Yale University
Department of Computer Science

A Type System for Certified Binaries

Zhong Shao Bratin Saha Valery Trifonov Nikolaos Papaspyrou
Yale University

YALEU/DCS/TR-1211
March 2001 (revised September 2001)

This research is based on work supported in part by DARPA OASIS grant F30602-99-1-0519, NSF grant CCR-9901011, and NSF ITR grant CCR-0081590. Any opinions, findings, and conclusions contained in this document are those of the authors and do not reflect the views of these agencies.

Abstract

A *certified binary* is a value together with a proof that the value satisfies a given specification. Existing compilers that generate certified code have focused on simple memory and control-flow safety rather than more advanced properties. In this paper, we present a general framework for explicitly representing complex propositions and proofs in typed intermediate and assembly languages. The new framework allows us to reason about certified programs that involve effects while still maintaining decidable typechecking. We show how to integrate an entire proof system (the calculus of inductive constructions) into a compiler intermediate language and how the intermediate language can undergo complex transformations (CPS and closure conversion) while preserving proofs represented in the type system. Our work provides a foundation for the process of automatically generating certified binaries in a type-theoretic framework.

A Type System for Certified Binaries

Zhong Shao Bratin Saha Valery Trifonov Nikolaos Papaspyrou
Department of Computer Science, Yale University
New Haven, CT 06520-8285, U.S.A.
{shao, saha, trifonov, nickie}@cs.yale.edu

Technical Report YALEU/DCS/TR-1211
March 2001 (revised September 2001)

Abstract

A *certified binary* is a value together with a proof that the value satisfies a given specification. Existing compilers that generate certified code have focused on simple memory and control-flow safety rather than more advanced properties. In this paper, we present a general framework for explicitly representing complex propositions and proofs in typed intermediate and assembly languages. The new framework allows us to reason about certified programs that involve effects while still maintaining decidable typechecking. We show how to integrate an entire proof system (the calculus of inductive constructions) into a compiler intermediate language and how the intermediate language can undergo complex transformations (CPS and closure conversion) while preserving proofs represented in the type system. Our work provides a foundation for the process of automatically generating certified binaries in a type-theoretic framework.

1 Introduction

Proof-carrying code (PCC), as pioneered by Necula and Lee [30, 29], allows a code producer to provide a machine-language program to a host, along with a formal proof of its safety. The proof can be mechanically checked by the host; the producer need not be trusted because a valid proof is incontrovertible evidence of safety.

The PCC framework is general because it can be applied to certify arbitrary data objects with complex specifications [32, 2]. For example, the Foundational PCC system [3] can certify any property expressible in Church's higher-order logic. Harper *et al.* [19, 7] call all these proof-carrying constructs certified binaries (or deliverables [7]). A *certified binary* is a value (which can be a function, a data structure, or a combination of both) together with a proof that the value satisfies a given specification.

Unfortunately, little is known on how to construct or generate certified binaries. Existing certifying compilers [31, 9] have focused on simple memory and control-flow safety only. Typed intermediate languages [22] and typed assembly languages [28] are effective techniques for automatically generating certified code; however, none of these type systems can rival the expressiveness of the actual higher-order logic as used in some PCC systems [3].

In this paper, we present a type-theoretic framework for constructing, composing, and reasoning about certified binaries. Our plan is to use the *formulae-as-types* principle [24] to represent propositions and proofs in a general type system, and then to investigate their relationship with compiler intermediate and assembly languages. We show how to integrate an entire proof system (the calculus of inductive constructions [35, 11]) into an intermediate language, and how to define complex transformations (CPS and closure conversion) of programs in this language so that they preserve proofs represented in the type system. Our paper builds upon a large body of previous work in the logic and theorem-proving community (see Barendregt *et al.* [5, 4] for a good summary), and makes the following new contributions:

- We show how to design new typed intermediate languages that are capable of representing and manipulating propositions and proofs. In particular, we show how to maintain decidability of typechecking when reasoning about certified programs that involve effects. This is different from the work done in the logic community which focuses on strongly normalizing (primitive recursive) programs.
- We maintain a phase distinction between compile-time typechecking and run-time evaluation. This property is often lost in the presence of dependent types (which are necessary for representing proofs in predicate logic). We achieve this by never having the type language (see Section 3) dependent on the computation language (see Section 4). Proofs are instead always represented at the type level using dependent kinds.
- We show how to use propositions to express program invariants and how to use proofs to serve as static capabilities. Following Xi and Pfenning [44], we use singleton types [23] to support the necessary interaction between the type and computation languages. We can assign an accurate type to unchecked vector (or array) access (see Section 4.2). Xi and Pfenning [44] can achieve the same using constraint checking, but their system does not support arbitrary propositions and (explicit) proofs, so it is less general than ours.
- We use a single type language to typecheck different compiler intermediate languages. This is crucial because it is impractical to have separate proof libraries for each intermediate language. We achieve this by using inductive definitions to define all types used to classify computation terms. This in turn nicely fits our work on (fully reflexive) intensional type analysis [39] into a single system.
- We show how to perform CPS and closure conversion on our intermediate languages while still preserving proofs represented in the type system. Existing algorithms [28, 21, 26, 6] all require that the transformation be performed on the entire type language. This is impractical because proofs are large in size; transforming them can alter their meanings and break the sharing among different languages. We present new techniques that completely solve these problems (Sections 5–6).

This research is based on work supported in part by DARPA OASIS grant F30602-99-1-0519, NSF grant CCR-9901011, and NSF ITR grant CCR-0081590. Any opinions, findings, and conclusions contained in this document are those of the authors and do not reflect the views of these agencies.

- Our type language is a variant of the calculus of inductive constructions [35, 11]. Following Werner [41], we give rigorous proofs for its meta-theoretic properties (subject reduction, strong normalization, confluence, and consistency of the underlying logic). We also give the soundness proof for our sample computation language. See Sections 3 and 4, and the appendix for more details.

As far as we know, our work is the first comprehensive study on how to incorporate higher-order predicate logic (with inductive terms and predicates) into typed intermediate languages. Our results are significant because they open up many new exciting possibilities in the area of type-based language design and compilation. The fact that we can internalize a very expressive logic into our type system means that formal reasoning traditionally done at the meta level can now be expressed inside the actual language itself. For example, much of the past work on program verification using Hoare-like logics may now be captured and made explicit in a typed intermediate language.

From the standpoint of type-based language design, recent work [22, 44, 13, 15, 40, 39] has produced many specialized, increasingly complex type systems, each with its own meta-theoretical proofs, yet it is unclear how they will fit together. We can hope to replace them with one very general type system whose meta theory is proved once and for all, and that allows the definition of specialized type operators via the general mechanism of inductive definitions. For example, inductive definitions subsume and generalize earlier systems on intensional type analysis [22, 14, 39].

We have started implementing our new type system in the FLINT compiler [36, 37], but making the implementation realistic still involves solving many remaining problems (*e.g.*, efficient proof representations). Nevertheless, we believe our current contributions constitute a significant step toward the goal of providing a practical end-to-end compiler that generates certified binaries.

2 Approach

Our main objectives are to design typed intermediate and low-level languages that can directly manipulate propositions and proofs, and then to use them to certify realistic programs. We want our type system to be simple but general; we also want to support complex transformations (CPS and closure conversion) that preserve proofs represented in the type system. In this section, we describe the main challenges involved in achieving these goals and give a high-level overview of our main techniques.

Before diving into the details, we first establish a few naming conventions that we will use in the rest of this paper. Typed intermediate languages are usually structured in the same way as typed λ-calculi. Figure 1 gives a fragment of a richly typed λ-calculus, organized into four levels: kind schema (*kscm*) u, kind κ, type τ, and expression (*exp*) e. If we ignore kind schema and other extensions, this is just the polymorphic λ-calculus F_ω [18].

We divide each typed intermediate language into a type sub-language and a computation sub-language. The type language contains the top three levels. Kind schemas classify kind terms while kinds classify type terms. We often say that a kind term κ has kind schema u, or a type term τ has kind κ. We assume all kinds used to classify type terms have kind schema Kind, and all types used to classify expressions have kind Ω. Both the function type $\tau_1 \to \tau_2$ and the polymorphic type $\forall t : \kappa.\, \tau$ have kind Ω. Following the tradition, we sometimes say "a kind κ" to imply that κ has kind schema Kind, "a type τ" to imply that τ has kind Ω, and "a type constructor τ" to imply that τ has kind "$\kappa \to \cdots \to \Omega$." Kind terms with other kind schemas, or type terms with other kinds are strictly referred to as "kind terms" or "type terms."

THE TYPE LANGUAGE:

(*kscm*) $u ::= \mathsf{Kind} \mid \ldots$

(*kind*) $\kappa ::= \kappa_1 \to \kappa_2 \mid \Omega \mid \ldots$

(*type*) $\tau ::= t \mid \lambda t{:}\kappa.\, \tau \mid \tau_1\, \tau_2 \mid \tau_1 \to \tau_2 \mid \forall t{:}\kappa.\, \tau \mid \ldots$

THE COMPUTATION LANGUAGE:

(*exp*) $e ::= x \mid \lambda x{:}\tau.\, e \mid e_1\, e_2 \mid \Lambda t{:}\kappa.\, e \mid e[\tau] \mid \ldots$

Figure 1: Typed λ-calculi—a skeleton

The computation language contains just the lowest level which is where we write the actual program. This language will eventually be compiled into machine code. We often use names such as computation terms, computation values, and computation functions to refer to various constructs at this level.

2.1 Representing propositions and proofs

The first step is to represent propositions and proofs for a particular logic in a type-theoretic setting. The most established technique is to use the *formulae-as-types* principle (a.k.a. the Curry-Howard correspondence) [24] to map propositions and proofs into a typed λ-calculus. The essential idea, which is inspired by constructive logic, is to use types (of kind Ω) to represent propositions, and expressions to represent proofs. A proof of an implication $P \supset Q$ is a function object that yields a proof of proposition Q when applied to a proof of proposition P. A proof of a conjunction $P \wedge Q$ is a pair (e_1, e_2) such that e_1 is a proof of P and e_2 is a proof of Q. A proof of disjunction $P \vee Q$ is a pair (b, e)—a tagged union—where b is either 0 or 1 and if $b = 0$, then e is a proof of P; if $b = 1$ then e is a proof of Q. There is no proof for the false proposition. A proof of a universally quantified proposition $\forall x \in B.P(x)$ is a function that maps every element b of the domain B into a proof of $P(b)$ where P is a unary predicate on elements of B. Finally, a proof of an existentially quantified proposition $\exists x \in B.P(x)$ is a pair (b, e) where b is an element of B and e is a proof of $P(b)$.

Proof-checking in the logic now becomes typechecking in the corresponding typed λ-calculus. There has been a large body of work done along this line in the last 30 years; most type-based proof assistants are based on this fundamental principle. Barendregt *et al.* [5, 4] give a good survey on previous work in this area.

2.2 Representing certified binaries

Under the type-theoretic setting, a certified binary S is just a pair (v, e) that consists of:

- a value v of type τ where v could be a function, a data structure, or any combination of both;
- and a proof e of $P(v)$ where P is a unary predicate on elements of type τ.

Here e is just an expression with type $P(v)$. The predicate P is a dependent type constructor with kind $\tau \to \Omega$. The entire package S has a dependent strong-sum type $\Sigma x{:}\tau.P(x)$.

For example, suppose Nat is the domain for natural numbers and $Prime$ is a unary predicate that asserts an element of Nat as a prime number, we introduce a type nat representing Nat, and a type constructor prime (of kind $\mathsf{nat} \to \Omega$) representing $Prime$. We can build a certified prime-number package by pairing a value v

(a natural number) with a proof for the proposition $\mathsf{prime}(v)$; the resulting certified binary has type $\Sigma x{:}\mathsf{nat}.\ \mathsf{prime}(x)$.

Function values can be certified in the same way. Given a function f that takes a natural number and returns another one as the result (*i.e.*, f has type $\mathsf{nat} \to \mathsf{nat}$), in order to show that f always maps a prime to another prime, we need a proof for the following proposition:

$$\forall x{\in}Nat.\ Prime(x) \supset Prime(f(x))$$

In a typed setting, this universally quantified proposition is represented as a dependent product type:

$$\Pi x{:}\mathsf{nat}.\ \mathsf{prime}(x) \to \mathsf{prime}(f(x))$$

The resulting certified binary has type

$$\Sigma f{:}\mathsf{nat} \to \mathsf{nat}.\ \Pi x{:}\mathsf{nat}.\ \mathsf{prime}(x) \to \mathsf{prime}(f(x))$$

Here the type is not only dependent on values but also on function applications such as $f(x)$, so verifying a certified binary involves typechecking the proof which in turn requires evaluating the underlying function application.

2.3 The problems with dependent types

The above scheme unfortunately fails to work in the context of typed intermediate (or assembly) languages. There are at least four problems with dependent types; the third and fourth are present even in the general context.

First, real programs often involve effects such as assignment, I/O, or non-termination. Effects interact badly with dependent types. In our previous example, suppose the function f does not terminate on certain inputs; then clearly, typechecking—which could involve applying f—would become undecidable. It is possible to use the effect discipline [38] to force types to be dependent on pure computation only, but this does not work in some typed λ-calculi; for example, a "pure" term in Girard's λU [18] could still diverge.

Even if applying f does not involve any effects, we still have more serious problems. In a type-preserving compiler, the body of the function f has to be compiled down to typed low-level languages. A few compilers perform typed CPS conversion [28], but in the presence of dependent types, this is a very difficult problem [6]. Also, typechecking in low-level languages would now require performing the equivalent of β-reductions on the low-level (assembly) code; this is awkward and difficult to support cleanly.

Third, it is important to maintain a phase distinction between compile-time typechecking and run-time evaluation. Having dependent strong-sum and dependent product types makes it harder to preserve this property. It is also difficult to support first-class certified binaries.

Finally, it would be nice to support a notion of subset types [10, 33]. A certified binary of type $\Sigma x{:}\mathsf{nat}.\ \mathsf{prime}(x)$ contains a natural number v and a proof that v is a prime. However, in some cases, we just want v to belong to a subset type $\{x{:}\mathsf{nat} \mid \mathsf{prime}(x)\}$, *i.e.*, v is a prime number but the proof of this is not together with v; instead, it can be constructed from the current context.

2.4 Separating the type and computation languages

We solve these problems by making sure that our type language is never dependent on the computation language. Because the actual program (*i.e.*, the computation term) would have to be compiled down to assembly code in any case, it is a bad idea to treat it as part of types. This strong separation immediately gives us back the phase-distinction property.

To represent propositions and proofs, we lift everything one level up: we use kinds to represent propositions, and type terms to represent proofs. The domain Nat is now represented by a kind Nat; the predicate $Prime$ is represented by a dependent kind term Prime which maps a type term of kind Nat into a proposition. A proof for proposition $\mathsf{Prime}(n)$ certifies that the type term n is a prime number.

To maintain decidable typechecking, we insist that the type language is strongly normalizing and free of side effects. This is possible because the type language no longer depends on any runtime computation. Given a type-level function g of kind $\mathsf{Nat} \to \mathsf{Nat}$, we can certify that it always maps a prime to another prime by building a proof τ_p for the following proposition, now represented as a dependent product kind:

$$\Pi t{:}\mathsf{Nat}.\mathsf{Prime}(t) \to \mathsf{Prime}(g(t)).$$

Essentially, we circumvent the problems with dependent types by replacing them with dependent kinds and by lifting everything (in the proof language) one level up.

To reason about actual programs, we still have to connect terms in the type language with those in the computation language. We follow Xi and Pfenning [44] and use singleton types [23] to relate computation values to type terms. In the previous example, we introduce a singleton type constructor snat of kind $\mathsf{Nat} \to \Omega$. Given a type term n of kind Nat, if a computation value v has type $\mathsf{snat}(n)$, then v denotes the natural number represented by n.

A certified binary for a prime number now contains three parts: a type term n of kind Nat, a proof for the proposition $\mathsf{Prime}(n)$, and a computation value of type $\mathsf{snat}(n)$. We can pack it up into an existential package and make it a first-class value with type:

$$\exists n{:}\mathsf{Nat}.\exists t{:}\mathsf{Prime}(n).\mathsf{snat}(n).$$

Here we use $\exists$ rather than Σ to emphasize that types and kinds are no longer dependent on computation terms. Under the erasure semantics [16], this certified binary is just an integer value of type $\mathsf{snat}(n)$ at run time.

A value v of the subset type (for prime numbers) would simply have type $\mathsf{snat}(n)$ as long as we can construct a proof for $\mathsf{Prime}(n)$ based on the information from the context.

We can also build certified binaries for programs that involve effects. Returning to our example, assume again that f is a function in the computation language which may not terminate on some inputs. Suppose we want to certify that if the input to f is a prime, and the call to f does return, then the result is also a prime. We can achieve this in two steps. First, we construct a type-level function g of kind $\mathsf{Nat} \to \mathsf{Nat}$ to simulate the behavior of f (on all inputs where f does terminate) and show that f has the following type:

$$\forall n{:}\mathsf{Nat}.\ \mathsf{snat}(n) \to \mathsf{snat}(g(n))$$

Here following Figure 1, we use $\forall$ and $\to$ to denote the polymorphic and function types for the computation language. The type for f says that if it takes an integer of type $\mathsf{snat}(n)$ as input and does not loop forever, then it will return an integer of type $\mathsf{snat}(g(n))$. Second, we construct a proof τ_p showing that g always maps a prime to another prime. The certified binary for f now also contains three parts: the type-level function g, the proof τ_p, and the computation function f itself. We can pack it into an existential package with type:

$$\exists g{:}\mathsf{Nat} \to \mathsf{Nat}.\ \exists p{:}(\Pi t{:}\mathsf{Nat}.\mathsf{Prime}(t) \to \mathsf{Prime}(g(t))).\\ \forall n{:}\mathsf{Nat}.\ \mathsf{snat}(n) \to \mathsf{snat}(g(n))$$

Notice this type also contains function applications such as $g(n)$, but g is a type-level function which is always strongly normalizing, so typechecking is still decidable.

