\).

- Suppose it was by \(\text{eval}_{\text{STM}_{\text{SD}}\text{PAIR}}\). So the step looks like

\[
SD_{((y:T_1) \ast T_2)}^{(S_1 \ast S_2)} <v_1, v_2> \rightarrow SD_{T_1}^{S_1} v_1, SD_{(v_2/y:T_2)}^{S_2} <v_1, v_2> \quad \text{\text{eval}_{\text{STM}_{\text{SD}}\text{PAIR}}}
\]

We must show \(\Gamma \vdash SD_{T_1}^{S_1} v_1, SD_{(v_2/y:T_2)}^{S_2} <v_1, v_2> : S_1 \ast S_2\), while we have the fact \(\Gamma \vdash <v_1, v_2> : (y:T_1) \ast T_2\) available as a premise to the rule. By inversion on the judgment \(S_1 \ast S_2 \iff (y:T_1) \ast T_2\) we get \(S_1 \iff T_1\) and \(S_2 \iff T_2\). By inversion (lemma 26) on \(\Gamma \vdash <v_1, v_2> : (y:T_1) \ast T_2\) we find \(\Gamma \vdash v_1 : T_1\) and \(\Gamma \vdash v_2 : [v_1/y] T_2\).

We wish to apply \(\text{WF}_{\text{STM}_{\text{PAIR}}}\). We directly get the first premise, namely \(\Gamma \vdash SD_{T_1}^{S_1} v_1 : S_1\), by \(\text{WF}_{\text{STM}_{\text{SD}}}\). For the second premise we must show \(\Gamma \vdash SD_{(v_2/y:T_2)}^{S_2} v_2 : S_2\). By lemma 27 we have \(S_2 \iff [v_1/y] T_2\), so this also follows from \(\text{WF}_{\text{STM}_{\text{SD}}}\).
- Suppose it was by \(\text{eval}_{\text{STM}_{\text{SD}}\text{CONST}}\). So the step looks like

\[
\begin{align*}
  & C:S \rightarrow A \in \Psi_0 \\
  & C:(y:T_1) \rightarrow B t_1 \in \Psi_0 \\
  & \text{argToS}_{C} C v = u \quad \text{eval}_{\text{STM}_{\text{SD}}\text{CONST}}
\end{align*}
\]

We must show \(\Gamma \vdash C u : A\), while we have the fact \(\Gamma \vdash C v : B t\) available as a premise to the rule. By inversion (lemma 26) we get \(\Gamma \vdash v : T_1\). So by property 7 we get that \(\Gamma \vdash u : S\), and hence \(\Gamma \vdash C u : A\) as required.
• Suppose it was by EVAL\_STM\_SD\_UNIT. So the step looks like
\[
\begin{align*}
\text{SD}^{\text{Unit}}_{\text{unit}} & \rightarrow \text{EVAL\_STM\_SD\_UNIT} \\
\end{align*}
\]
We must show \(\Gamma \vdash \text{unit} : \text{Unit}\), which is straightforwardly true.

**Case wf\_stm\_letd:** The rule looks like
\[
\begin{align*}
\Gamma & \vdash t : T \\
\Gamma, y : T & \vdash s : S \\
\Gamma & \vdash \text{letd} y = t \text{in} \ s : S \quad \text{WF\_STM\_LETD}
\end{align*}
\]
We consider the ways the expression \text{letd} \( y = t \text{in} \ s \) may step.

• By EVAL\_STM\_CTX. So \(E_s\) is \text{letd} \( y = \emptyset \text{in} \ s\), we have \( t \rightarrow t'\), and the transition looks like \text{letd} \( y = t \text{in} \ s \rightarrow \text{letd} y = t' \text{in} \ s\). By mutual IH we know \(\Gamma \vdash t' : T\), so we conclude by re-applying WF\_STM\_LETD.

• By EVAL\_STM\_LETD. So the transition is \text{letd} \( y = v \text{in} \ s \rightarrow [v/y] s\). By substitution (part (2) of lemma 16) we get \(\Gamma \vdash [v/y] s : S\) as required.

The cases for \(\Gamma \vdash [t_0/y_0] s : S\) are all immediate by IH except two, namely

**Case wf\_stm\_sd.** The situation looks like this:
\[
\begin{align*}
\Gamma & \vdash [t_0/y_0] \ y \ : [t_0/y_0] T \\
S & \leftrightarrow [t_0/y_0] T \\
\Gamma & \vdash \text{SD}^{[t_0/y_0]}_{T} [t_0/y_0] t : S \\
\end{align*}
\]
(Notice that simple types never contain any term variables, so applying a substitution to \(S\) does not do anything). By the mutual IH we get \(\Gamma \vdash [t_0'/y_0] t : [t_0/y_0] T\). By applying lemma 27 twice we get \(S \leftrightarrow [t_0'/y_0] T\). So we can re-apply the rule to get \(\Gamma \vdash \text{SD}^{[t_0'/y_0]}_{T} [t_0'/y_0] t : S\) as required.

**Case wf\_stm\_letd.** We can pick the variable bound by the letd-expression to be different from \(y_0\). Then after pushing the substitution in the situation looks like this:
\[
\begin{align*}
\Gamma & \vdash [t_0/y_0] t : T \\
\Gamma, y : T & \vdash [t_0/y_0] s : S \\
\Gamma & \vdash \text{letd} y = [t_0'/y_0] t \text{in} \ [t_0/y_0] s : S \quad \text{WF\_STM\_LETD}
\end{align*}
\]
Now by the mutual IH we get \(\Gamma \vdash [t_0'/y_0] t : T\), while by IH we get \(\Gamma, y : T \vdash [t_0'/y] s : S\). So we re-apply the rule to get \(\Gamma \vdash \text{letd} y = [t_0'/y_0] t \text{in} \ [t_0'/y_0] s : S\) as required.

The cases for \(\Gamma \vdash [t_0/y_0] t : T\) are:

**Case wf\_dtm\_var.** Since variables do not step we must have \([t_0/y_0] t = [t_0'/y_0] t\) and the result is trivial.

**Case wf\_dtm\_abs.** So \([t_0/y_0] t\) is a \(\lambda\)-abstraction. Considering the possibilities for \(t\), this means that either \(t = y_0\) or \(t\) is a \(\lambda\)-abstraction. However, the former is impossible because abstractions don’t step. We can pick the bound variable in \(t\) to be distinct from \(y_0\) and push the substitution in. Then the situation looks like this:
\[
\begin{align*}
\Gamma, y : [t_0/y_0] T_1 & \vdash [t_0/y_0] t : T_2 \\
\Gamma & \vdash \lambda y : [t_0/y_0] T_1 : [t_0'/y_0] t : \ (y : [t_0/y_0] T_1) \rightarrow T_2 \\
\end{align*}
\]
So we need to prove \(\Gamma \vdash \lambda y : [t_0'/y_0] T_1 : [t_0'/y_0] t : (y : [t_0'/y_0] T_1) \rightarrow T_2\).

By EQ\_DTM\_STEP we know \(\Gamma \vdash t_0 \equiv t_0'\), so by lemma 19 we have \(\Gamma \vdash [t_0/y_0] T_1 \equiv [t_0'/y_0] T_1\). By the IH we know \(\Gamma, y : [t_0/y_0] T_1 \vdash [t_0'/y_0] t : T_2\), so by context conversion (lemma 20) we have \(\Gamma, y : [t_0'/y_0] T_1 \vdash [t_0'/y_0] t : T_2\). Now we re-apply WF\_DTM\_ABS to get \(\Gamma \vdash \lambda y : [t_0'/y_0] T_1 : [t_0'/y_0] t : (y : [t_0'/y_0] T_1) \rightarrow T_2\).

Finally by WF\_DTM\_CONV this gives \(\Gamma \vdash \lambda y : [t_0'/y_0] T_1 : [t_0'/y_0] t : (y : [t_0'/y_0] T_1) \rightarrow T_2\) as required.
Case \texttt{wf\_dtm\_app}. So \([t_0/y_0]t\) is an application, and \(T\) is an arrow type. This can happen in two ways: either \(t\) is \(y_0\), or \(t\) is an application.

If \(t\) is an application, we can choose the bound variable in the arrow type to be different from \(y_0\) and push the substitution in. Then the situation looks like this:

\[
\begin{align*}
\Gamma &\vdash [t_0/y_0]t_1 : (y : T_1) \rightarrow T_2 \\
\Gamma &\vdash [t_0/y_0]t_2 : T_1 \\
\Gamma &\vdash [[t_0/y_0]t_2/y]T_2 : \ast \\
\Gamma &\vdash [t_0/y_0]t_1 : [t_0/y_0]t_2/y]T_2 : \ast \\
\end{align*}
\]

By the IH we get \(\Gamma \vdash [t_0/y_0]t_1 : (y : T_1) \rightarrow T_2\) and \(\Gamma \vdash [t_0/y_0]t_2 : T_1\). Since \(y_0 \notin \text{fv}\ (T_2)\), we have that \([[t_0/y_0]t_2/y]T_2 = [t_0/y_0][t_2/y]T_2\) and \([[t_0/y_0]t_2/y]T_2 = [t_0/y_0][t_2/y]T_2\). So by the mutual IH we get \(\Gamma \vdash [[t_0/y_0]t_2/y]T_2 : \ast\). So re-applying \texttt{WD\_DTM\_APP} we get

\[
\Gamma \vdash [t_0/y_0]t_1 [t_0/y_0]t_2 : [[t_0/y_0]t_2/y]T_2.
\]

Now by \texttt{EQ\_DTM\_STEP} we have \(\Gamma \vdash t_0 \equiv t'_0\), so (again noting that \([[t_0/y_0]t_2/y]T_2 = [t_0/y_0][t_2/y]T_2\)) by lemma 19 we have \(\Gamma \vdash [[t_0/y_0]t_2/y]T_2 \equiv [[t_0/y_0]t_2/y]T_2\). So by \texttt{WD\_DTM\_CONV} we get

\[
\Gamma \vdash [t_0/y_0]t_1 [t_0/y_0]t_2 : [[t_0/y_0]t_2/y]T_2
\]

as required.

On the other hand, suppose that the \(t\) is \(y_0\), that is \(t_0\) is an application which steps and we need to show that its type is preserved. The situation looks like

\[
\begin{align*}
\Gamma &\vdash t_1 : (y : T_1) \rightarrow T_2 \\
\Gamma &\vdash t_2 : T_1 \\
\Gamma &\vdash [t_2/y]T_2 : \ast \\
\Gamma &\vdash t_1 t_2 : [t_2/y]T_2 : \ast
\end{align*}
\]

We consider the ways \(t_1, t_2\) can step.

- By \texttt{EVAL\_DTM\_CTX} when \(E_t\) is \(\square t_2\). So \(t_1 \rightarrow t'_1\). By the IH, \(\Gamma \vdash t'_1 : (y : T_1) \rightarrow T_2\) so \(\Gamma \vdash t'_1 t_2 : T_2\).
- By \texttt{EVAL\_DTM\_CTX} when \(E_t\) is \(v \square\). So \(t_2 \rightarrow t'_2\). By the IH \(\Gamma \vdash t'_2 : T_1\), so by \texttt{WD\_DTM\_APP} we have that \(\Gamma \vdash v t'_2 : [t'_2/y]T_2\). So by lemma 19 and one use of \texttt{WD\_DTM\_CONV} we have that \(\Gamma \vdash v t'_2 : [t_2/y]T_2\) (taking advantage of the fact that \(\Gamma \vdash t_2 \equiv t'_2\) by \texttt{EQ\_DTM\_STEP}).
- By \texttt{EVAL\_DTM\_BETA}. So \(t_1 = \lambda y : T'_1.t\) and \(t_2\) is some value \(v\), and the step is \((\lambda y : T'_1.t) v \rightarrow [v/y]t\). By inversion (lemma 26) we know \(\Gamma, y : T'_1 \vdash t : T'_2\) for some \(T'_2\) such that \(\Gamma \vdash (y : T'_1) \rightarrow T'_2 \equiv (y : T_1) \rightarrow T_2\).