We can also restrict f so that it can only be applied to prime numbers; all we need is to add an additional proof argument, so f has type:

$$\forall n{:}\mathsf{Nat}.\forall t{:}\mathsf{Prime}(n).\ \mathsf{snat}(n) \to \mathsf{snat}(g(n)).$$

Here, the parameter t serves as a static capability; a proof for $\mathsf{Prime}(n)$ exists only if n is indeed a prime.

2.5 Designing the type language

We can incorporate propositions and proofs into typed intermediate languages, but designing the actual type language is still a challenge. For decidable typechecking, the type language should not depend on the computation language and it must satisfy the usual meta-theoretical properties (*e.g.* strong normalization).

But the type language also has to fulfill its usual responsibilities. First, it must provide a set of types (of kind Ω) to classify the computation terms. A typical compiler intermediate language supports a large number of basic type constructors (*e.g.*, integer, array, record, tagged union, and function). These types may change their forms during compilation, so different intermediate languages may have different definitions of Ω; for example, a computation function at the source level may be turned into CPS-style, or later, to one whose arguments are machine registers [28]. We also want to support intensional type analysis [22] which is crucial for typechecking runtime services [27].

Our solution is to provide a general mechanism of inductive definitions in our type language and to define each such Ω as an inductive kind. This was made possible only recently [39] and it relies on the use of polymorphic kinds. Taking the type language in Figure 1 as an example, we add kind variables k and polymorphic kinds $\Pi k{:}u.\,\kappa$, and replace Ω and its associated type constructors with inductive definitions (not shown):

$$\begin{array}{ll}
(\textit{kscm}) & u ::= \mathsf{Kind} \mid \ldots \\
(\textit{kind}) & \kappa ::= \kappa_1 \to \kappa_2 \mid k \mid \Pi k{:}u.\,\kappa \mid \ldots \\
(\textit{type}) & \tau ::= t \mid \lambda t{:}\kappa.\,\tau \mid \tau_1\,\tau_2 \mid \lambda k{:}u.\,\tau \mid \tau[\kappa] \mid \ldots
\end{array}$$

At the type level, we add kind abstraction $\lambda k{:}u.\,\tau$ and kind application $\tau[\kappa]$. The kind Ω is now inductively defined as follows (see Sections 3–4 for more details):

$$\begin{array}{lll}
\mathsf{Inductive}\ \Omega\ :\ \mathsf{Kind} & := \twoheadrightarrow : & \Omega \to \Omega \to \Omega \\
& \mid \forall\ : & \Pi k{:}\mathsf{Kind}.\,(k \to \Omega) \to \Omega \\
& \vdots &
\end{array}$$

Here $\twoheadrightarrow$ and $\forall$ are two of the constructors (of Ω). The polymorphic type $\forall t:\kappa.\,\tau$ is now written as $\forall[\kappa]\,(\lambda t:\kappa.\,\tau)$; the function type $\tau_1 \to \tau_2$ is just $\twoheadrightarrow \tau_1\tau_2$.

Inductive definitions also greatly increase the programming power of our type language. We can introduce new data objects (*e.g.*, integers, lists) and define primitive recursive functions, all at the type level; these in turn are used to help model the behaviors of the computation terms.

To have the type language double up as a proof language for higher-order predicate logic, we add dependent product kind $\Pi t:\kappa_1.\,\kappa_2$, which subsumes the arrow kind $\kappa_1 \to \kappa_2$; we also add kind-level functions to represent predicates. Thus the type language naturally becomes the calculus of inductive constructions [35].

Notice standard formulation of Church's higher-order logic puts propositions at the same level as terms (which are type terms in our setup); proofs are then represented at a level below (parallel to our computation language). This does not work because we already require polymorphic kinds for the inductive definition of Ω; with impredicative polymorphism on both the kind and type levels, the proof language becomes Girard's λU [18] which is known to be inconsistent.

2.6 Proof-preserving compilation

Even with a proof system integrated into our intermediate languages, we still have to make sure that they can be CPS- and closure-converted down to low-level languages. These transformations should preserve proofs represented in the type system; in fact, they should not traverse the proofs at all since doing so is impractical with large proof libraries.

These challenges are non-trivial but the way we set up our type system makes it easier to solve them. First, because our type language does not depend on the computation language, we do not have the difficulties involved in CPS-converting dependently typed λ-calculi [6]. Second, all our intermediate languages share the same type language thus also the same proof library; this is possible because the Ω kind (and the associated types) for each intermediate language is just a regular inductive definition.

Finally, a type-preserving program transformation often requires translating the source types (of the source Ω kind) into the target types (of the target Ω kind). Existing CPS- and closure-conversion algorithms [28, 21, 26] all perform such translation at the meta-level; they have to go through every type term (thus every proof term in our setting) during the translation, because any type term may contain a sub-term which has the source Ω kind. In our framework, the fact that each Ω kind is inductively defined means that we can internalize and write the type-translation function inside our type language itself. This leads to elegant algorithms that do not traverse any proof terms but still preserve typing and proofs (see Sections 5–6 for details).

2.7 Putting it all together

A certifying compiler in our framework will have a series of intermediate languages, each corresponding to a particular stage in the compilation process; all will share the same type language. An intermediate language is now just the type language plus the corresponding computation terms, along with the inductive definition for the corresponding Ω kind. In the rest of this paper, we first give a formal definition of our type language (which will be named as TL from now on) in Section 3; we then present a sample computation language λ_H in Section 4; we show how λ_H can be CPS- and closure-converted into low-level languages in Sections 5–6; finally, we discuss related work and then conclude.

3 The Type Language TL

Our type language TL resembles the calculus of inductive constructions (CIC) implemented in the Coq proof assistant [25]. This is a great advantage because Coq is a very mature system and it has a large set of proof libraries which we can potentially reuse. For this paper, we decided not to directly use CIC as our type language for three reasons. First, CIC contains some features designed for program extraction [34] which are not required in our case (where proofs are only used as specifications for the computation terms). Second, as far as we know, there are still no formal studies covering the entire CIC language. Third, for theoretical purposes, we want to understand what are the most essential features for modeling certified binaries.

Motivations Following the discussion in Section 2.5, we organize TL into the following three levels:

$$
\begin{array}{lll}
(\textit{kscm}) & u ::= z \mid \Pi t\!:\!\kappa.\, u \mid \Pi k\!:\!u_1.\, u_2 \mid \mathsf{Kind} \\
(\textit{kind}) & \kappa ::= k \mid \lambda t\!:\!\kappa_1.\, \kappa_2 \mid \kappa[\tau] \mid \lambda k\!:\!u.\, \kappa \mid \kappa_1\, \kappa_2 \\
& \quad \mid \Pi t\!:\!\kappa_1.\, \kappa_2 \mid \Pi k\!:\!u.\, \kappa \mid \Pi z\!:\!\mathsf{Kscm}.\, \kappa \\
& \quad \mid \mathsf{Ind}(k\!:\!\mathsf{Kind})\{\vec{\kappa}\} \mid \mathsf{Elim}[\kappa', u](\tau)\{\vec{\kappa}\} \\
(\textit{type}) & \tau ::= t \mid \lambda t\!:\!\kappa.\, \tau \mid \tau_1\, \tau_2 \mid \lambda k\!:\!u.\, \tau \mid \tau[\kappa] \\
& \quad \mid \lambda z\!:\!\mathsf{Kscm}.\, \tau \mid \tau[u] \mid \mathsf{Ctor}\,(i, \kappa) \\
& \quad \mid \mathsf{Elim}[\kappa', \kappa](\tau')\{\vec{\tau}\}
\end{array}
$$

Here kind schemas (*kscm*) classify kind terms while kinds classify type terms. There are variables at all three levels: kind-schema variables z, kind variables k, and type variables t. We have an external constant Kscm classifying all the kind schemas; essentially, TL has an additional level above *kscm*, of which Kscm is the sole member.

A good way to comprehend TL is to look at its five Π constructs: there are three at the kind level and two at the kind-schema level. We use a few examples to explain why each of them is necessary. Following the tradition, we use arrow terms (*e.g.*, $\kappa_1 \to \kappa_2$) as a syntactic sugar for the non-dependent Π terms (*e.g.,* $\Pi t\!:\!\kappa_1.\, \kappa_2$ is non-dependent if t does not occur free in κ_2).

- Kinds $\Pi t : \kappa_1.\, \kappa_2$ and $\kappa_1 \to \kappa_2$ are used to typecheck the type-level function $\lambda t : \kappa.\, \tau$ and its application form $\tau_1\, \tau_2$. Assuming Ω and Nat are inductive kinds (defined later) and Prime is a predicate with kind schema $\mathsf{Nat} \to \mathsf{Kind}$, we can write a type term such as $\lambda t : \Omega.\, t$ which has kind $\Omega \to \Omega$, a type-level arithmetic function such as plus which has kind $\mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Nat}$, or the universally quantified proposition in Section 2.2 which is represented as a kind $\Pi t\!:\!\mathsf{Nat}.\mathsf{Prime}(t) \to \mathsf{Prime}(g(t))$.

- Kinds $\Pi k : u.\, \kappa$ and $u \to \kappa$ are used to typecheck the type-level kind abstraction $\lambda k\!:\!u.\, \tau$ and its application form $\tau[\kappa]$. As mentioned in Section 2.5, this is needed to support intensional analysis of quantified types [39]. It can also be used to define logic connectives and constants, *e.g.*

$$
\begin{array}{rcl}
\mathsf{True} : \mathsf{Kind} & = & \Pi k\!:\!\mathsf{Kind}.\, k \to k \\
\mathsf{False} : \mathsf{Kind} & = & \Pi k\!:\!\mathsf{Kind}.\, k
\end{array}
$$

  True has the polymorphic identity as a proof:

$$
\mathsf{id} : \mathsf{True} \quad = \quad \lambda k\!:\!\mathsf{Kind}.\, \lambda t\!:\!k.\, t
$$

  but False is not inhabited (this is essentially the consistency property of TL which we will show later).

- Kind $\Pi z\!:\!\mathsf{Kscm}.\, \kappa$ is used to typecheck the type-level kind-schema abstraction $\lambda z : \mathsf{Kscm}.\, \tau$ and its application form $\tau[u]$. This is not in the core calculus of constructions [11]. We use it in the inductive definition of Ω (see Section 4) where both the $\forall_{\mathsf{Kscm}}$ and $\exists_{\mathsf{Kscm}}$ constructors have kind $\Pi z\!:\!\mathsf{Kscm}.\, (z \to \Omega) \to \Omega$. These two constructors in turn allow us to typecheck predicate-polymorphic computation terms, which occur fairly often since the closure-conversion phase turns all functions with free predicate variables (e.g, Prime) into predicate-polymorphic ones.

- Kind schemas $\Pi t\!:\!\kappa.\, u$ and $\kappa \to u$ are used to typecheck the kind-level type abstraction $\lambda t\!:\!\kappa_1.\, \kappa_2$ and its application form $\kappa[\tau]$. The predicate Prime has kind schema $\mathsf{Nat} \to \mathsf{Kind}$. A predicate with kind schema $\Pi t : \mathsf{Nat}.\, \mathsf{Prime}(t) \to \mathsf{Kind}$ is only applicable to prime numbers. We can also define *e.g.* a binary relation:

$$
\mathsf{LT} \quad : \quad \mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Kind}
$$

  so that $\mathsf{LT}\ t_1\ t_2$ is a proposition asserting that the natural number represented by t_1 is less than that of t_2.

$$
\begin{array}{l}
\mathsf{Inductive\ Bool} : \mathsf{Kind} := \mathsf{true} : \mathsf{Bool} \\
\qquad\qquad\qquad\qquad\qquad\quad \mid \mathsf{false} : \mathsf{Bool} \\
\\
\mathsf{Inductive\ Nat} : \mathsf{Kind} := \mathsf{zero} : \mathsf{Nat} \\
\qquad\qquad\qquad\qquad\qquad\quad \mid \mathsf{succ} : \mathsf{Nat} \to \mathsf{Nat} \\
\\
\mathsf{plus} : \mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Nat} \\
\mathsf{plus}(\mathsf{zero}) \quad = \quad \lambda t\!:\!\mathsf{Nat}.\, t \\
\mathsf{plus}(\mathsf{succ}\ t) \quad = \quad \lambda t'\!:\!\mathsf{Nat}.\, \mathsf{succ}\ ((\mathsf{plus}\ t)\ t') \\
\\
\mathsf{ifez} : \mathsf{Nat} \to (\Pi k\!:\!\mathsf{Kind}.\, k \to (\mathsf{Nat} \to k) \to k) \\
\mathsf{ifez}(\mathsf{zero}) \quad = \quad \lambda k\!:\!\mathsf{Kind}.\, \lambda t_1\!:\!k.\, \lambda t_2\!:\!\mathsf{Nat} \to k.\, t_1 \\
\mathsf{ifez}(\mathsf{succ}\ t) \quad = \quad \lambda k\!:\!\mathsf{Kind}.\, \lambda t_1\!:\!k.\, \lambda t_2\!:\!\mathsf{Nat} \to k.\, t_2\ t \\
\\
\mathsf{le} : \mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Bool} \\
\mathsf{le}(\mathsf{zero}) \quad = \quad \lambda t\!:\!\mathsf{Nat}.\, \mathsf{true} \\
\mathsf{le}(\mathsf{succ}\ t) \quad = \quad \lambda t'\!:\!\mathsf{Nat}.\, \mathsf{ifez}\ t'\ \mathsf{Bool}\ \mathsf{false}\ (\mathsf{le}\ t) \\
\\
\mathsf{lt} : \mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Bool} \\
\mathsf{lt} \quad = \quad \lambda t\!:\!\mathsf{Nat}.\, \mathsf{le}\ (\mathsf{succ}\ t) \\
\\
\mathsf{Cond} : \mathsf{Bool} \to \mathsf{Kind} \to \mathsf{Kind} \to \mathsf{Kind} \\
\mathsf{Cond}(\mathsf{true}) \quad = \quad \lambda k_1\!:\!\mathsf{Kind}.\, \lambda k_2\!:\!\mathsf{Kind}.\, k_1 \\
\mathsf{Cond}(\mathsf{false}) \quad = \quad \lambda k_1\!:\!\mathsf{Kind}.\, \lambda k_2\!:\!\mathsf{Kind}.\, k_2
\end{array}
$$

Figure 2: Examples of inductive definitions

- Kind schemas $\Pi k : u_1.\, u_2$ and $u_1 \to u_2$ are used to typecheck the kind-level function $\lambda k : u.\, \kappa$ and its application form $\kappa_1\, \kappa_2$. We use it to write higher-order predicates and logic connectives. For example, the logical negation operator can be written as follows:

$$
\mathsf{Not} \ : \ \mathsf{Kind} \to \mathsf{Kind} \quad = \quad \lambda k\!:\!\mathsf{Kind}.\, (k \to \mathsf{False})
$$

  The consistency of TL implies that a proposition and its negation cannot be both inhabited—otherwise applying the proof of the second to that of the first would yield a proof of False.

TL also provides a general mechanism of inductive definitions [35]. The term $\mathsf{Ind}(k : \mathsf{Kind})\{\vec{\kappa}\}$ introduces an inductive kind k containing a list of constructors whose kinds are specified by $\vec{\kappa}$. Here k must only occur "positively" inside each κ_i (see Appendix D for the formal definition of positivity). The term $\mathsf{Ctor}\,(i, \kappa)$ refers to the i-th constructor in an inductive kind κ. For presentation, we will use a more friendly syntax in the rest of this paper. An inductive kind $I = \mathsf{Ind}(k\!:\!\mathsf{Kind})\{\vec{\kappa}\}$ will be written as:

$$
\begin{array}{rl}
\mathsf{Inductive}\ I\ :\ \mathsf{Kind} := & \mathsf{c}_1 : [I/k]\kappa_1 \\
& \mid \mathsf{c}_2 : [I/k]\kappa_2 \\
& \vdots \\
& \mid \mathsf{c}_n : [I/k]\kappa_n
\end{array}
$$

We give an explicit name c_i to each constructor, so c_i is just an abbreviation of $\mathsf{Ctor}\,(i, I)$. For simplicity, the current version of TL does not include parameterized inductive kinds, but supporting them is quite straightforward [41, 35].

TL provides two iterators to support primitive recursion on inductive kinds. The small elimination $\mathsf{Elim}[\kappa', \kappa](\tau')\{\vec{\tau}\}$ takes a type term τ' of inductive kind κ', performs the iterative operation specified by $\vec{\tau}$ (which contains a branch for each constructor of κ'), and returns a type term of kind $\kappa[\tau']$ as the result. The large elimination $\mathsf{Elim}[\kappa', u](\tau)\{\vec{\kappa}\}$ takes a type term τ of inductive kind κ', performs the iterative operation specified by $\vec{\kappa}$, and returns a kind

$$
\begin{array}{lll}
(\textit{sort}) & s & ::= \mathsf{Kind} \mid \mathsf{Kscm} \mid \mathsf{Ext} \\
(\textit{var}) & X & ::= z \mid k \mid t \\
(\textit{ptm}) & A, B & ::= s \mid X \mid \lambda X\!:\!A.\, B \mid A\ B \mid \Pi X\!:\!A.\, B \\
 & & \quad \mid \mathsf{Ind}(X\!:\!\mathsf{Kind})\{\vec{A}\} \mid \mathsf{Ctor}\,(i, A) \\
 & & \quad \mid \mathsf{Elim}[A', B'](A)\{\vec{B}\}
\end{array}
$$

Figure 3: Syntax of the type language TL

term of kind schema u as the result. These iterators generalize the Typerec operator used in intensional type analysis [22, 14, 39].