By inversion on the type equality (lemma 23) we know \(\Gamma \vdash T'_1 \equiv T_1\) and \(\Gamma \vdash T'_2 \equiv T_2\). So by one application of \texttt{WD\_DTM\_CONV} we have \(\Gamma \vdash v : T'_1\); by substitution (lemma 16) \(\Gamma \vdash [v/y]t : T'_2\); and by a second application of \texttt{WD\_DTM\_CONV} we get \(\Gamma \vdash [v/y]t : T_2\).

Case \texttt{wf\_dtm\_pair} So \([t_0/y_0]t\) is a pair. Considering the possibilities for \(t\) this means that either \(t\) is \(y_0\) or \(t\) is a pair. However, the former is impossible because pairs don’t step. So pushing in the substitution, the situation looks like this:

\[
\begin{align*}
\Gamma &\vdash [t_0/y_0]t_1 : T_1 \\
\Gamma &\vdash [t_0/y_0]t_2 : [[t_0/y_0]t_1/y]T_2 \\
\Gamma &\vdash (y : T_1) \ast T_2 : \ast \\
\Gamma &\vdash <[t_0/y_0]t_1, [t_0/y_0]t_2> : (y : T_1) \ast T_2 \text{ WF\_DTM\_PAIR}
\end{align*}
\]

Now by IH we have \(\Gamma \vdash [t_0/y_0]t_1 : T_1\) and \(\Gamma \vdash [t_0/y_0]t_2 : [[t_0/y_0]t_1/y]T_2\). Since \(y_0 \notin \text{fv}\ (T_2)\) we know \([[t_0/y_0]t_1/y]T_2 = [t_0/y_0][t_1/y]T_2\), so by \texttt{EQ\_DTM\_STEP} and lemma 19 we have \(\Gamma \vdash [t_0/y_0]t_1/y]T_2 \equiv [[t_0/y_0]t_1/y]T_2\). So by \texttt{WD\_DTM\_CONV} (and regularity, lemma 22, to satisfy the kinding premise to conv) we get \(\Gamma \vdash [t_0/y_0]t_2 : [[t_0/y_0]t_1/y]T_2\). Then we can re-apply \texttt{WD\_DTM\_PAIR}.

48
Case \texttt{wf\_dtm\_proj1} So \([t_0/y_0] t\) is a projection. This means that either \(t\) is a projection, or \(t\) is \(y_0\).

In the first case, the situation looks like

\[
\frac{\Gamma \vdash [t_0/y_0] t : (y : T_1) \ast T_2}{\Gamma \vdash [t_0/y_0] t : 1 : T_1} \text{ \texttt{WF\_DTM\_PROJ1}}
\]

By the IH we get that \(\Gamma \vdash [t_0'/y_0] t : (y : T_1) \ast T_2\), and we can just re-apply \texttt{WF\_DTM\_PROJ1}.

In the other case, \(t_0\) itself is a projection that steps and we need to show preservation for it. We consider the ways it may step:

- By the evaluation context \(\Box\cdot 1\). This is immediate by IH, like the previous case.
- By \texttt{EVAL\_DTM\_PROJ1}. So the step is \(<v_1, v_2>\mapsto v_1\). By inversion (lemma 26) and inversion on the equivalence judgment (lemma 23) we have \(\Gamma \vdash v_1 : T_1'\) and \(\Gamma \vdash T_1' \equiv T_1\). So by regularity and \texttt{WF\_DTM\_CONV} we get \(\Gamma \vdash v_1 : T_1\).

Case \texttt{wf\_dtm\_proj2} Similar to the previous case.

Case \texttt{wf\_dtm\_ctor} The typing rule looks like

\[
\frac{C(y : T_1) \rightarrow B \ t' \in \Psi_0}{\frac{\Gamma \vdash t : T_1}{\Gamma \vdash B \ [t/y] t' : *}} \text{ \texttt{WF\_DTM\_CTOR}}
\]

The reasoning is similar to the \texttt{WF\_DTM\_APP} case, but there are fewer cases to consider since there is no \(\beta\)-rule for constructor applications.

Case \texttt{wf\_dtm\_case} So \([t_0/y_0] t\) is a case-expression, which means that either \(t\) is a case-expression or \(t\) is \(y_0\).

In the former case, we pick \(y_i\) to be different from \(y_0\) and push the substitution in, so the situation looks like

\[
\frac{\Gamma \vdash [t_0/y_0] t : B \ t'}{\frac{\Gamma \vdash T : *}{\frac{\text{constrs } B = C_i}{\frac{C_i(y_i : T_1) \rightarrow B \ t'_i \in \Psi_0}{\frac{\Gamma, y_i : T_1, t' \equiv t'_i, [t_0/y_0] t \equiv C_i y_i \vdash [t_0/y_0] t_i : T}{\Gamma \vdash \text{case } [t_0/y_0] t \text{ of } C_i y_i \rightarrow [t_0/y_0] t_i : T} \text{ \texttt{WF\_DTM\_CASE}}}}}}
\]

By the IH we get \(\Gamma \vdash [t_0'/y_0] t : B \ t'\) and \(\Gamma, y_i : T_1, t' \equiv t'_i, [t_0/y_0] t \equiv C_i y_i \vdash [t_0'/y_0] t_i : T\). By \texttt{EQ\_DTM\_STEP} and \texttt{EQ\_DTM\_SUBST} we get \(\Gamma, y_i : T_1, t' \equiv t'_i, [t_0/y_0] t \equiv [t_0'/y_0] t\). So by context conversion (lemma 21) we get \(\Gamma, y_i : T_1, t' \equiv t'_i, [t_0/y_0] t \equiv C_i y_i \vdash [t_0'/y_0] t_i : T\). We conclude by re-applying \texttt{WF\_DTM\_CASE}.

In the other case, \(t_0\) itself is a case-expression which steps, and we must show that its type is preserved. The typing rule looks like

\[
\frac{\Gamma \vdash t : B \ t'}{\frac{\text{constrs } B = C_i}{\frac{C_i(y_i : T_1) \rightarrow B \ t'_i \in \Psi_0}{\frac{\Gamma, y_i : T_1, t' \equiv t'_i, t \equiv C_i y_i \vdash t_i : T}{\frac{\text{case } t \text{ of } C_i y_i \rightarrow t_i : T}} \text{ \texttt{WF\_DTM\_CASE}}}}}}
\]
We consider the ways the expression case of $C_i y_i \rightarrow t_i^{Γ}$ may step:

- By eval_dtm_ctx and the evaluation context case $Γ$ of $C_i y_i \rightarrow t_i^{Γ}$.

  Then $t \rightarrow t''$ so IH gives us $Γ \vdash t'' : T_i$. Additionally, by eq_dtm_step we have $Γ, y_i : T_i \vdash t \equiv t''$, so by context conversion (lemma 21) applied to the premise $Γ, y_i : T_i, t' \equiv t'' \equiv C_i y_i \vdash t_i : T$ we get $Γ, y_i : T_i, t' \equiv t_i, t'' \equiv C_i y_i \vdash t_i : T$. So by wf_dtm_case the final result is well-typed.

- By eval_dtm_case.

  Then $t = C_i v$ for some branch $C_i$ of the case expression, and the expression steps to $[v/y_i]t_i$. By inversion (lemma 26) we know $Γ \vdash v : T_i$ with $C_i(y_i : T_i) \rightarrow B[t'] \in Ψ_0$ and $Γ \vdash B'[v/y_i]t_i \equiv B'$. Since the signature cannot contain duplicate declarations, we know that $B' = B$ and that this $T_i$ is the same that was used to typecheck the $i$th branch of the case expression. Then we have (remember that $t$ is $C_i v$)

  $$Γ, y_i : T_i, t' \equiv t_i, C_i v \equiv C_i y_i \vdash t_i : T$$

  so by substitution we get

  $$Γ, [v/y_i]t' \equiv [v/y_i]t_i, C_i [v/y_i]v \equiv C_i v \vdash [v/y_i]t_i : [v/y_i]T$$

  Since $y_i$ is a bound variable in the case branch and in the constructor declaration, we can pick it suitably fresh. Then $y_i$ can not occur in $t'$ or in $v$ or in $T$, so we can simplify this to

  $$Γ, t' \equiv [v/y_i]t_i, C_i v \equiv C_i v \vdash [v/y_i]t_i : T.$$

  Now the two equalities in the context are provable: we get $Γ \vdash t' \equiv [v/y_i]t_i$ by inversion (lemma 23) on the derivation $Γ \vdash B'[v/y_i]t_i \equiv B' t'$, while $Γ \vdash C_i v \equiv C_i v$ follows by eq_dtm_refl. So by cut (lemma 18) we have

  $$Γ \vdash [v/y_i]t_i : T$$

  as required.

**Case** wt_dtm_ds So $[t_0/y_0]t$ is a DS-boundary. Either $t$ is a DS-boundary, or $t$ is $y_0$. In the former case, the situation looks like this:

  $$Γ \vdash [t_0/y_0]s : S$$
  $$Γ \vdash [t_0/y_0] T : *$$
  $$S \equiv [t_0/y_0]T \quad \text{WF_DTM_DS}$$

  By the IH we get $Γ \vdash [t_0/y_0]s : [t_0/y_0]S$, by the mutual IH we get $Γ \vdash [t_0/y_0] T : *$, and by applying lemma 27 twice we get $S \equiv [t_0/y_0] T$. So re-applying WF_DTM_DS we have $Γ \vdash DS_{[t_0/y_0]T}^ {[t_0/y_0]S}[t_0/y_0]s : [t_0/y_0] T$. Then by lemma 19 and wf_dtm_conv we get $Γ \vdash DS_{[t_0/y_0]T}^ {[t_0/y_0]S}[t_0/y_0]s : [t_0/y_0] T$ as required.

  In the other case, $t_0$ itself is a DS-boundary which steps, and we must show that its type is preserved. We consider the ways the expression $DS_{S_i}^ T s$ can step:

  - By congruence, so $s \rightarrow s'$. Then by IH $Γ \vdash s' : S$ and thus $Γ \vdash DS_{S_i}^ T s' : T$.
  - By eval_dtm_ds_abs. So the step looks like

    $$DS_{(S_1 \rightarrow S_2)}^ {(\lambda x : S_1') \rightarrow T_2} (λx : S_1', s : λy : T_1, DS_{S_2}^ T (λx : S_1', s) (SD_{S_1}^ T y)) \quad \text{EVAL_DTM_DS_ABS}$$

    Then we must show that $Γ \vdash λy : T_1, DS_{S_2}^ T (λx : S_1', s) (SD_{S_1}^ T y) : (y : T_1) \rightarrow T_2$, while we have the fact $Γ \vdash (λx : S_1', s) : S_1 \rightarrow S_2$ available as a premise to the typing rule.

    Constructing such a typing derivation is straightforward utilizing the fact that since $S_1 \rightarrow S_2 \iff (y : T_1) \rightarrow T_2$ then $S_1 \iff T_1$ and $S_2 \iff T_2$ (under a context $Γ, y : T_1$) by inversion of compat_arr. Eventually we must show that $Γ, y : T_1 \vdash λx : S_1, s : S_1 \rightarrow S_2$. We are given that $Γ \vdash λx : S_1, s : S_1 \rightarrow S_2$ so by weakening (lemma 11) we arrive at the desired result.

50
• Suppose it was by EVAL_DTM_DS_PAIR. So the step looks like

\[ \text{EVAL_DTM_DS_PAIR} \]

\[ \text{DS}(S_1 \times S_2) \xrightarrow{\langle u_1, u_2 \rangle} \langle y' = \text{DS}_S^T u_1 \text{ in } \langle y' \cdot \text{DS}_S^y T_2 u_2 \rangle \xi \]

We have \( \Gamma \vdash \langle u_1, u_2 \rangle : S_1 \times S_2 \) as a premise to the typing rule, directly by inversion on that typing we get \( \Gamma \vdash u_1 : S_1 \) and \( \Gamma \vdash u_2 : S_2 \). By inversion on TRANS_PAIR we get that \( S_1 \leftrightarrow T_1 \) and \( S_2 \leftrightarrow T_2 \).

We must construct a typing derivation \( \Gamma \vdash y = \text{DS}_S^T u_1 \text{ in } \langle y', \text{DS}_S^y T_2 u_2 \rangle \) \( \xi \) (Here we rename the \( y' \) to \( y \) in order to simplify the expression). We will do this by applying the derived rule WF_DTM_PAIR (lemma 28), which requires showing the two premises \( \Gamma \vdash \text{DS}_S^T u_1 : T_1 \) and \( \Gamma, y: T_1 \vdash \langle y, \text{DS}_S^y T_2 u_2 \rangle : (y : T_1) \times T_2 \). The third (kinding) premise follows immediately by regularity (lemma 22).

From \( \Gamma \vdash u_1 : S_1 \) and \( S_1 \leftrightarrow T_1 \) we directly get \( \Gamma \vdash \text{DS}_S^T u_1 : T_1 \).

For the second premise, we want to apply WF_DTM_PAIR. So we must show the three premises of that rule.

1. \( \Gamma, y : T_1 \vdash y : T_1 \). Immediate by WF_DTM_VAR.
2. \( \Gamma, y : T_1 \vdash \text{DS}_S^T u_2 : T_2 \). Also immediate, using the fact that \( S_2 \leftrightarrow T_2 \) as we noted before.
3. \( \Gamma, y : T_1 \vdash (y : T_1) \times T_2 : * \). By regularity (lemma 22).

• Suppose it was by EVAL_DTM_DS_CONSTR. So the step looks like

\[ \text{EVAL_DTM_DS_CONSTR} \]

\[ C : S \rightarrow A \in \Psi_0 \]
\[ C : (y : T_1) \rightarrow B t_1 \in \Psi_0 \]
\[ \text{argToD}_C u = v \]
\[ \text{DS}_S^T (C u) \xrightarrow{\xi} t \equiv [v/y] t_1 \triangleright (C v) \]

and we must show \( \Gamma \vdash t \equiv [v/y] t_1 \triangleright C v : B t \).

By property 6 we have \( \Gamma \vdash v : T_1 \). So \( \Gamma \vdash C v : B [v/y] t_1 \). By EQ_DTM_ASSUMPTION and EQ_DTY_APP we have \( \Gamma, t \equiv [v/y] t_1 \vdash B [v/y] t_1 \equiv B t \), so by WF_DTM_CONV we have \( \Gamma, t \equiv [v/y] t_1 \vdash C v : B t \).

By inversion on the premise \( A \equiv B t \) we get \( B : T_0 \Rightarrow * \in \Psi_0 \) and FO \( \text{T}_0 \), so by lemma 29 and substitution and weakening, we get \( \Gamma \vdash [v/y] t_1 : T_0 \). Also, from inversion (lemma 25) on the premise \( B : T_1 : * \), we get \( \Gamma \vdash t : T_0 \). Hence by WF_DTM_GUARD we get \( \Gamma \vdash t \equiv [v/y] t_1 \triangleright C v : B t \) as required.

• Suppose it was by EVAL_DTM_DS_UNIT. So the step looks like

\[ \text{EVAL_DTM_DS_UNIT} \]

\[ \text{DS}_{\text{Unit}} \xrightarrow{\xi} \text{Unit} \]

We must show \( \Gamma \vdash \text{Unit} \), which is straightforwardly true.

Case WF_DTM_GUARD. So \( [t_0/y_0] t \) is a guard-expression, which means that either \( t \) is a guard-expression or \( t \) is \( y_0 \).

In the former case, we can push the substitution in and the situation looks like this:

\[ \Gamma \vdash [t_0/y_0] t_1 : T_0 \]
\[ \Gamma \vdash [t_0/y_0] t_2 : T_0 \]
\[ \text{FO}(T_0) \]
\[ \Gamma, [t_0/y_0] t_1 \equiv [t_0/y_0] t_2 \vdash [t_0/y_0] t : T \]
\[ \Gamma \vdash [t_0/y_0] t_1 \equiv [t_0/y_0] t_2 \triangleright [t_0/y_0] t : T \quad \text{WF_DTM_GUARD} \]
Directly by the IH we get $\Gamma \vdash [t_0' / y_0]t_1 : T_0$ and $\Gamma \vdash [t_0' / y_0]t_2 : T_0$. The IH also gives us $\Gamma, [t_0 / y_0]t_1 \equiv [t_0' / y_0]t_2 \vdash [t_0' / y_0]t : T$. Now by $\text{EQ}_\text{DTM}_\text{STEP}$ we have $\Gamma \vdash t_0 \equiv t_0'$, so by $\text{EQ}_\text{DTM}_\text{SUBST}$ we know $\Gamma \vdash [t_0 / y_0]t_1 \equiv [t_0' / y_0]t_1$. Similarly for $t_2$. So by Context Conversion (lemma 21) we get $\Gamma, [t_0' / y_0]t_1 \equiv [t_0' / y_0]t_2 \vdash [t_0' / y_0]t : T$. We conclude by re-applying $\text{WF}_\text{DTM}_\text{GUARD}$.

The other possibility is that the entire expression is a guard-expression which steps, and we must prove that its type is preserved. So the typing rule looks like

\[
\begin{align*}
\Gamma \vdash t_0 & : T_0 \\
\Gamma \vdash t_1 & : T_0 \\
\text{FO}(T_0) & \\
\Gamma, t_1 \equiv t_0 & \vdash t : T \\
\Gamma \vdash t_1 \equiv t_0 & \vdash t : T & \text{WF}_\text{DTM}_\text{GUARD}
\end{align*}
\]

We consider the ways the expression $t_1 \equiv t_0 \triangleright t$ can step:

- **By $\text{Eval}_\text{DTM}_\text{CTX}$** when the context is $\square \equiv t_0 \triangleright t$ and $t_1 \rightarrow t_1'$. We must show $\Gamma \vdash t_1' \equiv t_0 \triangleright t : T$.

  By the IH we have $\Gamma \vdash t_1' : T_0$, so it suffices to show $\Gamma, t_1' \equiv t_0 \vdash t : T$, and then we can re-apply $\text{WF}_\text{DTM}_\text{GUARD}$. By $\text{EQ}_\text{DTM}_\text{STEP}$ we know that $\Gamma \vdash t_1 \equiv t_1'$ and by $\text{EQ}_\text{DTM}_\text{REFL}$ we know $\Gamma \vdash t_0 \equiv t_0$. So this follows by context conversion (lemma 21) on the assumption $\Gamma, t_1 \equiv t_0 \vdash t : T$.

- **By $\text{Eval}_\text{DTM}_\text{CTX}$** when the context is $v \equiv \square \triangleright t$. This is similar to the previous case.

- **By $\text{Eval}_\text{DTM}_\text{GUARD}_\text{REFL}$.** In this case the expression steps to $t$.

  The premise to the rule says $\Gamma, v \equiv v \vdash t : T$, but by $\text{EQ}_\text{DTM}_\text{REFL}$ we have $\Gamma \vdash v \equiv v$, so by $\text{Cut}$ (lemma 18) we get $\Gamma \vdash t : T$ as required.

- **By $\text{Eval}_\text{DTM}_\text{GUARD}_\text{ERROR}$.** In this case the entire expression steps to $\text{error}$, and we can indeed type $\Gamma \vdash \text{error} : T$ as required (using regularity, lemma 22, for the required kinding premise).

**Case $\text{wf}_\text{dtm}_\text{unit}$.** Since unit doesn’t step we must have $[t_0 / y_0]t = [t_0' / y_0]t$ and the result is trivial.

**Case $\text{wf}_\text{dtm}_\text{error}$.** Similar to the previous case.

The cases for $\Gamma \vdash [t_0 / y_0]T : K$ are:

**Case $\text{wf}_\text{dtm}_\text{arr}$.** The type $[t_0 / y_0]T$ must be some arrow type. Since the variable is bound by the arrow we can pick it to not clash with $y_0$, so the type is in fact of the form $(y : [t_0 / y_0]T_1) \rightarrow [t_0 / y_0]T_2$, and the situation looks like

\[
\begin{align*}
\Gamma \vdash [t_0 / y_0]T_1 & : * \\
\Gamma, y : [t_0 / y_0]T_1 & \vdash [t_0 / y_0]T_2 : * \\
\Gamma & \vdash (y : [t_0 / y_0]T_1) \rightarrow [t_0 / y_0]T_2 : * & \text{WF}_\text{DTM}_\text{ARR}
\end{align*}
\]

Directly by the IH we get $\Gamma \vdash [t_0' / y_0]T_1 : *$. By the IH we get $\Gamma \vdash [t_0' / y_0]T_1 : *$ and $\Gamma, y : [t_0 / y_0]T_1 \vdash [t_0' / y_0]T_2 : *$. By $\text{EQ}_\text{DTM}_\text{STEP}$ we know $\Gamma \vdash t_0 \equiv t_0'$, so by lemma 19 $\Gamma \vdash [t_0 / y_0]T_1 \equiv [t_0' / y_0]T_1$. So by context conversion (lemma 20) we have $\Gamma, y : [t_0' / y_0]T_1 \vdash [t_0' / y_0]T_2 : *$. Re-apply $\text{WF}_\text{DTM}_\text{ARR}$ to get $\Gamma \vdash (y : [t_0' / y]T_1) \rightarrow [t_0' / y]T_2 : *$ as required.

**Case $\text{wf}_\text{dtm}_\text{pair}$.** Similar to the previous case.

**Case $\text{wf}_\text{dtm}_\text{app}$.** The situation looks like:

\[
\begin{align*}
\Gamma & \vdash [t_0 / y_0]T : T_1 \Rightarrow * \\
\Gamma \vdash [t_0 / y_0]t_1 : T_1 \\
\Gamma & \vdash ([t_0 / y_0]T) ([t_0 / y_0]t_1) : * & \text{WF}_\text{DTM}_\text{APP}
\end{align*}
\]

By the IH we get $\Gamma \vdash [t_0' / y_0]T : T_1 \Rightarrow *$, and by the mutual IH we get $\Gamma \vdash [t_0' / y_0]t_1 : T_1$. Then we can re-apply $\text{WF}_\text{DTM}_\text{APP}$.
Case \texttt{wf\_dty\_data}. Since data constructors \(B\) do not step we must have \([t_0/y_0]T = [t'_0/y_0]T\) and the result is trivial.

Case \texttt{wf\_dtm\_conv}: The situation looks like:

\[
\begin{align*}
\Gamma &\vdash [t_0/y_0]t : T \\
\Gamma &\vdash T \equiv T' \\
\Gamma &\vdash T' : * \\
\end{align*}
\]

By the IH we get \(\Gamma \vdash [t'_0/y_0]t : T'\). Conclude by re-applying \texttt{wf\_dtm\_conv}.

\[\square\]

B.3 Progress

\textbf{Lemma 30} (Parallel reduction contains evaluation).