Figure 2 gives a few examples of inductive definitions including the inductive kinds Bool and Nat and several type-level functions which we will use in Section 4. The small elimination for Nat takes the following form $\mathsf{Elim}[\mathsf{Nat}, \kappa](\tau')\{\tau_1; \tau_2\}$. Here, κ is a dependent kind with kind schema $\mathsf{Nat} \to \mathsf{Kind}$; τ' is the argument which has kind Nat. The term in the zero branch, τ_1, has kind $\kappa[\tau']$. The term in the succ branch, τ_2, has kind $\mathsf{Nat} \to \kappa[\tau'] \to \kappa[\tau']$. TL uses the ι-reduction to perform the iterator operation. For example, the two ι-reduction rules for Nat work as follows:

$$
\begin{array}{l}
\mathsf{Elim}[\mathsf{Nat}, \kappa](\mathsf{zero})\{\tau_1; \tau_2\} \leadsto_\iota \tau_1 \\
\mathsf{Elim}[\mathsf{Nat}, \kappa](\mathsf{succ}\ \tau)\{\tau_1; \tau_2\} \leadsto_\iota \tau_2\ \tau\ (\mathsf{Elim}[\mathsf{Nat}, \kappa](\tau)\{\tau_1; \tau_2\})
\end{array}
$$

The general ι-reduction rule is defined formally in Appendix D. In our examples, we take the liberty of using the pattern-matching syntax (as in ML) to express the iterator operations, but they can be easily converted back to the Elim form.

In Figure 2, plus is a function which calculates the sum of two natural numbers. The function ifez behaves like a switch statement: if its argument is zero, it returns a function that selects the first branch; otherwise, the result takes the second branch and applies it to the predecessor of the argument. The function le evaluates to true if its first argument is less than or equal to the second. The function lt performs the less-than comparison.

The definition of function Cond, which implements a conditional with result at the kind level, uses large elimination on Bool. It has the form $\mathsf{Elim}[\mathsf{Bool}, u](\tau)\{\kappa_1; \kappa_2\}$, where τ is of kind Bool; both the true and false branches (κ_1 and κ_2) have kind schema u.

Formalization We want to give a formal semantics to TL and then reason about its meta-theoretical properties. But the five Π constructs have many redundancies, so in the rest of this paper, we will model TL as a pure type system (PTS) [4] extended with inductive definitions. Intuitively, instead of having a separate syntactical category for each level, we collapse all kind schemas u, kind terms κ, type terms τ, and the external constant Kscm into a single set of *pseudoterms* (*ptm*), denoted as A or B. Similar constructs can now share typing rules and reduction relations.

Figure 3 gives the syntax of TL, written in PTS style. There is now only one Π construct ($\Pi X : A.\, B$), one λ-abstraction ($\lambda X : A.\, B$), and one application form ($A\ B$); two iterators for inductive definitions are also merged into one ($\mathsf{Elim}[A', B'](A)\{\vec{B}\}$). We use X and Y to represent generic variables, but we will still use t, k, and z if the class of a variable is clear from the context.

TL has the following PTS specification which we will use to derive its typing rules:

$$
\begin{array}{lcl}
\mathcal{S} & = & \mathsf{Kind}, \mathsf{Kscm}, \mathsf{Ext} \\
\mathcal{A} & = & \mathsf{Kind}\!:\!\mathsf{Kscm}, \mathsf{Kscm}\!:\!\mathsf{Ext} \\
\mathcal{R} & = & (\mathsf{Kind}, \mathsf{Kind}), (\mathsf{Kscm}, \mathsf{Kind}), (\mathsf{Ext}, \mathsf{Kind}) \\
 & & (\mathsf{Kind}, \mathsf{Kscm}), (\mathsf{Kscm}, \mathsf{Kscm})
\end{array}
$$

Here $\mathcal{S}$ contains the set of sorts used to denote universes. We have to add the constant Ext to support quantification over Kscm. Our names for the sorts reflect the fact we lifted everything one level up; they are related to other systems via the following table:

Systems	Notations		
TL	Kind	Kscm	Ext
Werner [41]	Set	Type	Ext
Coq/CIC [25]	Set,Prop	Type(0)	Type(1)
Barendregt [4]	$*$	$\Box$	$\triangle$

The axioms in the set $\mathcal{A}$ denote the relationship between different sorts; an axiom "$s_1 : s_2$" means that s_2 classifies s_1. The rules in the set $\mathcal{R}$ are used to define well-formed Π constructs, from which we can deduce the set of well-formed λ-definitions and applications. For example, the five rules for TL can be related to the five Π constructs through the following table:

PTS rules\ptm	$\Pi X\!:\!A.\, B$	$\lambda X\!:\!A.\, B$	$A\ B$
(Kind, Kind)	$\Pi t\!:\!\kappa_1.\, \kappa_2$	$\lambda t\!:\!\kappa.\, \tau$	$\tau_1\ \tau_2$
(Kscm, Kind)	$\Pi k\!:\!u.\, \kappa$	$\lambda k\!:\!u.\, \tau$	$\tau[\kappa]$
(Ext, Kind)	$\Pi z\!:\!\mathsf{Kscm}.\, \kappa$	$\lambda z\!:\!\mathsf{Kscm}.\, \tau$	$\tau[u]$
(Kind, Kscm)	$\Pi t\!:\!\kappa.\, u$	$\lambda t\!:\!\kappa_1.\, \kappa_2$	$\kappa[\tau]$
(Kscm, Kscm)	$\Pi k\!:\!u_1.\, u_2$	$\lambda k\!:\!u.\, \kappa$	$\kappa\ \kappa'$

We define a context Δ as a list of bindings from variables to pseudoterms:

$$(\textit{ctxt}) \quad \Delta ::= \cdot \mid \Delta, X : A$$

The typing judgment for the PTS-style TL now takes the form $\Delta \vdash A : A'$ meaning that within context Δ, the pseudoterm A is well-formed and has A' as its classifier. We can now write a single typing rule for all the Π constructs:

$$\frac{\Delta \vdash A : s_1 \quad \Delta, X : A \vdash B : s_2 \quad (s_1, s_2) \in \mathcal{R}}{\Delta \vdash \Pi X\!:\!A.\, B : s_2} \qquad (\textsc{prod})$$

Take the rule (Kind, Kscm) as an example. To build a well-formed term $\Pi X : A.\, B$, which will be a kind schema (because s_2 is Kscm), we need to show that A is a well-formed kind and B is a well-formed kind schema assuming X has kind A. We can also share the typing rules for all the λ-definitions and applications:

$$\frac{\Delta, X : A \vdash B : B' \qquad \Delta \vdash \Pi X\!:\!A.\, B' : s}{\Delta \vdash \lambda X\!:\!A.\, B : \Pi X\!:\!A.\, B'} \qquad (\textsc{fun})$$

$$\frac{\Delta \vdash A : \Pi X\!:\!B'.\, A' \quad \Delta \vdash B : B'}{\Delta \vdash A\ B : [B/X]A'} \qquad (\textsc{app})$$

The reduction relations can also be shared. TL supports the standard β- and η-reductions (denoted as $\leadsto_\beta$ and $\leadsto_\eta$) plus the previously mentioned ι-reduction (denoted as $\leadsto_\iota$) on inductive objects (see Appendix D). We use $\rhd_\beta$, $\rhd_\eta$, and $\rhd_\iota$ to denote the relations that correspond to the rewriting of subterms using the relations $\leadsto_\beta$, $\leadsto_\eta$, and $\leadsto_\iota$ respectively. We use $\leadsto$ and $\rhd$ for the unions of the above relations. We also write $=_{\beta\eta\iota}$ for the reflexive-symmetric-transitive closure of $\rhd$.

The complete typing rules for TL and the definitions of all the reduction relations are given in Appendix D. Following Werner [41] and Geuvers [17], we have shown that TL satisfies all the key meta-theoretic properties including subject reduction, strong normalization, Church-Rosser (and confluence), and consistency of the underlying logic. The detailed proofs for these properties are given in Appendix D.

4 The Computation Language λ_H

The language of computations λ_H for our high-level certified intermediate format uses proofs, constructed in the type language, to

$$
\begin{array}{lll}
(\textit{exp}) & e & ::= x \mid \overline{n} \mid \mathsf{tt} \mid \mathsf{ff} \mid f \mid \mathsf{fix}\, x\!:\!A.\, f \mid e\ e' \mid e[A] \\
& & \quad \mid \langle X = A,\ e\!:\!A' \rangle \mid \mathsf{open}\ e\ \mathsf{as}\ \langle X,\ x \rangle\ \mathsf{in}\ e' \\
& & \quad \mid \langle e_0,\ \ldots\ e_{n-1} \rangle \mid \mathsf{sel}[A](e, e') \mid e\ \mathit{aop}\ e' \\
& & \quad \mid e\ \mathit{cop}\ e' \mid \mathsf{if}[A, A'](e,\ X_1.\, e_1,\ X_2.\, e_2) \\
& & \quad \text{where } n \in \mathbb{N} \\
(\textit{fun}) & f & ::= \lambda x\!:\!A.\, e \mid \Lambda X\!:\!A.\, f \\
(\textit{arith}) & \mathit{aop} & ::= \mathsf{+} \mid \ldots \\
(\textit{cmp}) & \mathit{cop} & ::= \mathsf{<} \mid \ldots
\end{array}
$$

Figure 4: Syntax of the computation language λ_H.

verify propositions which ensure the runtime safety of the program. Furthermore, in comparison with other higher-order typed calculi, the types assigned to programs can be more refined, since program invariants expressible in higher-order predicate logic can be represented in our type language. These more precise types serve as more complete specifications of the behavior of program components, and thus allow the static verification of more programs.

One approach to presenting a language of computations is to encode its syntax and semantics in a proof system, with the benefit of obtaining machine-checkable proofs of its properties, *e.g.* type safety. This appears to be even more promising for a system with a type language like CIC, which is more expressive than higher-order predicate logic: The CIC proofs of some program properties, embedded as type terms in the program, may not be easily representable in meta-logical terms, thus it may be simpler to perform all the reasoning in CIC. However our exposition of the language TL is focused on its use as a type language, and consequently it does not include all features of CIC. We therefore leave this possibility for future work, and give a standard meta-logical presentation instead; we address some of the issues related to adequacy in our discussion of type safety.

In this section we often use the unqualified "term" to refer to a computation term (expression) e, with syntax defined in Figure 4. Most of the constructs are borrowed from standard higher-order typed calculi. To simplify the exposition we only consider constants representing natural numbers ($\overline{n}$ is the value representing $n \in \mathbb{N}$) and boolean values (tt and ff). The term-level abstraction and application are standard; type abstractions and fixed points are restricted to function values, with the call-by-value semantics in mind and to simplify the CPS and closure conversions. The type variable bound by a type abstraction, as well as the one bound by the open construct for packages of existential type, can have either a kind or a kind schema. Dually, the type argument in a type application, and the witness type term A in the package construction $\langle X = A,\ e\!:\!A' \rangle$ can be either a type term or a kind term.

The constructs implementing tuple operations, arithmetic, and comparisons have nonstandard static semantics, on which we focus in section 4.1, but their runtime behavior is standard. The branching construct is parameterized at the type level with a proposition (which is dependent on the value of the test term) and its proof; the proof is passed to the executed branch.

Dynamic semantics We present a small step call-by-value operational semantics for λ_H in the style of Wright and Felleisen [42]. The values are defined as

$$v ::= \overline{n} \mid \mathsf{tt} \mid \mathsf{ff} \mid f \mid \mathsf{fix}\, x\!:\!A.\, f \mid \langle X = A,\ v\!:\!A' \rangle \mid \langle v_0,\ \ldots\ v_{n-1} \rangle$$

The reduction relation $\hookrightarrow$ is specified by the rules

$$(\lambda x\!:\!A.\, e)\ v \ \hookrightarrow\ [v/x]e \qquad \text{(R-}\beta\text{)}$$

$$(\Lambda X\!:\!B.\, f)[A] \ \hookrightarrow\ [A/X]f \qquad \text{(R-TY-}\beta\text{)}$$

$$\mathsf{sel}[A](\langle v_0,\ \ldots\ v_{n-1} \rangle, \overline{m}) \ \hookrightarrow\ v_m \qquad (m < n) \qquad \text{(R-SEL)}$$

$$\mathsf{open}\ \langle X' = A,\ v\!:\!A' \rangle\ \mathsf{as}\ \langle X,\ x \rangle\ \mathsf{in}\ e \ \hookrightarrow\ [v/x][A/X]e \qquad \text{(R-OPEN)}$$

$$(\mathsf{fix}\, x\!:\!A.\, f)\ v \ \hookrightarrow\ ([\mathsf{fix}\, x\!:\!A.\, f/x]f)\ v \qquad \text{(R-FIX)}$$

$$(\mathsf{fix}\, x\!:\!A.\, f)[A'] \ \hookrightarrow\ ([\mathsf{fix}\, x\!:\!A.\, f/x]f)[A'] \qquad \text{(R-TYFIX)}$$

$$\overline{m} \mathsf{+} \overline{n} \ \hookrightarrow\ \overline{m+n} \qquad \text{(R-ADD)}$$

$$\overline{m} \mathsf{<} \overline{n} \ \hookrightarrow\ \mathsf{tt} \qquad (m < n) \qquad \text{(R-LT-T)}$$

$$\overline{m} \mathsf{<} \overline{n} \ \hookrightarrow\ \mathsf{ff} \qquad (m \geq n) \qquad \text{(R-LT-F)}$$

$$\mathsf{if}[B, A](\mathsf{tt},\ X_1.\, e_1,\ X_2.\, e_2) \ \hookrightarrow\ [A/X_1]e_1 \qquad \text{(R-IF-T)}$$

$$\mathsf{if}[B, A](\mathsf{ff},\ X_1.\, e_1,\ X_2.\, e_2) \ \hookrightarrow\ [A/X_2]e_2 \qquad \text{(R-IF-F)}$$

An evaluation context E encodes the call-by-value discipline:

$$
\begin{array}{l}
E ::= \bullet \mid E\ e \mid v\ E \mid E[A] \mid \langle X = A,\ E\!:\!A' \rangle \\
\quad \mid \mathsf{open}\ E\ \mathsf{as}\ \langle X,\ x \rangle\ \mathsf{in}\ e \mid \mathsf{open}\ v\ \mathsf{as}\ \langle X,\ x \rangle\ \mathsf{in}\ E \\
\quad \mid \langle v_0,\ \ldots v_i,\ E,\ e_{i+2},\ \ldots,\ e_{n-1} \rangle \mid \mathsf{sel}[A](E, e) \\
\quad \mid \mathsf{sel}[A](v, E) \mid E\ \mathit{aop}\ e \mid v\ \mathit{aop}\ E \mid E\ \mathit{cop}\ e \\
\quad \mid v\ \mathit{cop}\ E \mid \mathsf{if}[A, A'](E,\ X_1.\, e_1,\ X_2.\, e_2)
\end{array}
$$

The notation $E\{e\}$ stands for the term obtained by replacing the hole $\bullet$ in E by e. The single step computation $\mapsto$ relates $E\{e\}$ to $E\{e'\}$ when $e \hookrightarrow e'$, and $\mapsto^*$ is its reflexive transitive closure.

As shown the semantics is standard except for some additional passing of type terms in R-SEL and R-IF-T/F. However an inspection of the rules shows that types are irrelevant for the evaluation, hence a type-erasure semantics, in which all type-related operations and parameters are erased, would be entirely standard.

4.1 Static semantics

The static semantics of λ_H shows the benefits of using a type language as expressive as TL. We can now define the type constructors of λ_H as constructors of an inductive kind Ω, instead of having them built into λ_H. As we will show in Section 5, this property is crucial for the conversion to CPS, since it makes possible transforming direct-style types to CPS types within the type language.

$$
\begin{array}{rl}
\mathsf{Inductive}\ \Omega\ :\ \mathsf{Kind}\ := & \mathsf{snat}\ : \mathsf{Nat} \to \Omega \\
& \mid \mathsf{sbool}\ : \mathsf{Bool} \to \Omega \\
& \mid \twoheadrightarrow\ : \Omega \to \Omega \to \Omega \\
& \mid \mathsf{tup}\ : \mathsf{Nat} \to (\mathsf{Nat} \to \Omega) \to \Omega \\
& \mid \forall_{\mathsf{Kind}}\ : \Pi k\!:\!\mathsf{Kind}.\, (k \to \Omega) \to \Omega \\
& \mid \exists_{\mathsf{Kind}}\ : \Pi k\!:\!\mathsf{Kind}.\, (k \to \Omega) \to \Omega \\
& \mid \forall_{\mathsf{Kscm}}\ : \Pi z\!:\!\mathsf{Kscm}.\, (z \to \Omega) \to \Omega \\
& \mid \exists_{\mathsf{Kscm}}\ : \Pi z\!:\!\mathsf{Kscm}.\, (z \to \Omega) \to \Omega
\end{array}
$$

Informally, all well-formed computations have types of kind Ω, including singleton types of natural numbers $\mathsf{snat}\ A$ and boolean values $\mathsf{sbool}\ B$, as well as function, tuple, polymorphic and existential types. To improve readability we also define the syntactic sugar

$$
\left.
\begin{array}{l}
A \to B \equiv \twoheadrightarrow\ A\ B \\
\forall_s X\!:\!A.\, B \equiv \forall_s\ A\ (\lambda X\!:\!A.\, B) \\
\exists_s X\!:\!A.\, B \equiv \exists_s\ A\ (\lambda X\!:\!A.\, B)
\end{array}
\right\} \text{where } s \in \{\mathsf{Kind}, \mathsf{Kscm}\}
$$

and often drop the sort s when $s = \mathsf{Kind}$; *e.g.* the type void, containing no values, is defined as $\forall t\!:\!\Omega.\, t \equiv \forall_{\mathsf{Kind}}\ \Omega\ (\lambda t\!:\!\Omega.\, t)$.

Using this syntactic sugar we can give a familiar look to many of the formation rules for λ_H expressions and functional values. Figure 5 contains the inference rules for deriving judgments of the

form $\Delta;\ \Gamma \vdash\ e : A$, which assign type A to the expression e in a context Δ and a type environment Γ defined by

$$(\textit{type env}) \quad \Gamma ::= \cdot \mid \Gamma, x{:}A$$

We introduce some of the notation used in these rules in the course of the discussion.

Rules E-NAT, E-TRUE, and E-FALSE assign singleton types to numeric and boolean constants. For instance the constant $\overline{1}$ has type $\mathsf{succ\ zero}$ in any valid environment. In rule E-NAT we use the meta-function $\widehat{\cdot}$ to map natural numbers $n \in \mathbb{N}$ to their representations as type terms. It is defined inductively by $\widehat{0} = \mathsf{zero}$ and $\widehat{n+1} = \mathsf{succ}\ \widehat{n}$, so $\Delta \vdash \widehat{n} : \mathsf{Nat}$ holds for all valid Δ and $n \in \mathbb{N}$.

Singleton types play a central role in reflecting properties of values in the type language, where we can reason about them constructively. For instance rules E-ADD and E-LT use respectively the type terms plus and lt (defined in Section 3) to reflect the semantics of the term operations into the type level via singleton types.

However, if we could only assign singleton types to computation terms, in a decidable type system we would only be able to typecheck terminating programs. We regain expressiveness of the computation language using existential types to hide some of the too detailed type information. Thus for example one can define the usual types of all natural numbers and boolean values as

$$\begin{aligned}\mathsf{nat} &: \Omega = \exists t{:}\mathsf{Nat}.\ \mathsf{snat}\ t\\ \mathsf{bool} &: \Omega = \exists t{:}\mathsf{Bool}.\ \mathsf{sbool}\ t\end{aligned}$$

For any term e with singleton type $\mathsf{snat}\ A$ the package $\langle t = A,\ e : \mathsf{snat}\ t\rangle$ has type nat. Since in a type-erasure semantics of λ_H all types and operations on them are erased, there is no runtime overhead for the packaging. For each $n \in \mathbb{N}$ there is a value of this type denoted by $\widehat{\overline{n}} \equiv \langle t = \widehat{n},\ \overline{n} : \mathsf{snat}\ t\rangle$. Operations on terms of type nat are derived from operations on terms of singleton types of the form $\mathsf{snat}\ A$; for example an addition function of type $\mathsf{nat} \to \mathsf{nat} \to \mathsf{nat}$ is defined as the expression

$$\begin{aligned}&\mathsf{add} = \lambda \mathsf{x}_1{:}\mathsf{nat}.\ \lambda \mathsf{x}_2{:}\mathsf{nat}.\\ &\qquad \mathsf{open}\ \mathsf{x}_1\ \mathsf{as}\ \langle t_1,\ \mathsf{x}_1'\rangle\ \mathsf{in}\ \mathsf{open}\ \mathsf{x}_2\ \mathsf{as}\ \langle t_2,\ \mathsf{x}_2'\rangle\ \mathsf{in}\\ &\qquad\quad \langle t = \mathsf{plus}\ t_1\ t_2,\ \mathsf{x}_1' + \mathsf{x}_2' : \mathsf{snat}\ t\rangle\end{aligned}$$

Rule E-TUP assigns to a tuple a type of the form $\mathsf{tup}\ A\ B$, in which the tup constructor is applied to a type A representing the tuple size, and a function B mapping offsets to the types of the tuple components. This function is defined in terms of operations on lists of types:

$$\begin{aligned}&\mathsf{Inductive\ List} : \mathsf{Kind} := \mathsf{nil} \quad : \mathsf{List}\\ &\qquad\qquad\qquad\qquad\quad \mid \mathsf{cons} : \Omega \to \mathsf{List} \to \mathsf{List}\\ &\\ &\mathsf{nth} : \mathsf{List} \to \mathsf{Nat} \to \Omega\\ &\mathsf{nth\ nil} \qquad\quad = \lambda t{:}\mathsf{Nat}.\ \mathsf{void}\\ &\mathsf{nth}\ (\mathsf{cons}\ t_1\ t_2) = \lambda t{:}\mathsf{Nat}.\ \mathsf{ifez}\ t\ \Omega\ t_1\ (\mathsf{nth}\ t_2)\end{aligned}$$

Thus $\mathsf{nth\ L}\ \widehat{n}$ reduces to the n-th element of the list L when n is less than the length of L, and to void otherwise. We also use the infix form $A{::}A' \equiv \mathsf{cons}\ A\ A'$. The type of pairs is derived: $A \times A' \equiv \mathsf{tup}\ \widehat{2}\ (\mathsf{nth}\ (A{::}A'{::}\mathsf{nil}))$. Thus for instance $\cdot;\cdot \vdash\ \langle\overline{42}, \overline{7}\rangle : \mathsf{snat}\ \widehat{42} \times \mathsf{snat}\ \widehat{7}$ is a valid judgment.

The rules for selection and testing for the less-than relation (the only comparison we discuss for brevity) refer to the kind term LT with kind schema $\mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Kind}$. Intuitively, LT represents a binary relation on kind Nat, so $\mathsf{LT}\ \widehat{m}\ \widehat{n}$ is the kind of type terms representing proofs of $m < n$. LT can be thought of as the parameterized inductive kind of proofs constructed from instances of the axioms $\forall n \in \mathbb{N}.\ 0 < n{+}1$ and $\forall m, n \in \mathbb{N}.\ m < n \supset m{+}1 < n{+}1$:

$$\begin{aligned}&\mathsf{Inductive\ LT} : \mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Kind}\\ &\quad := \mathsf{ltzs} : \Pi t{:}\mathsf{Nat}.\ \mathsf{LT\ zero}\ (\mathsf{succ}\ t)\\ &\qquad \mid \mathsf{ltss} : \Pi t{:}\mathsf{Nat}.\ \Pi t'{:}\mathsf{Nat}.\ \mathsf{LT}\ t\ t' \to \mathsf{LT}\ (\mathsf{succ}\ t)\ (\mathsf{succ}\ t')\end{aligned}$$

To simplify the presentation of our type language, we allowed inductive kinds of kind scheme Kind only. Thus to stay within the scope of this paper we actually use a Church encoding of LT (defined later); this is sufficient since proof objects are never analyzed in λ_H, so the full power of elimination is not necessary for LT.

In the component selection construct $\mathsf{sel}[A](e, e')$ the type A represents a *proof* that the value of the subscript e' is less than the size of the tuple e. In rule E-SEL this condition is expressed as an application of the type term LT. Due to the consistency of the logic represented in the type language, only the existence and not the structure of the proof object A is important. Since its existence is ensured statically in a well-formed expression, A would be eliminated in a type-erasure semantics.

The branching construct $\mathsf{if}[B, A](e,\ X_1.\ e_1,\ X_2.\ e_2)$ takes a type term A representing a proof of the proposition encoded as either B true or B false, depending on the value of e. The proof is passed to the appropriate branch in its bound type variable (X_1 or X_2). The correspondence between the value of e and the kind of A is again established through a singleton type. Note that unlike Xi and Harper [43] we allow imprecise information flow into the branches by not restricting B false to be the negation of B true. In particular this makes possible the encoding of the usual oblivious (in proof-passing sense) if using $B = \lambda t{:}\mathsf{Bool}.\ \mathsf{True}$.

4.2 Example: bound check elimination

A simple example of the generation, propagation, and use of proofs in λ_H is a function which computes the sum of the components of any vector of naturals. Let us first introduce some auxiliary types and functions. The type assigned to a homogeneous tuple (vector) of n terms of type A is $\beta\eta\iota$-convertible to the form $\mathsf{vec}\ \widehat{n}\ A$ for

$$\begin{aligned}&\mathsf{vec} : \mathsf{Nat} \to \Omega \to \Omega\\ &\mathsf{vec} = \lambda t{:}\mathsf{Nat}.\ \lambda t'{:}\Omega.\ \mathsf{tup}\ t\ (\mathsf{nth}\ (\mathsf{repeat}\ t\ t'))\end{aligned}$$

where

$$\begin{aligned}&\mathsf{repeat} : \mathsf{Nat} \to \Omega \to \mathsf{List}\\ &\mathsf{repeat\ zero} \quad = \lambda t'{:}\Omega.\ \mathsf{nil}\\ &\mathsf{repeat}\ (\mathsf{succ}\ t) = \lambda t'{:}\Omega.\ t'{::}(\mathsf{repeat}\ t)\ t'\end{aligned}$$

Then we can define a term which sums the elements of a vector with a given length as follows:

$$\begin{aligned}&\mathsf{sumVec} : \forall t{:}\mathsf{Nat}.\ \mathsf{snat}\ t \to \mathsf{vec}\ t\ \mathsf{nat} \to \mathsf{nat}\\ &\qquad \equiv \Lambda t{:}\mathsf{Nat}.\ \lambda \mathsf{n}{:}\mathsf{snat}\ t.\ \lambda \mathsf{v}{:}\mathsf{vec}\ t\ \mathsf{nat}.\\ &\qquad\quad (\mathsf{fix\ loop} : \mathsf{nat} \to \mathsf{nat} \to \mathsf{nat}.\\ &\qquad\qquad \lambda \mathsf{i}{:}\mathsf{nat}.\ \lambda \mathsf{sum}{:}\mathsf{nat}.\\ &\qquad\qquad\quad \mathsf{open\ i\ as}\ \langle t',\ \mathsf{i}'\rangle\ \mathsf{in}\\ &\qquad\qquad\quad\ \mathsf{if}[\mathsf{LTOrTrue}\ t'\ t, \mathsf{ltPrf}\ t'\ t]\\ &\qquad\qquad\quad\quad (\mathsf{i}' < \mathsf{n},\\ &\qquad\qquad\quad\qquad t_1.\ \mathsf{loop}\ (\mathsf{add\ i}\ \widehat{\overline{1}})\\ &\qquad\qquad\quad\qquad\qquad (\mathsf{add\ sum}\ (\mathsf{sel}[t_1](\mathsf{v}, \mathsf{i}'))),\\ &\qquad\qquad\quad\qquad t_2\,.\,\mathsf{sum})\ \widehat{\overline{0}}\ \widehat{\overline{0}}\end{aligned}$$

where

$$\begin{aligned}&\mathsf{LTOrTrue} : \mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Bool} \to \mathsf{Kind}\\ &\mathsf{LTOrTrue} = \lambda t_1{:}\mathsf{Nat}.\ \lambda t_2{:}\mathsf{Nat}.\ \lambda t{:}\mathsf{Bool}.\ \mathsf{Cond}\ t\ (\mathsf{LT}\ t_1\ t_2)\ \mathsf{True}\end{aligned}$$

and ltPrf of kind $\Pi t' : \mathsf{Nat}.\ \Pi t : \mathsf{Nat}.\ \mathsf{LTOrTrue}\ t'\ t\ (\mathsf{lt}\ t'\ t)$ is a type term defined later.

The comparison $\mathsf{i}' < \mathsf{n}$, used in this example as a loop termination test, checks whether the index i' is smaller than the vector size n. If it is, the adequacy of the type term lt with respect to the less-than relation ensures that the type term $\mathsf{ltPrf}\ t'\ t$ represents a proof of the corresponding proposition at the type level, namely $\mathsf{LT}\ t'\ t$. This proof is then bound to t_1 in the first branch of the if, and the sel construct uses it to verify that the i'-th element of v exists, thus avoiding a second test. The type safety of λ_H (Theorem 1) guaran-

$$\frac{\Delta \vdash \mathsf{Kind} : \mathsf{Kscm}}{\Delta \vdash \cdot \ ok} \quad \text{(TE-MT)} \qquad \frac{\Delta \vdash \Gamma \ ok}{\Delta; \Gamma \vdash x : \Gamma(x)} \quad \text{(E-VAR)} \qquad \frac{\Delta \vdash \Gamma \ ok}{\Delta; \Gamma \vdash \mathsf{tt} : \mathsf{sbool}\ \mathsf{true}} \quad \text{(E-TRUE)}$$

$$\frac{\Delta \vdash \Gamma \ ok \qquad \Delta \vdash A : \Omega}{\Delta \vdash \Gamma, x{:}A \ ok} \quad \text{(TE-EXT)} \qquad \frac{\Delta \vdash \Gamma \ ok}{\Delta; \Gamma \vdash \overline{n} : \mathsf{snat}\ \widehat{n}} \quad \text{(E-NAT)} \qquad \frac{\Delta \vdash \Gamma \ ok}{\Delta; \Gamma \vdash \mathsf{ff} : \mathsf{sbool}\ \mathsf{false}} \quad \text{(E-FALSE)}$$

$$\frac{\Delta \vdash A : \Omega \qquad \Delta; \Gamma, x{:}A \vdash f : A}{\Delta; \Gamma \vdash \mathsf{fix}\, x{:}A.\, f : A} \quad \text{(E-FIX)} \qquad \frac{\Delta; \Gamma \vdash e : \mathsf{snat}\ A \qquad \Delta; \Gamma \vdash e' : \mathsf{snat}\ A'}{\Delta; \Gamma \vdash e + e' : \mathsf{snat}\ (\mathsf{plus}\ A\ A')} \quad \text{(E-ADD)}$$

$$\frac{\Delta \vdash A : \Omega \qquad \Delta; \Gamma, x{:}A \vdash e : A'}{\Delta; \Gamma \vdash \lambda x{:}A.\, e : A \to A'} \quad \text{(E-FUN)} \qquad \frac{\Delta; \Gamma \vdash e : \mathsf{snat}\ A \qquad \Delta; \Gamma \vdash e' : \mathsf{snat}\ A'}{\Delta; \Gamma \vdash e < e' : \mathsf{sbool}\ (\mathsf{lt}\ A\ A')} \quad \text{(E-LT)}$$

$$\frac{\Delta; \Gamma \vdash e_1 : A \to A' \qquad \Delta; \Gamma \vdash e_2 : A}{\Delta; \Gamma \vdash e_1\ e_2 : A'} \quad \text{(E-APP)} \qquad \frac{\textit{for all } i < n \qquad \Delta; \Gamma \vdash e_i : A_i}{\Delta; \Gamma \vdash \langle e_0, \ldots e_{n-1} \rangle : \mathsf{tup}\ \widehat{n}\ (\mathsf{nth}\ (A_0 :: \ldots :: A_{n-1} :: \mathsf{nil}))} \quad \text{(E-TUP)}$$

$$\frac{\Delta \vdash B : s \qquad \Delta, X{:}B; \Gamma \vdash f : A}{\Delta; \Gamma \vdash \Lambda X{:}B.\, f : \forall_s X{:}B.\, A} \begin{pmatrix} X \notin \Delta \\ s \neq \mathsf{Ext} \end{pmatrix} \quad \text{(E-TFUN)} \qquad \frac{\Delta; \Gamma \vdash e : \mathsf{tup}\ A''\ B \qquad \Delta; \Gamma \vdash e' : \mathsf{snat}\ A' \qquad \Delta \vdash A : \mathsf{LT}\ A'\ A''}{\Delta; \Gamma \vdash \mathsf{sel}[A](e, e') : B\ A'} \quad \text{(E-SEL)}$$

$$\frac{\Delta; \Gamma \vdash e : \forall_s X{:}B.\, A' \qquad \Delta \vdash A : B}{\Delta; \Gamma \vdash e[A] : [A/X]A'}\ (s \neq \mathsf{Ext}) \quad \text{(E-TAPP)}$$

$$\frac{\Delta \vdash A : B \qquad \Delta \vdash B : s \qquad \Delta; \Gamma \vdash e : [A/X]A'}{\Delta; \Gamma \vdash \langle X{=}A,\, e{:}A' \rangle : \exists_s X{:}B.\, A'}\ (s \neq \mathsf{Ext}) \quad \text{(E-PACK)}$$

$$\frac{\begin{array}{ll} \Delta \vdash B : \mathsf{Bool} \to \mathsf{Kind} & \Delta; \Gamma \vdash e : \mathsf{sbool}\ A'' \\ \Delta \vdash A : B\ A'' & \Delta, X_1{:}B\ \mathsf{true}; \Gamma \vdash e_1 : A' \\ \Delta \vdash A' : \Omega & \Delta, X_2{:}B\ \mathsf{false}; \Gamma \vdash e_2 : A' \end{array}}{\Delta; \Gamma \vdash \mathsf{if}[B, A](e,\, X_1.\, e_1,\, X_2.\, e_2) : A'} \quad \text{(E-IF)}$$

$$\frac{\Delta; \Gamma \vdash e : \exists_s X'{:}B.\, A \qquad \Delta \vdash A' : \Omega \qquad \Delta, X{:}B; \Gamma, x{:}[X/X']A \vdash e' : A'}{\Delta; \Gamma \vdash \mathsf{open}\ e\ \mathsf{as}\ \langle X, x \rangle\ \mathsf{in}\ e' : A'} \begin{pmatrix} X \notin \Delta \\ s \neq \mathsf{Ext} \end{pmatrix} \quad \text{(E-OPEN)}$$

$$\frac{\Delta; \Gamma \vdash e : A \qquad A =_{\beta\eta\iota} A' \qquad \Delta \vdash A' : \Omega}{\Delta; \Gamma \vdash e : A'} \quad \text{(E-CONV)}$$

Figure 5: Static semantics of the computation language λ_H.

tees that implementations of sel need not check the subscript at runtime. Since the proof t_2 is ignored in the "else" branch, $\mathsf{ltPrf}\ t'\ t$ is defined to reduce to the trivial proof of True when the value of i' is not less than that of n.