1. If \(t \rightarrow t'\) then \(t \rightarrow_p t'\).

2. If \(s \rightarrow s'\) then \(s \rightarrow_p s'\).

\textit{Proof}. Easy from inspecting the definition of \(\rightarrow_p\). \[\square\]

\textbf{Property 8.} If \(\text{argToD}_C u\) is defined, then \(\text{argToD}_C[u_1/x_1]u = [u_1/x_1](\text{argToD}_C u)\) and \(\text{argToD}_C[v_1/y_1]u = [v_1/y_1](\text{argToD}_C u)\).

\textbf{Property 9.} If \(\text{argToS}_C v\) is defined, then \(\text{argToS}_C[u_1/x_1]v = [u_1/x_1](\text{argToS}_C v)\) and \(\text{argToS}_C[v_1/y_1]v = [v_1/y_1](\text{argToS}_C v)\).

\textbf{Property 10.} If \(u \rightarrow_p u'\), then \(\text{argToD}_C u \rightarrow_p \text{argToD}_C u'\).

\textbf{Property 11.} If \(v \rightarrow_p v'\), then \(\text{argToS}_C v \rightarrow_p \text{argToS}_C v'\).

\textbf{Lemma 31} (Substitution for parallel reduction). Suppose \(u \rightarrow_p u'\), \(s \rightarrow_p s'\), \(v \rightarrow_p v'\), \(t \rightarrow_p t'\), \(S \rightarrow_p S'\), and \(T \rightarrow_p T'\). Then

1. \([u/x]s_2 \rightarrow_p [u'/x]s'_2\)
2. \([u/x]t_2 \rightarrow_p [u'/x]t'_2\)
3. \([u/x]S \rightarrow_p [u'/x]S'\)
4. \([u/x]T \rightarrow_p [u'/x]T'\)
5. \([v/y]s_2 \rightarrow_p [v'/y]s'_2\)
6. \([v/y]t_2 \rightarrow_p [v'/y]t'_2\)
7. \([v/y]S \rightarrow_p [v'/y]S'\)
8. \([v/y]T \rightarrow_p [v'/y]T'\)

\textit{Proof}. By mutual induction on \(s \rightarrow_p s'\), \(t \rightarrow_p t'\), \(S \rightarrow_p S'\) and \(T \rightarrow_p T'\). Most of the cases are very similar, we show two representative ones (for substitution of dependent terms \(v\) into dependent applications \(t_1 t_2\)). We also show the cases involving DS/SD-boundaries on constructors, since those motivate the substitution properties for \text{argToD} and \text{argToS}.
Case **par_eval_dtm_app**: The rule looks like

\[
\begin{array}{c}
t_1 \rightarrow_p t'_1 \\
t_2 \rightarrow_p t'_2 \\
(t_1, t_2) \rightarrow_p (t'_1, t'_2)
\end{array}
\]

PAR_EVAL_DTM_APP

By the IH we get \([v/y]t_1 \rightarrow_p [v'/y]t'_1\) and \([v/y]t_2 \rightarrow_p [v'/y]t'_2\). So re-applying `PAR_EVAL_DTM_APPBETA` we get \([v/y](t_1 t_2) \rightarrow_p [v'/y](t_1 t'_2)\) as required.

Case **par_eval_dtm_appBeta**: The rule looks like

\[
\begin{array}{c}
t_1 \rightarrow_p t'_1 v_2 \\
(\lambda y_1: T_1) v_2 \rightarrow_p v'_2 y_1 t'_1
\end{array}
\]

PAR_EVAL_DTM_APPBETA

Since \(y_1\) is a bound variable we can pick so that \(y_1 \notin \text{fv}(v_2)\). The IH gives us \([v/y]t_1 \rightarrow_p [v'/y]t'_1\) and \([v/y]v_2 \rightarrow_p [v'/y]v'_2\). By lemma 12 \([v/y]v_2\) is still a value, so pushing down the substitution and re-applying `PAR_EVAL_DTM_APPBETA` we get \([v/y](\lambda y_1: T_1) v_2) \rightarrow_p [v'/y]v'_2 [y'/y]t'_1\). Noting that \(y_1 \notin \text{fv}(v'_2)\) we have \([v'/y]v'_2[y'/y]t'_1 = [v'/y][v'_2/y_1]t'_1\), so we have showed \([v/y](\lambda y_1: T_1) v_2) \rightarrow_p [v'/y][v'_2/y_1]t'_1\) as required.

Case **par_eval_dtm_ds_constr**: The rule looks like

\[
\begin{array}{c}
C: S \rightarrow A \in \Psi_0 \\
C(\lambda y_1: T_1) \rightarrow B t_1 \in \Psi_0 \\
\text{argToD}_C u' = v_1 \\
\text{u} \rightarrow_p u' \\
\text{t} \rightarrow_p t' \\
DS^{(B t)}_A (C u) \rightarrow_p \text{t'} \cong [v_1/y_1]t_1 \triangleright (C v_1)
\end{array}
\]

PAR_EVAL_DTM_DS_CONSTR

By mutual IH we get \([v/y]u \rightarrow_p [v'/y]u'\). So by property 10, \(\text{argToD}_C[v/y]u \rightarrow_p \text{argToD}_C[v'/y]u'\). Also by IH, we have \([v/y]t \rightarrow_p [v'/y]t\). So re-applying `PAR_EVAL_DTM_DS_CONSTR`, we have that

\[
\text{DS}^{(B [v/y])}_A (C [v/y]u) \rightarrow_p [v'/y]t' \cong [\text{argToD}_C[v'/y]u/y_1]t_1 \triangleright (C [\text{argToD}_C[v'/y]u]).
\]

By property 8 we know that \(\text{argToD}_C[v'/y]u = [v'/y][\text{argToD}_C u]\), so

\[
[\text{argToD}_C[v'/y]u/y_1]t_1 = [v'/y][\text{argToD}_C u/y_1]t_1.
\]

From the assumption that the signature is well-formed \((\vdash \Psi)\) we in particular get that \(\vdash (y: T_1) \rightarrow B t_1 : \ast\), so \(y \notin \text{fv}(t_1)\), and \([v'/y][\text{argToD}_C u/y_1]t_1 = [v'/y][\text{argToD}_C u/y_1]t_1\). So pulling the substitutions out, we have in fact shown

\[
[v/y]DS^{(B t)}_A (C u) \rightarrow_p [v'/y]t' \cong [v'/y][\text{argToD}_C u/y_1]t_1 \triangleright (C [v'/y]([\text{argToD}_C u])),
\]

as required.

Case **par_eval_stm_sd_constr**: The rule looks like

\[
\begin{array}{c}
\text{constrs} \text{ } A = \Sigma^i \\
C: S \rightarrow A \in \Psi_0 \\
C(\lambda y_1: T_1) \rightarrow B t_1 \in \Psi_0 \\
B: T_2 \Rightarrow \ast \in \Psi_0 \\
\text{argToS}_C v'_1 = u_2 \\
v_1 \rightarrow_p v'_1 \\
SD^{(B t)}_A C v_1 \rightarrow_p C u_1
\end{array}
\]

PAR_EVAL_STM_SD_CONSTR

54
By mutual IH we get \([v/y]v_1 \rightarrow_p [v'/y]v_1'\). So by re-applying \(\text{PAR-EVAL-STM-SD-CONSTR}\) we get
\[
[v/y](\text{SD}^A_{(B_1)}(C \ v_1)) \rightarrow_p C (\text{argToS}_C([v'/y]v_1')).
\]
By property 9 we can commute the substitution past \(\text{argToS}\), so we have in fact shown
\[
[v/y](\text{SD}^A_{(B_1)}(C \ v_1)) \rightarrow_p [v'/y](C (\text{argToS}_C v_1')),
\]
as required.

\[\tag*{\square}\]

**Lemma 32** (One-step diamond property for parallel reduction).

1. If \(s \rightarrow_p s_1\) and \(s \rightarrow_p s_2\), then there exists some \(s'\) such that \(s_1 \rightarrow_p s'\) and \(s_2 \rightarrow_p s'\).

2. If \(S \rightarrow_p S_1\) and \(S \rightarrow_p S_2\), then there exists some \(S'\) such that \(S_1 \rightarrow_p S'\) and \(S_2 \rightarrow_p S'\).

3. If \(t \rightarrow_p t_1\) and \(t \rightarrow_p t_2\), then there exists some \(t'\) such that \(t_1 \rightarrow_p t'\) and \(t_2 \rightarrow_p t'\).

4. If \(T \rightarrow_p T_1\) and \(T \rightarrow_p T_2\), then there exists some \(T'\) such that \(T_1 \rightarrow_p T'\) and \(T_2 \rightarrow_p T'\).

**Proof.** By induction on the structure of \(s, S, t\) and \(T\). In each case we consider the (non-REFL) ways the term/type can step. (If one of the steps is by REF\(L\) the result is trivial).

**Cases for \(s\):**

**Case \(x\).** Trivial since \(x\) doesn’t step.

**Case \(\text{unit}\), \(\text{error}\).** Similar.

**Case \(\lambda x:S.s\).** The only way this expression can step is by \(S\) and \(s\) stepping; apply IH.

**Case \(s_1 s_2\).** Consider the pairs of ways that the expression may step:

- Both are \(\text{PAR-EVAL-STM-APP}\). In other words, we have \(s_1 s_2 \rightarrow_p s_11 s_21\) and \(s_1 s_2 \rightarrow_p s_12 s_22\). By the IH for \(s_1\) we get \(s_11 \rightarrow_p s'_1\) and \(s_12 \rightarrow_p s'_1\) for some \(s'_1\), and similarly for \(s_2\). So then by \(\text{PAR-EVAL-STM-APP}\), we get \(s_11 s_12 \rightarrow_p s'_1 s'_2\) and \(s_12 s_22 \rightarrow_p s'_1 s'_2\) as required.

- One of them is \(\text{PAR-EVAL-STM-APP}\) and one is \(\text{PAR-EVAL-STM-BETA}\). In other words, we have

\[
(\lambda x:S.s_0) \ u_2 \rightarrow_p ([u_21/x]s_0) \quad \text{where } s_0 \rightarrow_p s_01 \text{ and } u_2 \rightarrow_p u_21
\]

\[
(\lambda x:S.s_0) \ u_2 \rightarrow_p (\lambda x:S.s_0) \ u_22 \quad \text{where } s_0 \rightarrow_p s_02 \text{ and } u_2 \rightarrow_p u_22
\]

By the IH we have \(s_01 \rightarrow_p s'_1\) and \(s_02 \rightarrow_p s'_2\) for some \(s'_0\), and also \(u_21 \rightarrow_p u'_2\) and \(u_22 \rightarrow_p u'_2\) for some \(u'_2\). By lemma 31 we have \([u_21/x]s_01 \rightarrow_p [u'_2/x]s'_0\), and by \(\text{PAR-EVAL-STM-BETA}\) we have
\[
(\lambda x:S.s_02) \ u_2 \rightarrow_p [u'_2/x]s'_0,\text{ as required.}
\]

- Both of them are \(\text{PAR-EVAL-STM-BETA}\). In other words we have

\[
(\lambda x:S.s_0) \ u_2 \rightarrow_p ([u_21/x]s_0) \quad \text{where } s_0 \rightarrow_p s_01 \text{ and } u_2 \rightarrow_p u_21
\]

\[
(\lambda x:S.s_0) \ u_2 \rightarrow_p ([u_22/x]s_0) \quad \text{where } s_0 \rightarrow_p s_02 \text{ and } u_2 \rightarrow_p u_22
\]

By the IH we have \(s_01 \rightarrow_p s'_1\) and \(s_02 \rightarrow_p s'_2\) for some \(s'_0\), and also \(u_21 \rightarrow_p u'_2\) and \(u_22 \rightarrow_p u'_2\) for some \(u'_2\). Now by lemma 31, \([u_21/x]s_01 \rightarrow_p [u'_2/x]s'_0\) and \([u_22/x]s_02 \rightarrow_p [u'_2/x]s'_0\) as required.