The usual vector type, which keeps the length packaged with the content, is

$$\mathsf{vector} : \Omega \to \Omega = \lambda t{:}\Omega.\, \exists t'{:}\mathsf{Nat}.\, \mathsf{snat}\ t' \times \mathsf{vec}\ t'\ t.$$

Now we can write a wrapper function for sumVec with the standard type vector nat → nat; we leave the details to the reader.

4.3 Type safety

The type safety of λ_H is a corollary of its properties of progress and subject reduction. A pivoting element in proving progress (Lemma 4 in Appendix A) is the connection between the existence of a proof (type) term of kind $\mathsf{LT}\ \widehat{m}\ \widehat{n}$, provided by rule E-SEL, and the existence of a (meta-logical) proof of the side condition $m < n$, required by rule R-SEL. Similarly, subject reduction (Lemma 5 in Appendix A) in the cases of R-ADD and R-LT-T/F relies on the adequate representation of addition and comparison by plus and lt.

Lemma 1 (Adequacy of the TL representation of arithmetic)

1. For all $m, n \in \mathbb{N}$, $\mathsf{plus}\ \widehat{m}\ \widehat{n} =_{\beta\eta\iota} \widehat{m+n}$.
2. For all $m, n \in \mathbb{N}$, $\mathsf{lt}\ \widehat{m}\ \widehat{n} =_{\beta\eta\iota} \mathsf{true}$ if and only if $m < n$.
3. For all $m, n \in \mathbb{N}$, $m < n$ if and only if there exists a type A such that $\cdot \vdash A : \mathsf{LT}\ \widehat{m}\ \widehat{n}$.

Proof sketch (3) For the forward direction it suffices to observe that the structure of the meta-logical proof of $m < n$ (in terms of the above axioms of ordering) can be directly reflected in a type term of kind $\mathsf{LT}\ \widehat{m}\ \widehat{n}$. The inverse direction is shown by examining the structure of closed type terms of this kind in normal form. □

Theorem 1 (Safety of λ_H) If $\cdot;\cdot \vdash e : A$, then either $e \mapsto^* v$ and $\cdot;\cdot \vdash v : A$, or e diverges (*i.e.*, for each e', if $e \mapsto^* e'$, then there exists e'' such that $e' \mapsto e''$).

Proof sketch Follows from Lemmas 4 and 5 (Appendix A). □

Since CIC and TL are more expressive than higher-order predicate logic, adequacy of the representations of meta-proofs does not hold in general; in particular, the ability to eliminate inductive kinds in TL allows analysis of proof derivations to be used in proof construction, a technique not employed in standard meta-reasoning. This issue does not arise for first-order proof representations like LT (where no constructors have parameters of a function kind), and we do not expect it to be a concern in practice. In cases when it does arise, it could be resolved by using the underlying consistent logic of CIC instead of the meta-logic; for instance in our presentation the question of adequacy is raised because the operational semantics of λ_H is defined in meta-logical terms, but this question would be moot if λ_H and its semantics were defined as CIC terms. To eliminate the interaction with the meta-logic, this approach should be applied all the way down to the hardware specification (as done in some PCC system [3]); we plan to pursue this in the future.

4.4 An example of proof generation

Here we show the type term ltPrf which generates the proof of the proposition $\mathsf{LTOrTrue}\ t'\ t\ (\mathsf{lt}\ t'\ t)$, needed in the sumVec example. We first present a Church encoding of the kind term LT and its "constructors" ltzs and ltss.

$$\begin{array}{l}
\mathsf{LT} : \mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Kind} \\
\mathsf{LT} = \lambda t{:}\mathsf{Nat}.\ \lambda t'{:}\mathsf{Nat}. \\
\qquad \Pi R{:}\mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Kind}. \\
\qquad (\Pi t{:}\mathsf{Nat}.\ R\ \mathsf{zero}\ (\mathsf{succ}\ t)) \to \\
\qquad (\Pi t{:}\mathsf{Nat}.\ \Pi t'{:}\mathsf{Nat}.\ R\ t\ t' \to R\ (\mathsf{succ}\ t)\ (\mathsf{succ}\ t')) \to \\
\qquad R\ t\ t' \\
\mathsf{ltzs} : \Pi t{:}\mathsf{Nat}.\ \mathsf{LT}\ \mathsf{zero}\ (\mathsf{succ}\ t) \\
\mathsf{ltzs} = \lambda t{:}\mathsf{Nat}.\ \lambda R{:}\mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Kind}. \\
\qquad \lambda z{:}(\Pi t{:}\mathsf{Nat}.\ R\ \mathsf{zero}\ (\mathsf{succ}\ t)). \\
\qquad \lambda s{:}(\Pi t{:}\mathsf{Nat}.\ \Pi t'{:}\mathsf{Nat}.\ R\ t\ t' \to R\ (\mathsf{succ}\ t)\ (\mathsf{succ}\ t')). \\
\qquad z\ t \\
\mathsf{ltss} : \Pi t{:}\mathsf{Nat}.\ \Pi t'{:}\mathsf{Nat}.\ \mathsf{LT}\ t\ t' \to \mathsf{LT}\ (\mathsf{succ}\ t)\ (\mathsf{succ}\ t') \\
\mathsf{ltss} = \lambda t{:}\mathsf{Nat}.\ \lambda t'{:}\mathsf{Nat}.\ \lambda p{:}\mathsf{LT}\ t\ t'.\ \lambda R{:}\mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Kind}. \\
\qquad \lambda z{:}(\Pi t{:}\mathsf{Nat}.\ R\ \mathsf{zero}\ (\mathsf{succ}\ t)). \\
\qquad \lambda s{:}(\Pi t{:}\mathsf{Nat}.\ \Pi t'{:}\mathsf{Nat}.\ R\ t\ t' \to R\ (\mathsf{succ}\ t)\ (\mathsf{succ}\ t')). \\
\qquad s\ t\ t'\ (p\ R\ z\ s)
\end{array}$$

Next we define dependent conditionals on kinds Nat and Bool.

$$\begin{array}{l}
\mathsf{dep_ifez} : \Pi t{:}\mathsf{Nat}.\ \Pi k{:}\mathsf{Nat} \to \mathsf{Kind}. \\
\qquad\qquad k\ \mathsf{zero} \to (\Pi t'{:}\mathsf{Nat}.\ k\ (\mathsf{succ}\ t')) \to k\ t \\
\mathsf{dep_ifez\ zero} \quad = \lambda k{:}\mathsf{Nat} \to \mathsf{Kind}.\ \lambda t_1{:}k\ \mathsf{zero}. \\
\qquad\qquad \lambda t_2{:}(\Pi t'{:}\mathsf{Nat}.\ k\ (\mathsf{succ}\ t')).\ t_1 \\
\mathsf{dep_ifez}\ (\mathsf{succ}\ t) = \lambda k{:}\mathsf{Nat} \to \mathsf{Kind}.\ \lambda t_1{:}k\ \mathsf{zero}. \\
\qquad\qquad \lambda t_2{:}(\Pi t'{:}\mathsf{Nat}.\ k\ (\mathsf{succ}\ t')).\ t_2\ t \\
\\
\mathsf{dep_if} : \Pi t{:}\mathsf{Bool}.\ \Pi k{:}\mathsf{Bool} \to \mathsf{Kind}.\ k\ \mathsf{true} \to k\ \mathsf{false} \to k\ t \\
\mathsf{dep_if\ true} = \lambda k{:}\mathsf{Bool} \to \mathsf{Kind}.\ \lambda t_1{:}k\ \mathsf{true}.\ \lambda t_2{:}k\ \mathsf{false}.\ t_1 \\
\mathsf{dep_if\ false} = \lambda k{:}\mathsf{Bool} \to \mathsf{Kind}.\ \lambda t_1{:}k\ \mathsf{true}.\ \lambda t_2{:}k\ \mathsf{false}.\ t_2
\end{array}$$

Finally, some abbreviations, and then the proof generator itself.

$$\begin{array}{l}
\mathsf{LTcond} : \mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Kind} \\
\mathsf{LTcond} = \lambda t'{:}\mathsf{Nat}.\ \lambda t{:}\mathsf{Nat}.\ \mathsf{LTOrTrue}\ t'\ t\ (\mathsf{lt}\ t'\ t) \\
\\
\mathsf{LTimp} : \mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Bool} \to \mathsf{Kind} \\
\mathsf{LTimp} = \lambda t'{:}\mathsf{Nat}.\ \lambda t{:}\mathsf{Nat}.\ \lambda t''{:}\mathsf{Bool}. \\
\qquad \mathsf{LTOrTrue}\ t'\ t\ t'' \to \mathsf{LTOrTrue}\ (\mathsf{succ}\ t')\ (\mathsf{succ}\ t)\ t'' \\
\\
\mathsf{ltPrf} : \Pi t'{:}\mathsf{Nat}.\ \Pi t{:}\mathsf{Nat}.\ \mathsf{LTcond}\ t'\ t \\
\mathsf{ltPrf} = \lambda t'{:}\mathsf{Nat}. \\
\qquad \mathsf{Elim}[\mathsf{Nat}, \lambda t_1'{:}\mathsf{Nat}.\ \Pi t_1{:}\mathsf{Nat}.\ \mathsf{LTcond}\ t_1'\ t_1](t')\{ \\
\qquad\quad \lambda t_1{:}\mathsf{Nat}.\ \mathsf{dep_ifez}\ t_1\ (\mathsf{LTcond}\ \mathsf{zero})\ \mathsf{id}\ \mathsf{ltzs}; \\
\qquad\quad \lambda t_1'{:}\mathsf{Nat}.\ \lambda t_P{:}(\Pi t_1{:}\mathsf{Nat}.\ \mathsf{LTcond}\ t_1'\ t_1).\ \lambda t_1{:}\mathsf{Nat}. \\
\qquad\qquad \mathsf{dep_ifez}\ t_1 \\
\qquad\qquad\qquad (\mathsf{LTcond}\ (\mathsf{succ}\ t_1')) \\
\qquad\qquad\qquad \mathsf{id} \\
\qquad\qquad\qquad (\lambda t_1{:}\mathsf{Nat}.\ \mathsf{dep_if}\ (\mathsf{lt}\ t_1'\ t_1) \\
\qquad\qquad\qquad\qquad\qquad\qquad (\mathsf{LTimp}\ t_1'\ t_1) \\
\qquad\qquad\qquad\qquad\qquad\qquad (\mathsf{ltss}\ t_1'\ t_1) \\
\qquad\qquad\qquad\qquad\qquad\qquad (\mathsf{id}\ \mathsf{True}) \\
\qquad\qquad\qquad\qquad\qquad\qquad (t_P\ t_1))\}
\end{array}$$

5 CPS Conversion

In this section we show how to perform CPS conversion on λ_H while still preserving proofs represented in the type system. This stage transforms all unconditional control transfers, including function invocation and return, to function calls and gives explicit names to all intermediate computations. The basics of our approach, *i.e.* the target language and the transformation of types, are shown in this section. The static semantics of the target language and the transformation of terms are given in Appendix B.

We call the target calculus for this phase λ_K, with syntax:

$$\begin{array}{lll}
(\textit{val}) & v ::= x \mid \overline{n} \mid \mathsf{tt} \mid \mathsf{ff} \mid \langle X = A,\ v{:}A' \rangle \mid \langle v_0,\ \ldots\ v_{n-1} \rangle \\
& \qquad \mid \mathsf{fix}\ x'[X_1{:}A_1,\ \ldots X_n{:}A_n](x{:}A).\ e \\
(\textit{exp}) & e ::= v[A_1,\ \ldots A_n](v') \mid \mathsf{let}\ x = v\ \mathsf{in}\ e \\
& \qquad \mid \mathsf{let}\ \langle X,\ x \rangle = \mathsf{open}\ v\ \mathsf{in}\ e \mid \mathsf{let}\ x = \mathsf{sel}[A](v, v')\ \mathsf{in}\ e \\
& \qquad \mid \mathsf{let}\ x = v\ \mathit{aop}\ v'\ \mathsf{in}\ e \mid \mathsf{let}\ x = v\ \mathit{cop}\ v'\ \mathsf{in}\ e \\
& \qquad \mid \mathsf{if}[A, A'](v,\ X_1.\ e_1,\ X_2.\ e_2)
\end{array}$$

Expressions in λ_K consist of a series of let bindings followed by a function application or a conditional branch. There is only one abstraction mechanism, fix, which combines type and value abstraction. Multiple arguments may be passed by packing them in a tuple.

λ_K shares the TL type language with λ_H. The types for λ_K all have kind Ω_K which, as in λ_H, is an inductive kind defined in TL. The Ω_K kind has all the constructors of Ω plus one more (func). Since functions in CPS do not return values, the function type constructor of Ω_K has a different kind:

$$\twoheadrightarrow \quad : \quad \Omega_K \to \Omega_K$$

We use the more conventional syntax $A \to \bot$ for $\twoheadrightarrow\ A$. The new constructor func forms the types of function values:

$$\mathsf{func} \quad : \quad \Omega_K \to \Omega_K$$

Every function value is implicitly associated with a closure environment (for all the free variables), so the func constructor is useful in the closure-conversion phase (see Section 6).

Typed CPS conversion involves translating both types and computation terms. Existing algorithms [21, 28] require traversing and transforming every term in the type language (which would include all the proofs in our setting). This is impractical because proofs are large in size, and transforming them can alter their meanings and break the sharing among different intermediate languages.

To see the actual problem, let us convert the λ_H expression $\langle X = A,\ e : B \rangle$ to CPS, assuming that it has type $\exists X : A'.\ B$. We use $\mathcal{K}_{\text{typ}}$ to denote the meta-level translation function for the type language and $\mathcal{K}_{\text{exp}}$ for the computation language. Under existing algorithms, the translation also transforms the witness A:

$$\begin{array}{l}
\mathcal{K}_{\text{exp}}[\![\langle X = A,\ e : B \rangle]\!] = \\
\qquad \lambda \mathsf{k} : \mathcal{K}_{\text{typ}}[\![\exists X : A'.\ B]\!]. \\
\qquad\qquad \mathcal{K}_{\text{exp}}[\![e]\!]\ (\lambda x : \mathcal{K}_{\text{typ}}[\![[A/X]B]\!]. \\
\qquad\qquad\qquad \mathsf{k}\ \langle X = \mathcal{K}_{\text{typ}}[\![A]\!],\ x : \mathcal{K}_{\text{typ}}[\![B]\!] \rangle)
\end{array}$$

Here we CPS-convert e and apply it to a continuation, which puts the result of its evaluation in a package and hands it to the return continuation k. With proper definition of $\mathcal{K}_{\text{typ}}$ and assuming that $\mathcal{K}_{\text{typ}}[\![X]\!] = X$ on all variables X, we can show that the two types $\mathcal{K}_{\text{typ}}[\![[A/X]B]\!]$ and $[\mathcal{K}_{\text{typ}}[\![A]\!]/X](\mathcal{K}_{\text{typ}}[\![B]\!])$ are equivalent (under $=_{\beta\eta\iota}$). Thus the translation preserves typing.

But we do not want to touch the witness A, so the translation function should be defined as follows:

$$\begin{array}{l}
\mathcal{K}_{\text{exp}}[\![\langle X = A,\ e : B \rangle]\!] = \\
\qquad \lambda \mathsf{k} : \mathcal{K}_{\text{typ}}[\![\exists X : A'.\ B]\!]. \\
\qquad\qquad \mathcal{K}_{\text{exp}}[\![e]\!]\ (\lambda x : \mathcal{K}_{\text{typ}}[\![[A/X]B]\!]. \\
\qquad\qquad\qquad \mathsf{k}\ \langle X = A,\ x : \mathcal{K}_{\text{typ}}[\![B]\!] \rangle)
\end{array}$$

To preserve typing, we have to make sure that the two types $\mathcal{K}_{\text{typ}}[\![[A/X]B]\!]$ and $[A/X](\mathcal{K}_{\text{typ}}[\![B]\!])$ are equivalent. This seems impossible to achieve if $\mathcal{K}_{\text{typ}}$ is defined at the meta level.

Our solution is to internalize the definition of $\mathcal{K}_{\text{typ}}$ in our type language. We replace $\mathcal{K}_{\text{typ}}$ by a type function K of kind $\Omega \to \Omega_K$. For readability, we use the pattern-matching syntax, but it can be easily coded using the Elim construct.

$$
\begin{array}{lcl}
\mathsf{K}\ (\mathsf{snat}\ t) & = & \mathsf{snat}\ t \\
\mathsf{K}\ (\mathsf{sbool}\ t) & = & \mathsf{sbool}\ t \\
\mathsf{K}\ (t_1 \to t_2) & = & \mathsf{func}\ ((\mathsf{K}(t_1) \times \mathsf{K}_c(t_2)) \to \bot) \\
\mathsf{K}\ (\mathsf{tup}\ t_1\ t_2) & = & \mathsf{tup}\ t_1\ (\lambda t{:}\mathsf{Nat}.\ \mathsf{K}(t_2\ t)) \\
\mathsf{K}\ (\forall_{\mathsf{Kind}}\ k\ t) & = & \mathsf{func}\ (\forall_{\mathsf{Kind}}\ k\ (\lambda t_1{:}k.\ \mathsf{K}_c(t\ t_1) \to \bot)) \\
\mathsf{K}\ (\exists_{\mathsf{Kind}}\ k\ t) & = & \exists_{\mathsf{Kind}}\ k\ (\lambda t_1{:}k.\ \mathsf{K}(t\ t_1)) \\
\mathsf{K}\ (\forall_{\mathsf{Kscm}}\ z\ t) & = & \mathsf{func}\ (\forall_{\mathsf{Kscm}}\ z\ (\lambda k{:}z.\ \mathsf{K}_c(t\ k) \to \bot)) \\
\mathsf{K}\ (\exists_{\mathsf{Kscm}}\ z\ t) & = & \exists_{\mathsf{Kscm}}\ z\ (\lambda k{:}z.\ \mathsf{K}(t\ k)) \\
\\
\mathsf{K}_c & \equiv & \lambda t{:}\Omega.\ \mathsf{func}\ (\mathsf{K}(t) \to \bot)
\end{array}
$$

The definition of K is in the spirit of the interp function of Crary and Weirich [14]. However interp cannot be used in defining a similar CPS conversion, because its domain does not cover (nor is there an injection to it from) all types appearing in type annotations. In λ_H these types are in the inductive kind Ω and can be analyzed by K. We can now prove $\mathsf{K}\ ([A/X]B) =_{\beta\eta\iota} [A/X](\mathsf{K}\ (B))$ by first reducing B to the normal form B'. Clearly, $\mathsf{K}\ ([A/X]B) =_{\beta\eta\iota} \mathsf{K}\ ([A/X]B')$ and $[A/X](\mathsf{K}\ (B')) =_{\beta\eta\iota} [A/X](\mathsf{K}\ (B))$. We then prove $\mathsf{K}\ ([A/X]B') =_{\beta\eta\iota} [A/X](\mathsf{K}\ (B'))$ by induction over the structure of the normal form B'. The complete CPS-conversion algorithm is given in Appendix B.

6 Closure Conversion

In this section we address the issue of how to make closures explicit for all the CPS terms in λ_K. This stage rewrites all functions so that they contain no free variables. Any variables that appear free in a function value are packaged in an *environment*, which together with the closed code of the function form a *closure*. When a function is applied, the closed code and the environment are extracted from the closure and then the closed code is called with the environment as an additional parameter. Again, the basics of our approach are shown in this section and more details are given in Appendix C.

Our approach to closure conversion is based on Morrisett *et al.* [28], who adopt a type-erasure interpretation of polymorphism. We use the same idea for existential types. The language that we use for this phase is called λ_C with syntax:

$$
\begin{array}{lll}
(\textit{val}) & v ::= x \mid \overline{n} \mid \mathsf{tt} \mid \mathsf{ff} \mid \mathsf{fix}\ x'[X_1{:}A_1, \ldots X_n{:}A_n](x{:}A).\ e & \\
& \quad \mid v[A] \mid \langle v_0, \ldots v_{n-1} \rangle \mid \langle X = A,\ v{:}A' \rangle & \\
(\textit{exp}) & e ::= v\ v' \mid \mathsf{let}\ x = v\ \mathsf{in}\ e \mid \mathsf{let}\ x = \mathsf{sel}[A](v, v')\ \mathsf{in}\ e & \\
& \quad \mid \mathsf{let}\ \langle X,\ x \rangle = \mathsf{open}\ v\ \mathsf{in}\ e \mid \mathsf{let}\ x = v\ aop\ v'\ \mathsf{in}\ e & \\
& \quad \mid \mathsf{let}\ x = v\ cop\ v'\ \mathsf{in}\ e \mid \mathsf{if}[B, A](v,\ X_1.\ e_1,\ X_2.\ e_2) &
\end{array}
$$

λ_C is similar to λ_K, the main difference being that type application and value application are again separate. Type applications are values in λ_C reflecting the fact that they have no runtime effect in a type-erasure interpretation. We use the same kind of types Ω_K as in λ_K. We define the transformation of types as a function $\mathsf{Cl}{:}\Omega_K \to \Omega_K \to \Omega_K$, the second argument of which represents the type of the environment. As in CPS conversion, we write Cl as a TL function so that the closure-conversion algorithm does not have to traverse proofs represented in the type system.

$$
\begin{array}{lcl}
\mathsf{Cl}\ (\mathsf{snat}\ t) & = & \lambda t'{:}\Omega_K.\ \mathsf{snat}\ t \\
\mathsf{Cl}\ (\mathsf{sbool}\ t) & = & \lambda t'{:}\Omega_K.\ \mathsf{sbool}\ t \\
\mathsf{Cl}\ (t \to \bot) & = & \lambda t'{:}\Omega_K.\ (t' \times \mathsf{Cl}\ (t)\ \bot) \to \bot \\
\mathsf{Cl}\ (\mathsf{func}\ t) & = & \lambda t'{:}\Omega_K.\ \exists t_1{:}\Omega_K.\ (\mathsf{Cl}\ (t)\ t_1 \times t_1) \\
\mathsf{Cl}\ (\mathsf{tup}\ t_1\ t_2) & = & \lambda t'{:}\Omega_K.\ \mathsf{tup}\ t_1\ (\lambda t''{:}\mathsf{Nat}.\ \mathsf{Cl}\ (t_2\ t'')\ t') \\
\mathsf{Cl}\ (\forall_{\mathsf{Kind}}\ k\ t) & = & \lambda t'{:}\Omega_K.\ \forall_{\mathsf{Kind}}\ k\ (\lambda t_1{:}k.\ \mathsf{Cl}\ (t\ t_1)\ t') \\
\mathsf{Cl}\ (\exists_{\mathsf{Kind}}\ k\ t) & = & \lambda t'{:}\Omega_K.\ \exists_{\mathsf{Kind}}\ k\ (\lambda t_1{:}k.\ \mathsf{Cl}\ (t\ t_1)\ t') \\
\mathsf{Cl}\ (\forall_{\mathsf{Kscm}}\ z\ t) & = & \lambda t'{:}\Omega_K.\ \forall_{\mathsf{Kind}}\ z\ (\lambda k{:}z.\ \mathsf{Cl}\ (t\ k)\ t') \\
\mathsf{Cl}\ (\exists_{\mathsf{Kscm}}\ z\ t) & = & \lambda t'{:}\Omega_K.\ \exists_{\mathsf{Kscm}}\ z\ (\lambda k{:}z.\ \mathsf{Cl}\ (t\ k)\ t')
\end{array}
$$

7 Related Work

Our type language is a variant of the calculus of constructions [11] extended with inductive definitions (with both small and large elimination) [35, 41]. We omitted parameterized inductive kinds and dependent large elimination to simplify our presentation, however, all our meta-theoretic proofs carry over to a language that includes them. We support η-reduction in our language while the official Coq system does not. The proofs for the properties of TL are adapted from Geuvers [17] and Werner [41] (which in turn borrows ideas from Altenkirch [1]); the main difference is that our language has kind-schema variables and a new product formation rule (Ext, Kind) which are not in Werner's system.

The Coq proof assistant provides support for extracting programs from proofs [35]. It separates propositions and sets into two distinct universes Prop and Set. We do not distinguish between them because we are not aiming to extract programs from our proofs, instead, we are using proofs as specifications for our computation terms.

Burstall and McKinna [7] proposed the notion of deliverables, which is essentially the same as our notion of certified binaries. They use dependent strong sums to model each deliverable and give its categorical semantics. Their work does not support programs with effects and has all the problems mentioned in Section 2.3.

Xi and Pfenning's DML [44] is the first language that nicely combines dependent types with programs that may involve effects. Our ideas of using singleton types and lifting the level of the proof language are directly inspired by their work. Xi's system, however, does not support arbitrary propositions and explicit proofs. It also does not define the Ω kind as an inductive definition so it is unclear how it interacts with intensional type analysis [39] and how it preserves proofs during compilation.

We have discussed the relationship between our work and those on PCC, typed assembly languages, and intensional type analysis in Section 1. Inductive definitions subsume and generalize earlier systems on intensional type analysis [22, 14, 39]; the type-analysis construct in the computation language can be eliminated using the technique proposed by Crary *et al.* [16].

Concurrently with our work, Crary and Vanderwaart [12] recently proposed a system called LTT which also aims at adding explicit proofs to typed intermediate languages. LTT uses Linear LF [8] as its proof language. It shares some similarities with our system in that both are using singleton types [44] to circumvent the problems of dependent types. However, since LF does not have inductive definitions and the Elim construct, it is unclear how LTT can support intensional type analysis and type-level primitive recursive functions [15]. In fact, to define Ω as an inductive kind [39], LTT would have to add proof-kind variables and proof-kind polymorphism, which could significantly complicate the meta-theory of its proof language. LTT requires different type languages for different intermediate languages; it is unclear whether it can preserve proofs during CPS and closure conversion. The power of linear reasoning in LTT is desirable for tracking ephemeral prop-

erties that hold only for certain program states; we are working on adding such support into our framework.

8 Conclusions

We presented a general framework for explicitly representing propositions and proofs in typed intermediate or assembly languages. We showed how to integrate an entire proof system into our type language and how to perform CPS and closure conversion while still preserving proofs represented in the type system. Our work is a first step toward the goal of building realistic infrastructure for certified programming and certifying compilation.

Our type system is fairly concise and simple with respect to the number of syntactic constructs, yet it is powerful enough to express all the propositions and proofs in the higher-order predicate logic (extended with induction principles). In the future, we would like to use our type system to express advanced program invariants such as those involved in low-level mutable recursive data structures.

Our type language is not designed around any particular programming language. We can use it to typecheck as many different computation languages as we like; all we need is to define the corresponding Ω kind as an inductive definition. We hope to evolve our framework into a realistic typed common intermediate format.

Acknowledgment

We would like to thank Thorsten Altenkirch, Gilles Barthe, Thierry Coquand, Antony Courtney, Karl Crary, Christopher League, Zhaohui Luo, Christine Paulin-Mohring, Stefan Monnier, Henrik Nilsson, Walid Taha, and anonymous referees for discussions and comments on an earlier version of this paper. Benjamin Werner helped us understand the intricacies in the strong-normalization proof for the core calculus of inductive constructions.

References

[1] T. Altenkirch. *Constructions, Inductive Types and Strong Normalization*. PhD thesis, University of Edinburgh, UK, 1993.

[2] A. W. Appel and E. W. Felten. Models for security policies in proof-carrying code. Technical Report CS-TR-636-01, Princeton Univ., Dept. of Computer Science, March 2001.

[3] A. W. Appel and A. P. Felty. A semantic model of types and machine instructions for proof-carrying code. In *Proc. 27th ACM Symp. on Principles of Prog. Lang.*, pages 243–253. ACM Press, 2000.

[4] H. P. Barendregt. Lambda calculi with types. In S. Abramsky, D. Gabbay, and T. Maibaum, editors, *Handbook of Logic in Computer Science (volume 2)*. Oxford Univ. Press, 1991.

[5] H. P. Barendregt and H. Geuvers. Proof-assistants using dependent type systems. In A. Robinson and A. Voronkov, editors, *Handbook of Automated Reasoning*. Elsevier Sci. Pub. B.V., 1999.

[6] G. Barthe, J. Hatcliff, and M. Sorensen. CPS translations and applications: the cube and beyond. *Higher Order and Symbolic Computation*, 12(2):125–170, September 1999.

[7] R. Burstall and J. McKinna. Deliverables: an approach to program development in constructions. Technical Report ECS-LFCS-91-133, Univ. of Edinburgh, UK, 1991.

[8] I. Cervesato and F. Pfenning. A linear logical framework. In *Proc. 11th IEEE Symp. on Logic in Computer Science*, pages 264–275, July 1996.

[9] C. Colby, P. Lee, G. C. Necula, F. Blau, M. Plesko, and K. Cline. A certifying compiler for Java. In *Proc. 2000 ACM Conf. on Prog. Lang. Design and Impl.*, pages 95–107, New York, 2000. ACM Press.

[10] R. Constable. Constructive mathematics as a programming logic I: Some principles of theory. *Ann. of Discrete Mathemathics*, 24, 1985.

[11] T. Coquand and G. Huet. The calculus of constructions. *Information and Computation*, 76:95–120, 1988.

[12] K. Crary and J. Vanderwaart. An expressive, scalable type theory for certified code. Technical Report CMU-CS-01-113, School of Computer Science, Carnegie Mellon Univ., Pittsburg, PA, May 2001.

[13] K. Crary, D. Walker, and G. Morrisett. Typed memory management in a calculus of capabilities. In *Proc. 26th ACM Symp. on Principles of Prog. Lang.*, pages 262–275. ACM Press, 1999.

[14] K. Crary and S. Weirich. Flexible type analysis. In *Proc. 1999 ACM SIGPLAN Int'l Conf. on Functional Prog.*, pages 233–248. ACM Press, Sept. 1999.

[15] K. Crary and S. Weirich. Resource bound certification. In *Proc. 27th ACM Symp. on Principles of Prog. Lang.*, pages 184–198. ACM Press, 2000.

[16] K. Crary, S. Weirich, and G. Morrisett. Intensional polymorphism in type-erasure semantics. In *Proc. 1998 ACM SIGPLAN Int'l Conf. on Functional Prog.*, pages 301–312. ACM Press, Sept. 1998.

[17] H. Geuvers. *Logics and Type Systems*. PhD thesis, Catholic University of Nijmegen, The Netherlands, 1993.

[18] J.-Y. Girard. *Interprétation Fonctionnelle et Élimination des Coupures dans l'Arithmétique d'Ordre Supérieur*. PhD thesis, University of Paris VII, 1972.

[19] R. Harper. The practice of type theory. Talk presented at 2000 Alan J. Perlis Symposium, Yale University, New Haven, CT, April 2000.

[20] R. Harper, F. Honsell, and G. Plotkin. A framework for defining logics. *Journal of the ACM*, 40(1):143–184, 1993.

[21] R. Harper and M. Lillibridge. Explicit polymorphism and CPS conversion. In *Proc. 20th ACM Symp. on Principles of Prog. Lang.*, pages 206–219. ACM Press, 1993.

[22] R. Harper and G. Morrisett. Compiling polymorphism using intensional type analysis. In *Proc. 22nd ACM Symp. on Principles of Prog. Lang.*, pages 130–141. ACM Press, 1995.

[23] S. Hayashi. Singleton, union and intersection types for program extraction. In A. R. Meyer, editor, *Proc. International Conference on Theoretical Aspects of Computer Software*, pages 701–730, 1991.

[24] W. A. Howard. The formulae-as-types notion of constructions. In *To H.B.Curry: Essays on Computational Logic, Lambda Calculus and Formalism*. Academic Press, 1980.

[25] G. Huet, C. Paulin-Mohring, et al. The Coq proof assistant reference manual. Part of the Coq system version 6.3.1, May 2000.

[26] Y. Minamide, G. Morrisett, and R. Harper. Typed closure conversion. In *Proc. 23rd ACM Symp. on Principles of Prog. Lang.*, pages 271–283. ACM Press, 1996.

[27] S. Monnier, B. Saha, and Z. Shao. Principled scavenging. In *Proc. 2001 ACM Conf. on Prog. Lang. Design and Impl.*, pages 81–91, New York, 2001. ACM Press.

[28] G. Morrisett, D. Walker, K. Crary, and N. Glew. From System F to typed assembly language. In *Proc. 25th ACM Symp. on Principles of Prog. Lang.*, pages 85–97. ACM Press, Jan. 1998.

[29] G. Necula. Proof-carrying code. In *Proc. 24th ACM Symp. on Principles of Prog. Lang.*, pages 106–119, New York, Jan 1997. ACM Press.

[30] G. Necula and P. Lee. Safe kernel extensions without run-time checking. In *Proc. 2nd USENIX Symp. on Operating System Design and Impl.*, pages 229–243. USENIX Assoc., 1996.

[31] G. Necula and P. Lee. The design and implementation of a certifying compiler. In *Proc. 1998 ACM Conf. on Prog. Lang. Design and Impl.*, pages 333–344, New York, 1998. ACM Press.

[32] G. C. Necula. *Compiling with Proofs*. PhD thesis, School of Computer Science, Carnegie Mellon Univ., Sept. 1998.

[33] B. Nordstrom, K. Petersson, and J. Smith. *Programming in Martin-Löf's type theory*. Oxford University Press, 1990.

[34] C. Paulin-Mohring. Extracting F_ω's programs from proofs in the Calculus of Constructions. In *Proc. 16th ACM Symp. on Principles of Prog. Lang.*, pages 89–104, New York, Jan 1989. ACM Press.

[35] C. Paulin-Mohring. Inductive definitions in the system Coq—rules and properties. In M. Bezem and J. Groote, editors, *Proc. TLCA*. LNCS 664, Springer-Verlag, 1993.

[36] Z. Shao. An overview of the FLINT/ML compiler. In *Proc. 1997 ACM SIGPLAN Workshop on Types in Compilation*, June 1997.

[37] Z. Shao, C. League, and S. Monnier. Implementing typed intermediate languages. In *Proc. 1998 ACM SIGPLAN Int'l Conf. on Functional Prog.*, pages 313–323. ACM Press, 1998.

[38] M. A. Sheldon and D. K. Gifford. Static dependent types for first class modules. In *1990 ACM Conference on Lisp and Functional Programming*, pages 20–29, New York, June 1990. ACM Press.