- One of them is \(\text{PAR-EVAL-STM-ERROR}\). By considering the cases for the context \(E_x\), we see that the error transition is either \(\text{error} \rightarrow_p \text{error}\) or \(u_1 \rightarrow_p \text{error}\). Since \(\text{error}\) is not a value, the other transition can not be \(\text{PAR-EVAL-STM-BETA}\), so it must be either \(\text{ERROR}\) or \(\text{APP}\). If it is \(\text{ERROR}\), then both terms step to \(\text{error}\) and we are done; if it is \(\text{APP}\) then the term stepped to \(\text{error} s'_2\) or \(u'_1 \text{error}\), which can again step to \(\text{error}\).
Case \(<s_1, s_2>\). Consider the pairs of ways the expression may step:

- By two \textsc{par-\_eval-\_stm-\_pair} transitions. We reason similarly to the case for two \textsc{par-\_eval-\_stm-\_app} transitions above.
- By one \textsc{par-\_eval-\_stm-\_pair} and one \textsc{par-\_eval-\_stm-\_error} transition. Stepping by \textsc{pair} will still leave the term in a form where \textsc{error} applies.
- By two \textsc{par-\_eval-\_stm-\_error} transitions. Then both terms step to \textsc{error}, so we are done.

Case \(s.1, s.2, C s\). Similar to the previous case.

Case case \(s\) of \(C_i x_i \rightarrow s_i\). We consider the ways the expression may step.

- Both transitions are by \textsc{par-\_eval-\_stm-\_case}. We reason as in the above cases.
- One transition was by \textsc{par-\_eval-\_stm-\_case}, and one by \textsc{par-\_eval-\_stm-\_caseBeta}. In other words we have

\[
\text{case } C_i \ u \ 
\text{of } C_i x_i \rightarrow s_i \ 
\rightarrow_p [u_1/x_i]s_1 \ 
\text{where } u \rightarrow_p u_1 \ 
\text{and } s_i \rightarrow_p s_1
\]

\[
\text{case } C_i \ u \ 
\text{of } C_i x_i \rightarrow s_i \ 
\rightarrow_p \text{ case } C_i \ u_2 \ 
\text{of } C_i x_i \rightarrow s_i \ 
\rightarrow_p [u'/x_i]s_i'
\]

Now by IH we have \(u_i \rightarrow_p u_i'\) and \(u_2 \rightarrow_p u_2'\) for some \(u_i'\), and also \(s_i \rightarrow_p s_i'\) and \(s_2 \rightarrow_p s_2'\) for each \(i\). By lemma 31 we get \([u_1/x_i]s_1 \rightarrow_p [u'/x_i]s_i',\) and by \textsc{par-\_eval-\_caseBeta} we get \(\text{case } C_i \ u_2 \ 
\text{of } C_i x_i \rightarrow s_2 \ 
\rightarrow_p [u'/x_i]s_i',\) as required.

- Both transitions are by \textsc{par-\_eval-\_stm-\_caseBeta}. As in the case of two \textsc{par-\_eval-\_stm-\_beta} transitions, this follows by IH and lemma 31.

- One transition was by \textsc{par-\_eval-\_stm-\_caseBeta}. So the term must be \textsc{case error} of \(C_i x_i \rightarrow s_i\). We see that the other transition must be either \textsc{case} or \textsc{error}, and in both cases the resulting terms are joinable at \textsc{error}.

Case \texttt{letd}\(y = t\) in \(s\) Consider the pairs of ways the expressions may step:

- Both are \textsc{par-\_eval-\_stm-\_letd}. This follows directly by IH, similar to previous congruence cases.

- One transition is \textsc{par-\_eval-\_stm-\_error}. Considering the possibilities for \(E_s\), we see that the transition must be \texttt{letd}\(y = \textsc{error}\) in \(s\). Then, since \textsc{error} is not a value, the only possibilities for the other transition is \textsc{par-\_eval-\_stm-\_error} (in which case the terms already are joined at \textsc{error}) and \textsc{par-\_eval-\_stm-\_letd} (which reduces to a term where \textsc{par-\_eval-\_stm-\_error} can still fire).

- One transition is \textsc{par-\_eval-\_stm-\_letdBeta}, the other is \textsc{par-\_eval-\_stm-\_letd}. In other words we have

\[
\texttt{letd}\ y = v \ 
\text{in } s \ 
\rightarrow_p \ [v_1/y]s_1 \ 
\text{where } v \rightarrow_p v_1 \ 
\text{and } s \rightarrow_p s_1
\]

\[
\texttt{letd}\ y = v \ 
\text{in } s \ 
\rightarrow_p \texttt{letd}\ y = v_2 \ 
\text{in } s_2 \ 
\text{where } v \rightarrow_p v_2 \ 
\text{and } s \rightarrow_p s_2
\]

Now by the mutual IH we know \(v_1 \rightarrow_p v_1'\) and \(v_2 \rightarrow_p v_2'\) for some \(v_1'\), and by the IH similar for \(s\). So by lemma 31 we get \([v_1/y]s_1 \rightarrow_p [v'/y]s_1'\), while by \textsc{par-\_eval-\_letdBeta} we get \(\texttt{letd}\ y = v_2 \ 
\text{in } s_2 \ 
\rightarrow_p [v'/y]s_1',\) as required.

- Both are \textsc{par-\_eval-\_stm-\_letdBeta}. In other words we have

\[
\texttt{letd}\ y = v \ 
\text{in } s \ 
\rightarrow_p \ [v_1/y]s_1 \ 
\text{where } v \rightarrow_p v_1 \ 
\text{and } s \rightarrow_p s_1
\]

\[
\texttt{letd}\ y = v \ 
\text{in } s \ 
\rightarrow_p \ [v_2/y]s_1 \ 
\text{where } v \rightarrow_p v_2 \ 
\text{and } s \rightarrow_p s_2
\]

By mutual IH and IH we get that \(v_1 \rightarrow_p v_1'\) and \(s \rightarrow_p s_1',\) and conclude by lemma 31.
Case $SD_{S_2}^{T_2}.t$. Consider the pairs of ways the expression may step:

- Both are `PAR_EVAL_STM_SD`. We reason as in previous cases above.

- One transition is by `PAR_EVAL_STM_ERROR`. Then considering the possible evaluation contexts the term must be $SD_{S'}^{T'}_{error}$, and there is only one possible transition, so the other transition must be `PAR_EVAL_STM_ERROR` also.

- One transition is by `PAR_EVAL_STM_ABS` and one is by `PAR_EVAL_STM_SD`. In other words we have

$$SD_{((yT_1)\rightarrow T_2)}^{(S_1\rightarrow S_2)}(\lambda y: T_3.t \rightarrow p \lambda x: S_{12}.letd y' = DS_{S_{12}}^{T_{12}}x \in SD_{[y'/y]}^{S_{12}}(\lambda y: T_{31}.t_1) y')$$

where $T_1 \rightarrow p T_{11}, T_2 \rightarrow p T_{21}, S_1 \rightarrow p S_{11}, S_2 \rightarrow p S_{21}, T_3 \rightarrow p T_{31}, t \rightarrow p t_1$.

$$SD_{((yT_1)\rightarrow T_2)}^{(S_1\rightarrow S_2)}(\lambda y: T_3.t \rightarrow p SD_{((yT_1)\rightarrow T_2)}^{(S_1\rightarrow S_2)}(\lambda y: T_{32}.t_2)$$

where $T_1 \rightarrow p T_{12}, T_2 \rightarrow p T_{22}, S_1 \rightarrow p S_{12}, S_2 \rightarrow p S_{22}, T_3 \rightarrow p T_{32}, t \rightarrow p t_2$.

Now, by the (mutual) IH we get that $T_{11} \rightarrow p T'_{11}$ and $T_{12} \rightarrow p T'_{12}$ for some $T'$, and similarly for the other subterms. Since $y'$ is a value, we know by lemma 31 that $[y'/y]T_{21} \rightarrow p [y'/y]T_2'$. So by a combination of `PAR_EVAL_STM_ABS`, `PAR_EVAL_STM_LETD`, `PAR_EVAL_DTM_ABs`, `PAR_EVAL_STM_SD` and `PAR_EVAL_DTM_DS`, we have

$$\lambda x: S_{12}.letd y' = (DS_{S_{12}}^{T_{12}}x) \in SD_{[y'/y]}^{S_{12}}(\lambda y: T_{31}.t) y'$$

while by `PAR_EVAL_STM_DS_ABs` we have

$$SD_{(yT_1)\rightarrow T_2}^{(S_1\rightarrow S_2)}(\lambda y: T_{32}.t_2 \rightarrow p \lambda x: S'_{12}.letd y' = DS_{S'_{12}}^{T'_{12}}x \in SD_{[y'/y]}^{S'_{12}}(\lambda y: T'_{32}.t') y')$$

as required.

- Both transitions are by `PAR_EVAL_STM_SD_ABs`. In other words we have

$$SD_{((yT_1)\rightarrow T_2)}^{(S_1\rightarrow S_2)}(\lambda y: T_3.t \rightarrow p \lambda x: S_{12}.letd y' = DS_{S_{12}}^{T_{12}}x \in SD_{[y'/y]}^{S_{12}}(\lambda y: T_{31}.t_1) y')$$

where $T_1 \rightarrow p T_{11}, T_2 \rightarrow p T_{21}, S_1 \rightarrow p S_{11}, S_2 \rightarrow p S_{21}, T_3 \rightarrow p T_{31}, t \rightarrow p t_1$.

$$SD_{((yT_1)\rightarrow T_2)}^{(S_1\rightarrow S_2)}(\lambda y: T_3.t \rightarrow p \lambda x: S_{12}.letd y' = DS_{S_{12}}^{T_{12}}x \in SD_{[y'/y]}^{S_{12}}(\lambda y: T_{32}.t_2) y')$$

where $T_1 \rightarrow p T_{11}, T_2 \rightarrow p T_{21}, S_1 \rightarrow p S_{11}, S_2 \rightarrow p S_{21}, T_3 \rightarrow p T_{31}, t \rightarrow p t_1$.

By the (mutual) IH we get that $T_{11} \rightarrow p T'_{11}$ and $T_{12} \rightarrow p T'_{12}$ for some $T'$, and similarly for the other subterms. By reasoning similarly to the previous case we see that both terms step to

$\lambda x: S'_{12}.letd y' = DS_{S'_{12}}^{T'_{12}}x \in SD_{[y'/y]}^{S'_{12}}(\lambda y: T'_{31}.t') y')$.

- One transition is by `PAR_EVAL_STM_SD_PAIR` and the other one is by `PAR_EVAL_STM_SD`. In other words we have (by considering case for how e.g. the expression $S_1 S_2$ may step)

$$SD_{(yT_1)\rightarrow T_2}^{S_1+S_2}(\langle v_1, v_2 \rangle \rightarrow p SD_{(yT_1)\rightarrow T_2}^{S_1+v_{11}}SD_{(yT_1)\rightarrow T_2}^{S_2+v_{21}})$$

where $S_1 \rightarrow p S_{11}$ and $S_2 \rightarrow p S_{21}$.

$$SD_{(yT_1)\rightarrow T_2}^{S_1+S_2}(\langle v_1, v_2 \rangle \rightarrow p SD_{(yT_1)\rightarrow T_2}^{S_1+S_2}SD_{(yT_1)\rightarrow T_2}^{S_1+S_2} \langle u_1, u_2 \rangle)$$

where $S_1 \rightarrow p S_{12}$ and $S_2 \rightarrow p S_{22}$.