[39] V. Trifonov, B. Saha, and Z. Shao. Fully reflexive intensional type analysis. In *Proc. 2000 ACM SIGPLAN Int'l Conf. on Functional Prog.*, pages 82–93. ACM Press, September 2000.

[40] D. Walker. A type system for expressive security policies. In *Proc. 27th ACM Symp. on Principles of Prog. Lang.*, pages 254–267. ACM Press, 2000.

[41] B. Werner. *Une Théorie des Constructions Inductives*. PhD thesis, A L'Université Paris 7, Paris, France, 1994.

[42] A. K. Wright and M. Felleisen. A syntactic approach to type soundness. *Information and Computation*, 115(1):38–94, 1994.

[43] H. Xi and R. Harper. A dependently typed assembly language. In *Proc. 2001 ACM SIGPLAN Int'l Conf. on Functional Prog.*, to appear.

[44] H. Xi and F. Pfenning. Dependent types in practical programming. In *Proc. 26th ACM Symp. on Principles of Prog. Lang.*, pages 214–227. ACM Press, 1999.

A Properties of λ_H

The proof of the following lemma is by induction on the structure of typing derivations.

Lemma 2 If $\Delta, X{:}B; \Gamma \vdash e : A'$ and $\Delta \vdash A : B$, then $\Delta; \Gamma \vdash [A/X]e : [A/X]A'$.

We also need a proposition guaranteeing that equivalence of constructor applications implies equivalence of their arguments; it is a corollary of the confluence of TL (Theorem 76).

Lemma 3 If $\mathsf{Ctor}\,(i, I)\ \vec{A} =_{\beta\eta\iota} \mathsf{Ctor}\,(i', I')\ \vec{A'}$, then $i = i'$ and $I =_{\beta\eta\iota} I'$ and $\vec{A} =_{\beta\eta\iota} \vec{A'}$.

Lemma 4 (Progress) If $\cdot;\cdot \vdash e : A$, then either e is a value, or there exists e' such that $e \mapsto e'$.

Proof sketch By standard techniques [42] using induction on computation terms. Due to the transitivity of $=_{\beta\eta\iota}$ any derivation of $\Delta; \Gamma \vdash e : A$ can be converted to a standard form in which there is an application of rule E-CONV at its root, whose first premise ends with an instance of a rule other than E-CONV, all of whose term derivation premises are in standard form.

We omit the proofs for the cases of standard constructs and the induction on the structure of evaluation contexts. The interesting case is that of the dependently typed sel.

If $e = \mathsf{sel}[A'](v, v')$, by inspection of the typing rules the derivation of $\cdot;\cdot \vdash e : A$ in standard form must have an instance of rule E-SEL in the premise of its root. Hence the subderivation for v must assign to it a tuple type, and the whole derivation has the form

$$\dfrac{\dfrac{\mathcal{D}}{\cdot;\cdot \vdash v : \mathsf{tup}\ A_2\ A''} \quad \dfrac{\mathcal{D}'}{\cdot;\cdot \vdash v' : \mathsf{snat}\ A_1} \quad \dfrac{\mathcal{E}}{\cdot \vdash A' : \mathsf{LT}\ A_1\ A_2}}{\cdot;\cdot \vdash \mathsf{sel}[A'](v, v') : A''\ A_1}}{\cdot;\cdot \vdash \mathsf{sel}[A'](v, v') : A}$$

where $A =_{\beta\eta\iota} A''\ A_1$. By inspection of the typing rules, rules other than E-CONV assign to all values types which are applications of constructors of Ω. Since the derivation $\mathcal{D}$ is in standard form, it ends with an E-CONV, in the premise of which another rule assigns v a type $\beta\eta\iota$-equivalent to $\mathsf{tup}\ A_2\ A''$. Then by Lemma 3 this type must be an application of tup, and again by inspection the only rule which applies is E-TUP, which implies $v = \langle v_0, \ldots v_{n-1}\rangle$, and the derivation $\mathcal{D}$ must have the form

$$\dfrac{\forall i < n\ \dfrac{\mathcal{D}_i}{\cdot;\cdot \vdash v_i : A_1''\ \widehat{i}}}{\cdot;\cdot \vdash \langle v_0, \ldots v_{n-1}\rangle : \mathsf{tup}\ \widehat{n}\ A_1''}$$

Also by Lemma 3 $A_2 =_{\beta\eta\iota} \widehat{n}$. Similarly the only rule assigning to a value a type convertible to that in the conclusion of $\mathcal{D}'$ is E-NAT, hence $A_1 =_{\beta\eta\iota} \widehat{m}$ for some $m \in \mathbb{N}$, and $v' = \overline{m}$. Then, by adequacy of LT (Lemma 1(3)), the conclusion of $\mathcal{E}$ implies that $m < n$. Hence by rule R-SEL $e \mapsto v_m$. □

Lemma 5 (Subject Reduction) If $\cdot;\cdot \vdash e : A$ and $e \mapsto e'$, then $\cdot;\cdot \vdash e' : A$.

Proof sketch Since evaluation contexts bind no variables, it suffices to prove subject reduction for $\hookrightarrow$ and a standard term substitution lemma. We show only some cases of redexes involving sel and if.

- The derivation for $e = \mathsf{sel}[A'](\langle v_0, \ldots v_{n-1}\rangle, \overline{m})$ in standard form has the shape

$$\dfrac{\dfrac{\dfrac{\forall i < n\ \dfrac{\mathcal{D}_i}{\cdot;\cdot \vdash v_i : A_1''\ \widehat{i}}}{\cdot;\cdot \vdash \langle \vec{v}\rangle : \mathsf{tup}\ \widehat{n}\ A_1''} \quad \dfrac{\mathcal{D}'}{\cdot;\cdot \vdash \overline{m} : \mathsf{snat}\ \widehat{m}}}{\cdot;\cdot \vdash \langle \vec{v}\rangle : \mathsf{tup}\ A_2\ A''} \quad \dfrac{\mathcal{E}}{\cdot \vdash A' : \mathsf{LT}\ A_1\ A_2}}{\cdot;\cdot \vdash \mathsf{sel}[A'](\langle v_0, \ldots v_{n-1}\rangle, \overline{m}) : A''\ A_1}}{\cdot;\cdot \vdash \mathsf{sel}[A'](\langle v_0, \ldots v_{n-1}\rangle, \overline{m}) : A}$$

  where $A =_{\beta\eta\iota} A''\ A_1$, $A_1'' =_{\beta\eta\iota} A''$, and $A_1 =_{\beta\eta\iota} \widehat{m}$. Since $e \mapsto e'$ only by rule R-SEL, we have $m < n$ and $e' = v_m$, so from $\mathcal{D}_m$ and $A_1''\ \widehat{m} =_{\beta\eta\iota} A''\ \widehat{m} =_{\beta\eta\iota} A''\ A_1 =_{\beta\eta\iota} A$ we obtain a derivation of $\cdot;\cdot \vdash e' : A$.

- In the case of if the standard derivation $\mathcal{D}$ of

$$\cdot;\cdot \vdash \mathsf{if}[B, A'](\mathsf{tt},\ X_1.\, e_1,\ X_2.\, e_2) : A$$

  ends with an instance of E-CONV, preceded by an instance of E-IF. Using the notation from Figure 5, from the premises of this rule it follows that we have a derivation $\mathcal{E}$ of $\cdot \vdash A' : B\ A''$, and $A'' =_{\beta\eta\iota} \mathsf{true}$ (since rule E-TRUE assigns sbool true to tt), hence we have $\cdot \vdash A' : B\ \mathsf{true}$ by CONV. By Lemma 2 from $\mathcal{E}$ and the derivation of $X_1 : B\ \mathsf{true}$; $\cdot \vdash e_1 : A$ (provided as another premise), since X_1 is not free in A (ensured by the premise $\cdot \vdash A : \Omega$) we obtain a derivation of $\cdot;\cdot \vdash [A'/X_1]e_1 : A$. □

B CPS Conversion (Details)

We start by defining a version of λ_H using type-annotated terms. By $\bar{f}$ and $\bar{e}$ we denote the terms without annotations. Type annotations allow us to present the CPS transformation based on syntactic

instead of typing derivations.

$$
\begin{array}{lll}
(\textit{exp}) & e & ::= \bar{e}^A \\
& \bar{e} & ::= x \mid \overline{n} \mid \mathsf{tt} \mid \mathsf{ff} \mid f \mid \mathsf{fix}\, x\!:\!A.\, f \mid e\ e' \mid e[A] \\
& & \quad \mid \langle X = A,\, e\!:\!A' \rangle \mid \mathsf{open}\ e\ \mathsf{as}\ \langle X,\, x \rangle\ \mathsf{in}\ e' \\
& & \quad \mid \langle e_0,\, \ldots\ e_{n-1} \rangle \mid \mathsf{sel}[A](e, e') \mid e\ \mathit{aop}\ e' \\
& & \quad \mid e\ \mathit{cop}\ e' \mid \mathsf{if}[A, A'](e,\, X_1.\, e_1,\, X_2.\, e_2) \\
(\textit{fun}) & f & ::= \bar{f}^A \\
& \bar{f} & ::= \lambda x\!:\!A.\, e \mid \Lambda X\!:\!A.\, f
\end{array}
$$

The target language λ_K of the CPS conversion stage has been defined in Section 5. We use the following syntactic sugar to denote non-recursive function definitions and value applications in λ_K(here x' is a fresh variable):

$$
\begin{array}{l}
\lambda x\!:\!A.\, e \equiv \mathsf{fix}\ x'[](x\!:\!A).\, e \\
\quad v\ v' \equiv v[](v') \\
\Lambda X_1\!:\!A_1.\ \ldots \Lambda X_n\!:\!A_n.\, \lambda x\!:\!A.\, e \\
\qquad \equiv \mathsf{fix}\ x'[X_1\!:\!A_1,\ \ldots X_n\!:\!A_n](x\!:\!A).\, e
\end{array}
$$

In the static semantics of λ_K we use two forms of judgments. As in λ_H, the judgment $\Delta;\ \Gamma \vdash_K\ v : A$ indicates that the value v is well formed and of type A in the type and value contexts Δ and Γ respectively. Moreover, $\Delta;\ \Gamma \vdash_K\ e$ indicates that the expression e is well formed in Δ and Γ. In both forms of judgments, we omit the subscript from $\vdash_K$ when it can be deduced from the context.

The static semantics of λ_K is specified by the following formation rules (we omit the rules for environment formation, variables, constants, tuples, packages, and type conversion on values, which are the same as in λ_H):

$$
\frac{\begin{array}{c}\textit{for all } i \in \{1 \ldots n\} \qquad \Delta \vdash A_i : s_i \\ \Delta, X_1\!:\!A_1 \ldots, X_n\!:\!A_n \vdash A : \Omega \\ \Delta, X_1\!:\!A_1 \ldots, X_n\!:\!A_n;\ \Gamma, x'\!:\!A', x\!:\!A \vdash e\end{array}}{\begin{array}{l}\Delta;\ \Gamma \vdash\ \mathsf{fix}\ x'[X_1\!:\!A_1,\ \ldots X_n\!:\!A_n](x\!:\!A).\, e : A' \\ \textit{where} \\ A' = \mathsf{func}\ (\forall_{s_1} X_1\!:\!A_1 \ldots \forall_{s_n} X_n\!:\!A_n.\, A \to \bot)\end{array}} \quad (\text{K-FIX})
$$

$$
\frac{\begin{array}{c}\textit{for all } i \in \{1 \ldots n\} \qquad \Delta \vdash A_i : B_i \\ \Delta;\ \Gamma \vdash v' : \mathsf{func}\,(\forall_{s_1} X_1\!:\!B_1 \ldots \forall_{s_n} X_n\!:\!B_n.\, A \to \bot) \\ \Delta;\ \Gamma \vdash\ v : [A_1/X_1] \ldots [A_n/X_n]A\end{array}}{\Delta;\ \Gamma \vdash\ v'[A_1,\ \ldots A_n](v)} \quad (\text{K-APP})
$$

$$
\frac{\Delta;\ \Gamma \vdash\ v : A \qquad \Delta;\ \Gamma, x\!:\!A \vdash\ e}{\Delta;\ \Gamma \vdash\ \mathsf{let}\ x = v\ \mathsf{in}\ e} \quad (\text{K-VAL})
$$

$$
\frac{\begin{array}{c}\Delta;\ \Gamma \vdash\ v : \mathsf{tup}\ A''\ B \qquad \Delta;\ \Gamma \vdash\ v' : \mathsf{snat}\ A' \\ \Delta \vdash\ A : \mathsf{LT}\ A'\ A'' \qquad \Delta;\ \Gamma, x\!:\!B\ A' \vdash\ e\end{array}}{\Delta;\ \Gamma \vdash\ \mathsf{let}\ x = \mathsf{sel}[A](v, v')\ \mathsf{in}\ e} \quad (\text{K-SEL})
$$

$$
\frac{\begin{array}{c}\Delta;\ \Gamma \vdash\ v : \exists_s Y\!:\!B.\, A \\ \Delta, X\!:\!B;\ \Gamma, x\!:\![X/Y]A \vdash\ e\end{array}}{\Delta;\ \Gamma \vdash\ \mathsf{let}\ \langle X,\, x \rangle = \mathsf{open}\ v\ \mathsf{in}\ e} \begin{pmatrix} X \notin \Delta \\ s \neq \mathsf{Ext} \end{pmatrix} \quad (\text{K-OPEN})
$$

$$
\frac{\begin{array}{c}\Delta;\ \Gamma \vdash\ v : \mathsf{snat}\ A \qquad \Delta;\ \Gamma \vdash\ v' : \mathsf{snat}\ A' \\ \Delta;\ \Gamma, x\!:\!\mathsf{snat}\ (\mathsf{plus}\ A\ A') \vdash\ e\end{array}}{\Delta;\ \Gamma \vdash\ \mathsf{let}\ x = v + v'\ \mathsf{in}\ e} \quad (\text{K-ADD})
$$

$$
\frac{\begin{array}{c}\Delta;\ \Gamma \vdash\ v : \mathsf{snat}\ A \qquad \Delta;\ \Gamma \vdash\ v' : \mathsf{snat}\ A' \\ \Delta;\ \Gamma, x\!:\!\mathsf{sbool}\ (\mathsf{lt}\ A\ A') \vdash\ e\end{array}}{\Delta;\ \Gamma \vdash\ \mathsf{let}\ x = v < v'\ \mathsf{in}\ e} \quad (\text{K-LT})
$$

$$
\frac{\begin{array}{c}\Delta \vdash\ B : \mathsf{Bool} \to \mathsf{Kind} \qquad \Delta \vdash\ A : B\ A' \\ \Delta;\ \Gamma \vdash\ v : \mathsf{sbool}\ A' \\ \Delta, X_1\!:\!B\ \mathsf{true};\ \Gamma \vdash\ e_1 \qquad \Delta, X_2\!:\!B\ \mathsf{false};\ \Gamma \vdash\ e_2\end{array}}{\Delta;\ \Gamma \vdash\ \mathsf{if}[B, A](v,\, X_1.\, e_1,\, X_2.\, e_2)} \quad (\text{K-IF})
$$

Except for the rules K-FIX and K-APP, which must take into account the presence of func, the static semantics for λ_K is a natural consequence of the static semantics for λ_H.

The definition of the CPS transformation for computation terms of λ_H to computation terms of λ_K is given in Figure 6, where we use the abbreviations introduced in Section 5.

Proposition 2 (Type Correctness of CPS Conversion)
If $\cdot;\cdot \vdash_H\ e : A$, then $\cdot;\cdot \vdash_K\ \mathcal{K}_{\text{exp}}[\![\bar{e}^A]\!] : \mathsf{func}\ (\mathsf{K_c}(A) \to \bot)$.

C Closure Conversion (Details)

The main difference in the static semantics between λ_K and λ_C is that in the latter the body of a function must not contain free type or term variables. This is formalized in the rule C-FIX below. The rules C-TAPP and C-APP corresponding to the separate type and value application in λ_C are standard.

$$
\frac{\begin{array}{c}\textit{for all } i < n \qquad \cdot \vdash\ A_i : s_i \\ \cdot, X_1\!:\!A_1 \ldots, X_n\!:\!A_n \vdash\ A : \Omega \\ \cdot, X_1\!:\!A_1 \ldots, X_n\!:\!A_n;\ \cdot, x'\!:\!B, x\!:\!A \vdash\ e\end{array}}{\begin{array}{l}\Delta;\ \Gamma \vdash\ \mathsf{fix}\ x'[X_1\!:\!A_1,\ \ldots X_n\!:\!A_n](x\!:\!A).\, e : B \\ \textit{where } B = \forall_{s_1} X_1\!:\!A_1 \ldots \forall_{s_n} X_n\!:\!A_n.\, A \to \bot\end{array}} \quad (\text{C-FIX})
$$

$$
\frac{\Delta;\ \Gamma \vdash\ v : \forall_s X\!:\!A'.\, B \qquad \Delta \vdash\ A : A'}{\Delta;\ \Gamma \vdash\ v[A] : [A/X]B} \quad (\text{C-TAPP})
$$

$$
\frac{\Delta;\ \Gamma \vdash\ v_1 : A \to \bot \qquad \Delta;\ \Gamma \vdash\ v_2 : A}{\Delta;\ \Gamma \vdash\ v_1\ v_2} \quad (\text{C-APP})
$$

The definition of the closure transformation for the computation terms of λ_K is given in Figure 7.