By the IH we get $S_{11} \rightarrow p S'_{11}$ and $S_{12} \rightarrow p S'_{12}$ for some $S'_{1}$, and similarly for the other subterms.

By lemma 31 we know $[v_{11}/y]T_{21} \rightarrow p [v'_{11}/y]T_{21}$, so by various congruence rules

$SD_{(yT_1)\rightarrow T_2}^{S_1+S_2}SD_{(yT_1)\rightarrow T_2}^{S_1+S_2} \langle u_1, u_2 \rangle \rightarrow p SD_{(yT_1)\rightarrow T_2}^{S_1+S_2}SD_{(yT_1)\rightarrow T_2}^{S_1+S_2}$.

Meanwhile by `PAR_EVAL_SD_PAIR` we have

$SD_{(yT_1)\rightarrow T_2}^{S_1+S_2} \langle u_1, u_2 \rangle \rightarrow p SD_{(yT_1)\rightarrow T_2}^{S_1+S_2}SD_{(yT_1)\rightarrow T_2}^{S_1+S_2}$ as required.

- Both transitions are by `PAR_EVAL_STM_SD_PAIR`. Using lemma 31 and congruence rules, we get that the terms are joinable at

$$SD_{((yT_1)\rightarrow T_2)}^{S'_{1}}SD_{(yT_1)\rightarrow T_2}^{S'_{1}}.$$
• One transition is by \texttt{PAR\_EVAL\_STM\_SD\_CONSTR} and one is by \texttt{PAR\_EVAL\_STM\_SD}. In other words we have

\[
\begin{align*}
SD_{(B)}^{\lambda}(C_{v}) & \rightarrow_{p} C(\text{argToS}_{C,v_{1}}) & \text{where } v \rightarrow_{p} v_{1} \\
SD_{(A)}^{\lambda}(C_{v}) & \rightarrow_{p} SD_{(B_{z_{2}})}^{\lambda}(C_{v_{2}}) & \text{where } A \rightarrow_{p} A_{2}, t \rightarrow_{p} t_{2} \text{ and } v \rightarrow_{p} v_{2}
\end{align*}
\]

By the IH, we get that \(v_{1} \rightarrow_{p} v'\) and \(v_{2} \rightarrow_{p} v'\) for some \(v'\). By property 11, we have \(\text{argToS}_{C,v_{1}} \rightarrow_{p} \text{argToS}_{C,v'_{1}}\), so \(C(\text{argToS}_{C,v_{1}}) \rightarrow_{p} C(\text{argToS}_{C,v'_{1}})\). And by \texttt{PAR\_EVAL\_STM\_CONSTR} we have \(SD_{(B_{z_{2}})}^{\lambda}(C_{v_{2}}) \rightarrow_{p} C(\text{argToS}_{C,v'_{2}})\), as required.

• Both transitions are by \texttt{PAR\_EVAL\_STM\_CONSTR}. In other words, we have

\[
\begin{align*}
SD_{(B)}^{\lambda}(C_{v}) & \rightarrow_{p} C(\text{argToS}_{C,v_{1}}) & \text{where } v \rightarrow_{p} v_{1} \\
SD_{(A)}^{\lambda}(C_{v}) & \rightarrow_{p} C(\text{argToS}_{C,v_{2}}) & \text{where } v \rightarrow_{p} v_{2}
\end{align*}
\]

By the mutual IH we know \(v_{1} \rightarrow_{p} v'\) and \(v_{2} \rightarrow_{p} v'\) for some \(v'\). By property 11 we know \(\text{argToS}_{C,v_{1}} \rightarrow_{p} \text{argToS}_{C,v'_{1}}\) and \(\text{argToS}_{C,v_{2}} \rightarrow_{p} \text{argToS}_{C,v'_{2}}\). So by congruence we have \(C(\text{argToS}_{C,v_{1}}) \rightarrow_{p} C(\text{argToS}_{C,v'_{1}})\) and \(C(\text{argToS}_{C,v_{2}}) \rightarrow_{p} C(\text{argToS}_{C,v'_{2}})\) as required.

• One transition is by \texttt{PAR\_EVAL\_STM\_UNIT}. So the term is \(SD_{\text{unit}}^{\lambda}\), and there is only one possible transition, so the other transition must be \texttt{PAR\_EVAL\_STM\_UNIT} also.

Cases for \(S\): These are all trivial, since there are only congruence rules.

Cases for \(t\):

\textbf{Case } y, \textbf{unit, error}. These terms do not step.

\textbf{Case } \lambda y: T.t_{s}, <t_{1}, t_{2}> , t_{1}, t_{1}, \textbf{and } C t \ . These expressions can only stop by congruence rules, the proof is similar to some previous cases.

\textbf{Case } t_{1} t_{2} \textbf{ and case } t \textbf{ of } C_{1}, y \rightarrow_{t} C_{1}^{t} \ . These are similar to the corresponding cases for simply-typed terms.

\textbf{Case } DS_{S}^{T} s \ We consider the pairs of ways the expression may stop.

• Both transitions are by \texttt{PAR\_EVAL\_ERROR}. This follows by the IH and reasoning similar to the previous congruence cases.

• One transition is by \texttt{PAR\_EVAL\_DS}. By considering the possible evaluation contexts \(E_{t}\) we see that the transition must be \(DS_{S}^{T} \text{error} \rightarrow_{p} \text{error}\). The only possibilities for the other transition is that it also steps to \text{error} or that it is \(DS_{S}^{T} \text{error} \rightarrow_{p} DS_{S'}^{T} \text{error}\); in both cases the resulting terms are joinable at \text{error}.

• One transition is by \texttt{PAR\_EVAL\_DS\_ABS}, and the other one is by \texttt{PAR\_EVAL\_DS}. So the term must have the form \(DS_{(S_{1} \rightarrow S_{2})}^{(\langle y \rightarrow T_{1} \rangle \rightarrow T_{2})} \lambda x: S_{3}, s. \) By inversion on the rules, we know that the only way the subterm \((y: T_{1}) \rightarrow T_{2}\) can step by congruence if \(T_{1}\) and \(T_{2}\) steps. In other words we have

\[
\begin{align*}
& DS_{(S_{1} \rightarrow S_{2})}^{(\langle y \rightarrow T_{1} \rangle \rightarrow T_{2})} \lambda x: S_{3}, s \rightarrow_{p} \lambda y: T_{11}, DS_{S_{21}}^{S_{2}(\langle \lambda x: S_{31}, s_{1} \rangle (SD_{S_{11}, y}^{1}))} \\
& DS_{S_{1}}^{S_{1}, y} \rightarrow_{p} DS_{S_{11}}^{S_{11}, y} \rightarrow_{p} DS_{S_{11}}^{S_{11}, y} \rightarrow_{p} DS_{S_{11}}^{S_{11}, y} \rightarrow_{p} DS_{S_{11}}^{S_{11}, y}
\end{align*}
\]

where \(T_{1} \rightarrow_{p} T_{11}\) and \(T_{1} \rightarrow_{p} T_{12}\), and similar for the other subterms. By the IH we get \(T_{11} \rightarrow_{p} T_{1}'\) and \(T_{12} \rightarrow_{p} T_{1}'\) for some \(T'\), and similarly for the other subterms. So by a combination of congruence rules, \(\lambda y: T_{11}, DS_{S_{21}}^{S_{2}(\langle \lambda x: S_{31}, s_{1} \rangle (SD_{S_{11}, y}^{1}))} \rightarrow_{p} \lambda y: T_{1}' DS_{S_{21}}^{S_{2}(\langle \lambda x: S_{31}, s'_{1} \rangle (SD_{S_{11}, y}^{1}))}, while by \texttt{PAR\_EVAL\_DS\_ABS} DS_{S_{11}}^{S_{11}, y} \rightarrow_{p} DS_{S_{11}}^{S_{11}, y} \rightarrow_{p} \lambda y: T_{1}' DS_{S_{21}}^{S_{2}(\langle \lambda x: S_{31}, s'_{1} \rangle (SD_{S_{11}, y}^{1}))} as required.

58
• Both transitions are by \texttt{PAR-EVAL\_DS\_ABS}. So the transition are
\[
\begin{align*}
\text{DS}_{y:T'_1} & \rightarrow T_2 \quad \lambda x:S_1.s \rightarrow_p \lambda y:T_{11}.\text{DS}_{S_2}^T (\langle \lambda x:S_1.s_1 \rangle (\text{SD}_{S_1}^{T_1} \ y)) \\
\text{DS}_{y:T'_2} & \rightarrow T_2 \quad \lambda x:S_3.s \rightarrow_p \lambda y:T_{12}.\text{DS}_{S_2}^T (\langle \lambda x:S_2.s_2 \rangle (\text{SD}_{S_1}^{T_2} \ y))
\end{align*}
\]
which join at \(\lambda y:T'_1'.\text{DS}_{S_2}^T (\langle \lambda x:S'_1.s'_1 \rangle (\text{SD}_{S_1}^{T'_1} \ y))\) by congruence rules.

• One transition is by \texttt{PAR-EVAL\_DS\_PAIR}, one is by \texttt{PAR-EVAL\_DS}. In other words (and considering the possible transitions \((y:T_1) * T_2\) can make), we have
\[
\begin{align*}
\text{DS}_{y:T'_1} & \rightarrow T_2 \quad <u_1, u_2> \rightarrow_p y' \rightarrow DS_{S_1}^{T_1} u_11 \quad <y', DS_{S_2}^{T_1} u_21> \\
\text{DS}_{y:T'_2} & \rightarrow T_2 \quad <u_1, u_2> \rightarrow_p DS_{y:T'_1} T_2 \rightarrow <u_12, u_22>
\end{align*}
\]
where \(T_1 \rightarrow_p T_{11}\) and \(T_1 \rightarrow_p T_{12}\), etc. By the IH we get get \(T_{11} \rightarrow_p T'_1\) and \(T_{12} \rightarrow_p T'_2\), etc. By lemma 31 we know \([y'/y]T_{21} \rightarrow_p [y'/y]T_2\). So by various congruence rules we get
\[
\begin{align*}
\text{let } y' & = DS_{S_1}^{T_1} u_11 \text{ in } <y', DS_{S_2}^{T_1} u_21> \rightarrow_p y' \rightarrow DS_{S_1}^{T'_1} u_11' \text{ in } <y', DS_{S_2}^{T'_1} u_21'>
\end{align*}
\]
while by \texttt{PAR-EVAL\_DS\_PAIR} we have \(DS_{S_1}^{T_1} u_11 \rightarrow_p DS_{S_1}^{T'_1} u_11'\) in \(<y', DS_{S_2}^{T'_1} u_21'>\), as required.

• Both transitions are by \texttt{PAR-EVAL\_DS\_PAIR}. So the transitions are
\[
\begin{align*}
\text{DS}_{y:T'_1} & \rightarrow T_2 \quad <u_1, u_2> \rightarrow_p y' \rightarrow DS_{S_1}^{T_1} u_11 \quad <y', DS_{S_2}^{T_1} u_21> \\
\text{DS}_{y:T'_2} & \rightarrow T_2 \quad <u_1, u_2> \rightarrow_p DS_{y:T'_1} T_2 \rightarrow <u_12, u_22>
\end{align*}
\]
which join at \(let \ y' = DS_{S_1}^{T'_1} u_11' \text{ in } <y', DS_{S_2}^{T'_1} u_21'>\) by various congruence rules.

• One transition is by \texttt{PAR-EVAL\_DS\_CONSTR} and the other one is by \texttt{PAR-EVAL\_DS}. In other words we have
\[
\begin{align*}
\text{DS}_{A}^{(B \ t)} C & \rightarrow_p t_1 \equiv [\text{argToD}_C u_1/y] t \triangleright C (\text{argToD}_C u_1) \quad \text{where } t \rightarrow_p t_1 \text{ and } u \rightarrow_p u_1 \\
\text{DS}_{A}^{(B \ t)} C & \rightarrow_p DS_{A}^{(B \ t_2)} C u_2 \quad \text{where } t \rightarrow_p t_2 \text{ and } u \rightarrow_p u_2
\end{align*}
\]
By the IH we have \(t_1 \rightarrow_p t'\) and \(t_2 \rightarrow_p t'\) for some \(t'\), and \(u_1 \rightarrow_p u'\) and \(u_2 \rightarrow_p u'\) for some \(u'\). By property 10, we know \(\text{argToD}_C u_1 \rightarrow_p \text{argToD}_C u'\) and \(\text{argToD}_C u_2 \rightarrow_p \text{argToD}_C u'\). So by lemma 31 and congruence rules we have
\[
\begin{align*}
t_1 \equiv [\text{argToD}_C u_1/y] t \triangleright C (\text{argToD}_C u_1) \rightarrow_p t' \equiv [\text{argToD}_C u'/y] t \triangleright C (\text{argToD}_C u')
\end{align*}
\]
while by \texttt{PAR-EVAL\_DS\_CONSTR} (note that the term \(t\) comes out of the signature \(\Psi_0\) and is therefore always the same) we get
\[
\begin{align*}
\text{DS}_{A}^{(B \ t_2)} C u_2 & \rightarrow_p t' \equiv [\text{argToD}_C u'/y] t \triangleright C (\text{argToD}_C u')
\end{align*}
\]
as required.

• Both transitions are by \texttt{PAR-EVAL\_DS\_CONSTR}. In other words we have
\[
\begin{align*}
\text{DS}_{A}^{(B \ t)} C & \rightarrow_p t_1 \equiv [\text{argToD}_C u_1/y] t \triangleright C (\text{argToD}_C u_1) \quad \text{where } t \rightarrow_p t_1 \text{ and } u \rightarrow_p u_1 \\
\text{DS}_{A}^{(B \ t)} C & \rightarrow_p t_2 \equiv [\text{argToD}_C u_2/y] t \triangleright C (\text{argToD}_C u_2) \quad \text{where } t \rightarrow_p t_2 \text{ and } u \rightarrow_p u_2
\end{align*}
\]
Similarly to the previous case, by IH, property 10, lemma 31, and congruence rules, there terms are joinable at
\[
t' \equiv [\text{argToD}_C u'/y] t \triangleright C (\text{argToD}_C u').
\]
• One transition is by PAR_EVAL_DS_UNIT. That is, the transition looks like $\text{DS}_{\text{Unit}} \rightarrow_p \text{unit}$. The only possibility is that the other transition is PAR_EVAL_DS_UNIT also.

Case $t_1 \equiv t_2 \triangleright t$ We consider the pairs of ways the expression may step.

• Both transitions are PAR_EVAL_DTM_GUARD.
• One transition is PAR_EVAL_DTM_ERROR. By considering cases for the context $E$, we see that the transition must be one of $\text{error} \equiv t_2 \triangleright t \rightarrow_p \text{error}$ or $v_1 \equiv \text{error} \triangleright t \rightarrow_p \text{error}$. Since error is not a value, neither of PAR_EVAL_DTM_GUARD_REFL or PAR_EVAL_DTM_GUARD_ERROR applies, so we know the other transition must be by either PAR_EVAL_DTM_GUARD, in which case the reduct can step to error also, or PAR_EVAL_DTM_ERROR, in which case we are immediately done.
• One transition is PAR_EVAL_DTM_GUARD_REFL. So the term must be of the form $v \equiv v \triangleright t$. The only other transitions that can match is congruence or REF. If the other transition is also REF we can conclude directly by IH. If the other transition is PAR_EVAL_DTM_GUARD, then we have

$$v \equiv v \triangleright t \rightarrow_p t_1$$

where $t \rightarrow_p t_1$

$$v \equiv v \triangleright t \rightarrow_p v_2 \equiv v_{22} \triangleright t_2$$

where $v \rightarrow_p v_{12}$, $v \rightarrow_p v_{22}$ and $t \rightarrow_p t_2$.

By the IH we have that $t_1 \rightarrow_p t'$ and $t_2 \rightarrow_p t'$ for some $t'$, and by PAR_EVAL_DTM_GUARD_REFL, we have $v_2 \equiv v_{22} \triangleright t_2 \rightarrow_p t'$ as required.

• One transition is PAR_EVAL_DTM_GUARD_ERROR. The reasoning is similar to the previous case.

Cases for $T$: These are all trivial, since there are only congruence rules.

**Lemma 33** (Confluence of parallel reduction). If $t \rightarrow_p t_1$ and $t \rightarrow_p t_2$, then there exists some $t'$ such that $t_1 \rightarrow_p t'$ and $t_2 \rightarrow_p t'$.

**Proof.** This is a simple corollary of the 1-step version (lemma 32), by “diagram chasing to fill in the rectangle” (see e.g. [2], lemma 3.2.2). □

**Lemma 34** (Compatibility of parallel reduction). Suppose $t \rightarrow_p t'$ and $s \rightarrow_p s'$. Then

- $[t/y]t_1 \rightarrow_p [t'/y]t_1$
- $[t/y]s_1 \rightarrow_p [t'/y]s_1$
- $[t/y]T_1 \rightarrow_p [t'/y]T_1$
- $[t/y]S_1 \rightarrow_p [t'/y]S_1$
- $[s/x]t_1 \rightarrow_p [s'/x]t_1$
- $[s/x]s_1 \rightarrow_p [s'/x]s_1$
- $[s/x]T_1 \rightarrow_p [s'/x]T_1$
- $[s/x]S_1 \rightarrow_p [s'/x]S_1$

**Proof.** Mutual induction on the structure of $t_1$, $s_1$, $T_1$ and $S_1$. These are all similar, so we show only cases for $t_1$.

Case $y_1$. There are two cases depending on whether $y_1 = y$ or not. If it is, we must show $t \rightarrow_p t'$, which we have by assumption. If not we must show $y_1 \rightarrow_p y_1$, which is true by PAR_EVAL_DTM_REFL.

Case $t_1 t_2$. We note that $[t/y][t_1 t_2] = [t/y]t_1 [t/y]t_2$, so we can then apply the IH.

Case $<t_1, t_2>$, $t_1 . 1 , t_1 . 2 , C t_1 , DS_{T_1} s_1$, and $t_{11} \equiv t_{12} \triangleright t_1$. Similar to the previous case, except we also appeal to the mutual IH for $T_1$ and $S_1$.  

60
Case $\lambda y_1: T_1, t_1$ . Since $y_1$ is a bound variable we can pick it so that $y_1 \neq y$. Then $[t/y](\lambda y_1: T_1, t_1) = \lambda y_1: [t/y]T_1, [t/y]t_1$, and we conclude by (direct and mutual) IH.

Case $\text{case } t_1 \text{ of } \overline{C_i y_i} \rightarrow t_i^i$ . Similar to the previous case.

Case $\text{unit}$ . Trivial since $[t/y]\text{unit} = [t'/y]\text{unit} = \text{unit}$.

Case $\text{error}$ . Similar to the previous case.

\begin{IEEEproof}
Proof. We proceed by induction on $\cdot \vdash t_1 \equiv t_2$. The cases are

Case $\text{eq_dtm_assumption}$: This cannot happen because the context is empty.

Case $\text{eq_dtm_step}$: We are given $t_1 \rightarrow t_2$ as a premise to the rule. By lemma 30 we have $t_1 \rightarrow_p t_2$, so take $t' = t_2$.

Case $\text{eq_dtm_refl}$: Take $t' = t$.

Case $\text{eq_dtm_sym}$: Immediate from the IH.

Case $\text{eq_dtm_trans}$: The IH gives us that there exists $t_1$ and $t_2$ such that $t \rightarrow_p t_1$, $t' \rightarrow_p t_1$, $t' \rightarrow_p t_2$ and $t'' \rightarrow_p t_2$. So by confluence (lemma 33) applied to $t'$ we know there exists $t_3$ such that $t_1 \rightarrow_p t_3$ and $t_1 \rightarrow_p t_3$, which is what we needed.

Case $\text{eq_dtm_subst}$: The rule looks like

\[
\begin{array}{c}
\Gamma \vdash t_1 \equiv t_1' \\
y \not\in \text{dom}(\Gamma)
\end{array}
\frac{}{\Gamma \vdash [t_1/y]t \equiv [t_1'/y]t}^{\text{EQ_DTM_SUBST}}
\]

The IH gives us two chains of reductions:

- $t_1 \rightarrow_p t_{12} \rightarrow_p t_{13} \ldots \rightarrow_p t_n$
- $t_1' \rightarrow_p t_{12}' \rightarrow_p t_{13}' \ldots \rightarrow p t_n$.  

By lemma 34 we can lift these to chains

- $[t_1/y]t \rightarrow_p [t_{12}/y]t \rightarrow_p [t_{13}/y]t \ldots \rightarrow_p [t_n/y]t$
- $[t_1'/y]t \rightarrow_p [t_{12}'/y]t \rightarrow_p [t_{13}'/y]t \ldots \rightarrow_p [t_n/y]t$.

which is what we need.

Case $\text{eq_dtm_subst_val}$: The rule looks like

\[
\begin{array}{c}
\Gamma \vdash t \equiv t'
\end{array}
\frac{}{\Gamma \vdash [v/y]t \equiv [v/y]t'}^{\text{EQ_DTM_SUBST_Val}}
\]

The IH gives us two chains of reductions

- $t_1 \rightarrow_p t_{12} \rightarrow_p t_{13} \ldots \rightarrow_p t_n$
- $t_1' \rightarrow_p t_{12}' \rightarrow_p t_{13}' \ldots \rightarrow p t_n$.

Use part (6) of lemma 31 to get

- $[v/y]t_1 \rightarrow_p [v/y]t_{12} \rightarrow_p [v/y]t_{13} \ldots \rightarrow_p [v/y]t_n$
- $[v/y]t_1' \rightarrow_p [v/y]t_{12}' \rightarrow_p [v/y]t_{13}' \ldots \rightarrow_p [v/y]t_n$.

which is what we need.
Case `eq_dtm_ssubst_val`: Similar to the previous case.

**Lemma 36.** If $C_1 \neq C_2$, then we never have $\vdash C_1 v_1 \cong C_2 v_2$.

**Proof.** By the previous lemma there must be some term $t'$ such that $C_1 v_1 \rightarrow_P t'$ and $C_2 v_2 \rightarrow_P t'$. But that is impossible: by looking at the rules for $\rightarrow_P$ we see that they can never change the outermost constructor of a term.

**Lemma 37** (Canonical forms for `ss`).

1. If $\vdash u : S_1 \rightarrow S_2$ then $u$ is $\lambda x : S . s$.
2. If $\vdash u : S_1 * S_2$ then $u$ is $<u_1, u_2>$.
3. If $\vdash u : \text{Unit}$ then $u$ is $\text{unit}$.
4. If $\vdash u : A$ then $u$ is $C u'$ and $C : S \rightarrow A \in \Psi_0$.

**Proof.** By induction on the typing judgment $\vdash s : S$. The cases are:

**Case `wf_stm_var`:** This is impossible since the context is empty.

**Case `wf_stm_abs`:** The type is an arrow type, so only the first case applies. $s$ is indeed a $\lambda$-expression.

**Case `wf_stm_pair, wf_stmctor, wf_stm_unit`:** Similar to the previous case, $s$ does indeed have the right form.

**Case `wf_stm_app, proj1, proj2, case, letd, sd, error`:** In these rules, the subject of the typing is not a value.

**Lemma 38** (Canonical forms for `ts`).

1. If $\vdash v : (y : T_1) \rightarrow T_2$ then $v$ is $\lambda y : T . t$.
2. If $\vdash v : (y : T_1) * T_2$ then $v$ is $<v_1, v_2>$.
3. If $\vdash v : \text{Unit}$ then $v$ is $\text{unit}$.
4. If $\vdash v : B t$ then $v$ is $C u'$ and $C : (y : T) \rightarrow B t' \in \Psi_0$.

**Proof.** By induction on the typing judgment $\vdash t : T$. The cases are:

**Case `wf_dtm_var`:** This is impossible since the context is empty.

**Case `wf_dtm_abs`:** The type is an arrow type, so only the first item applies. $t$ is indeed a $\lambda$-expression.

**Case `wf_dtm_pair, wf_dtm_unit, wf_dtm_ctor`:** Similar to the abs case.

**Case `wf_dtm_app, proj1, proj2, case, ds, guard, error`:** In these rules the subject of the typing is not a value.
Case \textit{wf_dtm_conv}: The typing rule looks like

\[
\begin{align*}
\Gamma &\vdash t : T \\
\Gamma &\vdash T \equiv T' \\
\Gamma &\vdash T' : * \\
\hline
\Gamma &\vdash t : T' \quad \text{WEA DTM\_CONV}
\end{align*}
\]

We have as an assumption that the top-level shape of \(T'\) is \(\to, *\), Unit or \(B\), and we want to invoke the IH on the premise \(\cdot \vdash t : T\). So we need to establish that \(T\) has the same top-level shape as \(T'\). This follows by a case analysis on the judgment \(\cdot \vdash T \equiv T'\). We see that all the type-equivalence rules preserve the top-level shape of the type except \textit{eq_dty}\_incon and inconsistency is ruled out by lemma 36.

\begin{proof}
\end{proof}

\textbf{Property 12.}

1. If \(C : S \to A \in \Psi_0\) and \(\text{corr}(A, B)\), then \(C : (y : T_1) \to B \ t_1 \in \Psi_0\) for some \(T_1\) and \(t_1\).

2. If \(C : (y : T) \to B \ t' \in \Psi_0\) and \(\text{corr}(A, B)\), then \(C : S \to A \in \Psi_0\) for some \(S\).

\textbf{Lemma 39} (Case coverage). If \(\Gamma \vdash \text{case} \ C \ v \ of \ C_1 \ y_1 \to t_1 : T \ and \ \vdash \Psi_0\), then \(C\) is one of the constructors \(C_i\).

\textbf{Property 13.}

1. If \(C : S \to A \in \Psi_0\) and \(C : (y : T_1) \to B \ t_1 \in \Psi_0\) and \(\cdot \vdash u : S\), then \(\text{argToD}^{C}_u\) is defined.

2. If \(C : S \to A \in \Psi_0\) and \(C : (y : T_1) \to B \ t_1 \in \Psi_0\) and \(\cdot \vdash v : T_1\), then \(\text{argToS}^{C}_v\) is defined.

\textbf{Theorem 4} (Progress).

1. If \(\cdot \vdash t : T\) then either \(t \rightarrow t'\), \(t\) is a value, or \(t\) is error.

2. If \(\cdot \vdash s : S\) then either \(s \rightarrow s'\), \(s\) is a value, or \(s\) is error.

\textbf{Proof}. Proof by mutual induction on the judgments \(\cdot \vdash s : S\) and \(\cdot \vdash t : T\).

The cases for \(\cdot \vdash t : T\) are:

\textbf{Case \textit{wf_dtm_var}}: Impossible since the context is empty.

\textbf{Case \textit{wf_dtm_abs}}: \(t\) is already a value.

\textbf{Case \textit{wf_dtm_app}}: The case looks like

\[
\begin{align*}
\Gamma &\vdash t_1 : (y : T_1) \to T_2 \\
\Gamma &\vdash t_2 : T_1 \\
\Gamma &\vdash \{t_2/y\} T_2 : * \\
\hline
\Gamma &\vdash t_1 t_2 : \{t_2/y\} T_2 \quad \text{WEA DTM\_APP}
\end{align*}
\]

By the IH we get that \(t_1\) and \(t_2\) either step, are values, or are error. If either of them are error, then the term steps by \textit{eval_dtm_error}. Otherwise, if \(t_1\) steps, then the entire term steps by \textit{eval_dtm_app}. Similarly if \(t_1\) is a value and \(t_2\) steps.

Finally, suppose both \(t_1\) and \(t_2\) are values. Then, by lemma 38 \(t_1\) must be a \(\lambda\)-abstraction, so the application steps by \textit{eval_dtm_beta}.

\textbf{Case \textit{wf_dtm_proj1, wf_dtm_proj2}}: similar to \textit{app}.
Case \texttt{wf_dtm\_pair}: By the IH the components of the pair are \texttt{error}, one steps (in which case the entire expression steps), or they are values (in which case the entire expression is a value).

Case \texttt{wf_dtm\_ctor}: Similar to \texttt{PAIR}.

Case \texttt{wf_dtm\_case}: The case looks like
\[
\Gamma \vdash t : B t' \\
\Gamma \vdash T : * \\
\text{constrs } B = \overrightarrow{C_i} \\
\overrightarrow{C_i} : (y_i : T_i) \rightarrow B t' \in \Psi_0 \\
\Gamma, y_i : T_i, t' \equiv t'_i, t \equiv C_i, y_i \vdash t_i : T_i \\
\Gamma \vdash \text{case } t \text{ of } \overrightarrow{C_i, y_i} \rightarrow t'_i : T \quad \text{\texttt{WF\_DTM\_CASE}}
\]

By the IH, \(t\) either steps, is \texttt{error}, or is a value. In the first two cases the entire expression steps. If \(t\) is a value, then by canonical forms (lemma 38), we know that \(t\) is \(C\ v\) and \(C'(y : T) \rightarrow B t' \in \Psi_0\). Then by lemma 39 we know \(C\) is one of the branches of the case expression, so it can step by \texttt{WF\_DTM\_CASE}.

Case \texttt{wf_dtm\_ds}: The case looks like
\[
\Gamma \vdash s : S \\
\Gamma \vdash T : * \\
S \leftrightarrow T \\
\Gamma \vdash DS_S s : T \quad \text{\texttt{WF\_DTM\_DS}}
\]

By the mutual IH for \(s\), \(s\) steps, is a value, or is \texttt{error}. If it steps or is an \texttt{error}, the entire expression steps. So suppose \(s\) is a value.

By inversion on the judgment \(S \leftrightarrow T\) there are four possibilities:

- \(S\) is \(S_1 \rightarrow S_2\) and \(T\) is \((y : T_1) \rightarrow T_2\). By canonical forms (lemma 37), \(s\) must be a \(\lambda\)-abstraction, so the entire expression steps by \texttt{EVAL\_DTM\_DS\_ABS}.
- \(S\) is \(S_1 \ast S_2\) and \(T\) is \((y : T_1) \ast T_2\). By canonical forms (lemma 37), \(s\) must be a pair, so the entire expression steps by \texttt{EVAL\_DTM\_DS\_PAIR}.
- \(S\) and \(T\) are unit. By canonical forms (lemma 37) \(s\) must be unit, so the entire expression steps by \texttt{EVAL\_DTM\_DS\_ABS}.
- \(S\) is \(A\), \(T\) is \(B\ t\), and \(\text{corr}(A, B)\). By canonical forms (lemma 37, \(s\) is \(C\ u\') and \(C : S \rightarrow A \in \Psi_0\). So by property 12, \(C' : (y : T_1) \rightarrow B t_1 \in \Psi_0\) for some \(T_1\) and \(t_1\). We have \(\cdot \vdash u : S\) by assumption, so \(\argToD(u)\) is defined by property 13. Then the entire expression steps to \(t \equiv [v/y] t_1 \triangleright (C' \ (\argToD(u)))\) by \texttt{EVAL\_DTM\_SD\_CONSTR}.

Case \texttt{wf_dtm\_guard}: The case looks like
\[
\Gamma \vdash t_0 : T_0 \\
\Gamma \vdash t_1 : T_0 \\
\text{FO}(T_0) \\
\Gamma, t_2 \equiv t_0 \vdash t : T \\
\Gamma \vdash t_1 \equiv t_0 \triangleright t : T \quad \text{\texttt{WF\_DTM\_GUARD}}
\]

By the IH, \(t_1\) and \(t_0\) and each is a value, \texttt{error}, or steps. If they step or are error the entire expression steps by \texttt{EVAL\_DTM\_CTX} or \texttt{EVAL\_DTM\_ERROR}. Finally, if \(t_1\) and \(t_2\) are both values, then the expression steps by \texttt{EVAL\_DTM\_GUARD\_REFL} or \texttt{EVAL\_DTM\_GUARD\_ERROR}.

Case \texttt{wf_dtm\_error}: Here \(t\) is \texttt{error} as required.
Case **wf_dtm_conv**: The case looks like

\[
\begin{align*}
\Gamma &\vdash t : T \\
\Gamma &\vdash T \equiv T' \\
\Gamma &\vdash T' : * \\
\hline
\therefore \quad \Gamma &\vdash t : T' \tag{WF_DTM_CONV}
\end{align*}
\]

so the conclusion follows directly by the IH for \(t\).

The cases for \(\cdot \vdash s : S\) are mostly routine, but we show the one involving an SD-boundary:

Case **wf_stm_sd**: The case looks like

\[
\begin{align*}
\Gamma &\vdash t : T \\
S &\leftrightarrow T \\
\hline
\therefore \quad \Gamma &\vdash SD_\Psi^\gamma t : S \tag{WF_STM_SD}
\end{align*}
\]

By the mutual IH, \(t\) either, steps, is \text{error}, or is a value. If it steps or is \text{error} the entire expression steps, so assume it is a value.

By inversion on the judgment \(S \leftrightarrow T\) there are four possibilities:

- \(S\) is \(S_1 \rightarrow S_2\) and \(T\) is \((y : T_1) \rightarrow T_2\). By canonical forms (lemma 38) we know \(t\) is a lambda. So the expression steps by \text{EVAL_STM_SD_ABS}.
- \(S\) is \(S_1 \ast S_2\) and \(T\) is \((y : T_1) \ast T_2\). By canonical forms (lemma 38) we know \(t\) is a pair of values. So the expression steps by \text{EVAL_STM_SD_PAIR}.
- \(S\) is \text{Unit} and \(T\) is \text{Unit}. By canonical forms (lemma 38) we know \(t\) is \text{unit}. So the expression steps by \text{EVAL_STM_SD_UNIT}.
- \(S\) is \text{A} and \(T\) is \text{B t} and \text{corr} (\text{A}, \text{B}). By canonical forms (lemma 38) we know \(t\) is \(C v'\) and \(C(y : T) \rightarrow B t' \in \Psi_0\). So by property 12 we have \(C : S \rightarrow S \in \Psi_0\) for some \(S\). By property 13 we know \text{argToS} \_C \_v is defined. Then the expression steps by \text{EVAL_STM_SD_CONSTR} to \(C (\text{argToS}_C \_v)\).

\(\square\)