Proposition 3 (Type Correctness of Closure Conversion)
If $\cdot;\cdot \vdash_K\ v : A$, then $\cdot;\cdot \vdash_C\ \mathcal{C}_{\text{val}}[\![v]\!] : \mathsf{Cl}\ (A)\ \bot$.

D Formalization of TL (Details)

In this appendix we prove the meta-theoretic properties of our type language TL. The proofs are based on the methods in Werner [41]. We formalize the language in Section D.1. In Section D.2 we prove subject reduction, in Section D.3 we prove the strong normalization, in Section D.4 we prove the Church-Rosser property, in Section D.5 we prove the consistency of the underlying logic.

D.1 Syntax and semantics

The syntax for the pseudoterms is:

$$
\begin{array}{lll}
(\textit{ctxt}) & \Delta & ::= \cdot \mid \Delta, X\!:\!A \\
(\textit{sort}) & s & ::= \mathsf{Kind} \mid \mathsf{Kscm} \mid \mathsf{Ext} \\
(\textit{var}) & X & ::= z \mid k \mid t \\
(\textit{ptm}) & A, B & ::= s \mid X \mid \lambda X\!:\!A.\, B \mid A\ B \mid \Pi X\!:\!A.\, B \\
& & \quad \mid \mathsf{Ind}(X\!:\!\mathsf{Kind})\{\vec{A}\} \mid \mathsf{Ctor}\,(i, A) \\
& & \quad \mid \mathsf{Elim}[A', B'](A)\{\vec{B}\}
\end{array}
$$

$$
\begin{aligned}
\mathcal{K}_{\text{fval}}[\![(\lambda x\!:\!A.\, e^B)^{A\to B}]\!] &= \lambda x_{\text{arg}}\!:\!\mathsf{K}(A)\times\mathsf{K}_{\text{c}}(B).\\
&\quad \mathsf{let}\ x=\mathsf{sel}[\mathsf{ltPrf}\ \widehat{0}\ \widehat{2}](x_{\text{arg}},\overline{0})\ \mathsf{in}\\
&\quad \mathsf{let}\ \mathsf{k}=\mathsf{sel}[\mathsf{ltPrf}\ \widehat{1}\ \widehat{2}](x_{\text{arg}},\overline{1})\ \mathsf{in}\\
&\quad \mathcal{K}_{\text{exp}}[\![e^B]\!]\ \mathsf{k}\\
\mathcal{K}_{\text{fval}}[\![(\Lambda X\!:\!A.\, f^B)^{\forall_s X:A.\ B}]\!] &=\\
&\quad \Lambda X\!:\!A.\,\lambda \mathsf{k}\!:\!\mathsf{K}_{\text{c}}(B).\,\mathsf{k}\ (\mathcal{K}_{\text{fval}}[\![f^B]\!])\\
\mathcal{K}_{\text{exp}}[\![\bar{e}^A]\!] &= \lambda \mathsf{k}\!:\!\mathsf{K}_{\text{c}}(A).\,\mathsf{k}\ (\bar{e})\\
&\quad \text{for } \bar{e}^A \text{ one of } x^A,\ \overline{n}^{\mathsf{snat}\ \hat{n}},\ \mathsf{tt}^{\mathsf{sbool\ true}},\ \mathsf{ff}^{\mathsf{sbool\ false}}\\
\mathcal{K}_{\text{exp}}[\![f^A]\!] &= \lambda \mathsf{k}\!:\!\mathsf{K}_{\text{c}}(A).\,\mathsf{k}\ (\mathcal{K}_{\text{fval}}[\![f^A)]\!]\\
\mathcal{K}_{\text{exp}}[\![(\mathsf{fix}\ x\!:\!A.\, f^A)^A]\!] &=\\
&\quad \lambda \mathsf{k}\!:\!\mathsf{K}_{\text{c}}(A).\,\mathsf{k}\ (\mathsf{fix}\ x[](\mathsf{k}\!:\!\mathsf{K}_{\text{c}}(A)).\,\mathsf{k}\ (\mathcal{K}_{\text{fval}}[\![f^A]\!]))\\
\mathcal{K}_{\text{exp}}[\![(e_1{}^{A\to B}\ e_2{}^A)^B]\!] &= \lambda \mathsf{k}\!:\!\mathsf{K}_{\text{c}}(B).\\
&\quad \mathcal{K}_{\text{exp}}[\![e_1{}^{A\to B}]\!]\ (\lambda x_1\!:\!\mathsf{K}(A\to B).\\
&\quad \mathcal{K}_{\text{exp}}[\![e_2{}^A]\!]\ (\lambda x_2\!:\!\mathsf{K}(A).\\
&\quad x_1\ \langle x_2,\mathsf{k}\rangle))\\
\mathcal{K}_{\text{exp}}[\![(e^{\forall_s\ A'\ B}[A])^{B\ A}]\!] &= \lambda \mathsf{k}\!:\!\mathsf{K}_{\text{c}}(B\ A).\\
&\quad \mathcal{K}_{\text{exp}}[\![e^{\forall_s\ A'\ B}]\!]\ (\lambda x\!:\!\mathsf{K}(\forall_s\ A'\ B).\\
&\quad x[A](\mathsf{k}))\\
\mathcal{K}_{\text{exp}}[\![\langle e_0^{A_0},\ldots e_{n-1}^{A_{n-1}}\rangle^A]\!] &= \lambda \mathsf{k}\!:\!\mathsf{K}_{\text{c}}(A).\\
&\quad \mathcal{K}_{\text{exp}}[\![e_0^{A_0}]\!]\ (\lambda x_0\!:\!\mathsf{K}(A_0).\\
&\quad \vdots\\
&\quad \mathcal{K}_{\text{exp}}[\![e_{n-1}^{A_{n-1}}]\!]\ (\lambda x_{n-1}\!:\!\mathsf{K}(A_{n-1}).\\
&\quad \mathsf{k}\ \langle x_0,\ldots x_{n-1}\rangle)\ldots)\\
\mathcal{K}_{\text{exp}}[\![\mathsf{sel}[A](e_1{}^{\mathsf{tup}\ A''\ B},e_2{}^{\mathsf{snat}\ A'})^{B\ A'}]\!] &=\\
&\quad \lambda \mathsf{k}\!:\!\mathsf{K}_{\text{c}}(B\ A').\,\mathcal{K}_{\text{exp}}[\![e_1{}^{\mathsf{tup}\ A''\ B}]\!]\ (\lambda x_1\!:\!\mathsf{K}(\mathsf{tup}\ A''\ B).\\
&\quad \mathcal{K}_{\text{exp}}[\![e_2{}^{\mathsf{snat}\ A'}]\!]\ (\lambda x_2\!:\!\mathsf{K}(\mathsf{snat}\ A').\\
&\quad \mathsf{let}\ x'=\mathsf{sel}[A](x_1,x_2)\ \mathsf{in}\ \mathsf{k}\ x'))\\
\mathcal{K}_{\text{exp}}[\![\langle X=A,\ e^{[A/X]B}\!:\!B\rangle^{A'}]\!] &=\\
&\quad \lambda \mathsf{k}\!:\!\mathsf{K}_{\text{c}}(A').\,\mathcal{K}_{\text{exp}}[\![e^{[A/X]B}]\!]\ (\lambda x\!:\!\mathsf{K}([A/X]B).\\
&\quad \mathsf{k}\ \langle X=A,\ x\!:\!\mathsf{K}(B)\rangle)\\
\mathcal{K}_{\text{exp}}[\![(\mathsf{open}\ e_1{}^{\exists_s Y:A'.\ B}\ \mathsf{as}\ \langle X,\ x\rangle\ \mathsf{in}\ e_2{}^A)^A]\!] &=\\
&\quad \lambda \mathsf{k}\!:\!\mathsf{K}_{\text{c}}(A).\,\mathcal{K}_{\text{exp}}[\![e_1{}^{\exists_s Y:A'.\ B}]\!]\ (\lambda x_1\!:\!\mathsf{K}(\exists_s Y\!:\!A'.\ B).\\
&\quad \mathsf{let}\ \langle X,\ x\rangle=\mathsf{open}\ x_1\ \mathsf{in}\ \mathcal{K}_{\text{exp}}[\![e_2{}^A]\!]\ \mathsf{k})\\
\mathcal{K}_{\text{exp}}[\![(e_1{}^{\mathsf{snat}\ A}+e_2{}^{\mathsf{snat}\ A'})^{\mathsf{snat}\ (\mathsf{plus}\ A\ A')}]\!] &=\\
&\quad \lambda \mathsf{k}\!:\!\mathsf{K}_{\text{c}}(\mathsf{snat}\ (\mathsf{plus}\ A\ A')).\,\mathcal{K}_{\text{exp}}[\![e_1{}^{\mathsf{snat}\ A}]\!]\ (\lambda x_1\!:\!\mathsf{K}(\mathsf{snat}\ A).\\
&\quad \mathcal{K}_{\text{exp}}[\![e_2{}^{\mathsf{snat}\ A'}]\!]\ (\lambda x_2\!:\!\mathsf{K}(\mathsf{snat}\ A').\\
&\quad \mathsf{let}\ x'=x_1+x_2\ \mathsf{in}\ \mathsf{k}\ x'))\\
\mathcal{K}_{\text{exp}}[\![(e_1{}^{\mathsf{snat}\ A}<e_2{}^{\mathsf{snat}\ A'})^{\mathsf{sbool}\ (\mathsf{lt}\ A\ A')}]\!] &=\\
&\quad \lambda \mathsf{k}\!:\!\mathsf{K}_{\text{c}}(\mathsf{sbool}\ (\mathsf{lt}\ A\ A')).\,\mathcal{K}_{\text{exp}}[\![e_1{}^{\mathsf{snat}\ A}]\!]\ (\lambda x_1\!:\!\mathsf{K}(\mathsf{snat}\ A).\\
&\quad \mathcal{K}_{\text{exp}}[\![e_2{}^{\mathsf{snat}\ A'}]\!]\ (\lambda x_2\!:\!\mathsf{K}(\mathsf{snat}\ A').\\
&\quad \mathsf{let}\ x'=x_1<x_2\ \mathsf{in}\ \mathsf{k}\ x'))\\
\mathcal{K}_{\text{exp}}[\![(\mathsf{if}[B,A](e^{\mathsf{sbool}\ A''},\ X_1.\,e_1{}^{A'},\ X_2.\,e_2{}^{A'}))^{A'}]\!] &=\\
\lambda \mathsf{k}\!:\!\mathsf{K}_{\text{c}}(A').\,\mathcal{K}_{\text{exp}}[\![e^{\mathsf{sbool}\ A''}]\!]\ (\lambda x\!:\!\mathsf{K}(\mathsf{sbool}\ A'').&\\
\mathsf{if}[B,A](x,\ X_1.\,\mathcal{K}_{\text{exp}}[\![e_1{}^{A'}]\!]\ \mathsf{k},\ X_2.\,\mathcal{K}_{\text{exp}}[\![e_2{}^{A'}]\!]\ \mathsf{k}))&
\end{aligned}
$$

Figure 6: CPS conversion: from λ_H to λ_K.

In addition to the symbols defined in the syntax, we will also use C to denote general terms, Y and Z for variables, and I for inductive definitions. We use $\vec{A}$ to denote a sequence of terms $A_1,\ldots,A_n$. Also, we distinguish between A and $\vec{A}$ since every element in $\vec{A}$ would be referred as A_i anyway.

TL has the following PTS specification which will be used to derive its typing rules:

$$
\begin{array}{lcl}
\mathcal{S} & = & \mathsf{Kind},\mathsf{Kscm},\mathsf{Ext}\\
\mathcal{A} & = & \mathsf{Kind}:\mathsf{Kscm},\mathsf{Kscm}:\mathsf{Ext}\\
\mathcal{R} & = & (\mathsf{Kind},\mathsf{Kind}),(\mathsf{Kscm},\mathsf{Kind}),(\mathsf{Ext},\mathsf{Kind})\\
 & & (\mathsf{Kind},\mathsf{Kscm}),(\mathsf{Kscm},\mathsf{Kscm})
\end{array}
$$

In order to ensure that the interpretation of inductive definitions remains consistent, and they can be interpreted as terms closed under their introduction rules, we impose *positivity constraints* on the constructors of an inductive definition. The positivity constraints are defined in Definition 4 and 5.

Definition 4 A term A is *strictly positive in* X if A is either X or $\Pi Y:B.\,A'$, where A' is strictly positive in X, X does not occur free in B, and $X\neq Y$.

Definition 5 A term C is a *well-formed constructor kind* for X (written $wfc_X(C)$) if it has one of the following forms:

1. X;

$$
\begin{aligned}
\mathcal{C}_{\text{val}}[\![v]\!] &= v, \qquad \text{for } v \text{ one of } x,\ \overline{n},\ \mathsf{tt},\ \mathsf{ff}\\
\mathcal{C}_{\text{val}}[\![\langle v_0,\ \ldots\ v_{n-1}\rangle]\!] &= \langle \mathcal{C}_{\text{val}}[\![v_0]\!],\ \ldots \mathcal{C}_{\text{val}}[\![v_{n-1}]\!]\rangle\\
\mathcal{C}_{\text{val}}[\![\langle X=A,\ v\!:\!B\rangle]\!] &= \langle X=A,\ \mathcal{C}_{\text{val}}[\![v]\!]\!:\!\mathsf{Cl}\ (B)\ \bot\rangle\\
\mathcal{C}_{\text{val}}[\![\mathsf{fix}\ x'[X_1\!:\!A_1,\ \ldots X_n\!:\!A_n](x\!:\!A).\,e]\!] &=\\
&\quad \langle X=A_{\text{env}},\ \langle v_{\text{code}}[Y_1]\ldots[Y_m],v_{\text{env}}\rangle\!:\!A_X\rangle\\
&\text{where}\\
&A_X = A'_X\times X\\
&A'_X = \forall_{s_1}X_1\!:\!A_1.\ldots\forall_{s_n}X_n\!:\!A_n.\,(X\times\mathsf{Cl}\ (A)\ \bot)\to\bot\\
&\{x_0^{A'_0},\ \ldots x_{k-1}^{A'_{k-1}}\} = FV(e)-\{x,\,x'\}\\
&\{Y_1^{B'_1},\ \ldots Y_m^{B'_m}\} =\\
&\qquad FTV(\mathsf{fix}\ x'[X_1\!:\!A_1,\ \ldots X_n\!:\!A_n](x\!:\!A).\,e)\\
&A_{\text{env}} = \mathsf{Cl}\ (\mathsf{tup}\ \widehat{k}\ (\mathsf{nth}\ (A'_0{::}\ldots A'_{k-1}{::}\mathsf{nil})))\ \bot\\
&v_{\text{env}} = \langle x_0\ \ldots x_{k-1}\rangle\\
&v_{\text{code}} = \mathsf{fix}\ v_{\text{fix}}[Y_1\!:\!B'_1,\ \ldots Y_m\!:\!B'_m,X_1\!:\!A_1,\ \ldots X_n\!:\!A_n]\\
&\qquad (x_{\text{arg}}\!:\!A_{\text{env}}\times\mathsf{Cl}\ (A)\ \bot).\\
&\qquad \mathsf{let}\ x_{\text{env}}=\mathsf{sel}[\mathsf{ltPrf}\ \widehat{0}\ \widehat{2}](x_{\text{arg}},\overline{0})\ \mathsf{in}\\
&\qquad \mathsf{let}\ x=\mathsf{sel}[\mathsf{ltPrf}\ \widehat{1}\ \widehat{2}](x_{\text{arg}},\overline{1})\ \mathsf{in}\\
&\qquad \mathsf{let}\ x'=\langle X=A_{\text{env}},\\
&\qquad\qquad \langle v_{\text{fix}}[Y_1]\ldots[Y_m],x_{\text{env}}\rangle\!:\!A_X\rangle\ \mathsf{in}\\
&\qquad \mathsf{let}\ x_0=\mathsf{sel}[\mathsf{ltPrf}\ \widehat{0}\ \widehat{k}](x_{\text{env}},\overline{0})\ \mathsf{in}\ \ldots\\
&\qquad \mathsf{let}\ x_{k-1}=\mathsf{sel}[\mathsf{ltPrf}\ \widehat{k-1}\ \widehat{k}](x_{\text{env}},\overline{k-1})\ \mathsf{in}\ \mathcal{C}_{\text{exp}}[\![e]\!]\\
\mathcal{C}_{\text{exp}}[\![v_1[A_1,\ \ldots A_n](v_2)]\!] &= \mathsf{let}\ \langle X_{\text{env}},\ x_{\text{arg}}\rangle=\mathsf{open}\ \mathcal{C}_{\text{val}}[\![v_1]\!]\ \mathsf{in}\\
&\quad \mathsf{let}\ x_{\text{code}}=\mathsf{sel}[\mathsf{ltPrf}\ \widehat{0}\ \widehat{2}](x_{\text{arg}},\overline{0})\ \mathsf{in}\\
&\quad \mathsf{let}\ x_{\text{env}}=\mathsf{sel}[\mathsf{ltPrf}\ \widehat{1}\ \widehat{2}](x_{\text{arg}},\overline{1})\ \mathsf{in}\\
&\quad x_{\text{code}}[A_1]\ldots[A_n]\ \langle x_{\text{env}},\mathcal{C}_{\text{val}}[\![v_2]\!]\rangle\\
\mathcal{C}_{\text{exp}}[\![\mathsf{let}\ x=v\ \mathsf{in}\ e]\!] &= \mathsf{let}\ x=\mathcal{C}_{\text{val}}[\![v]\!]\ \mathsf{in}\ \mathcal{C}_{\text{exp}}[\![e]\!]\\
\mathcal{C}_{\text{exp}}[\![\mathsf{let}\ x=\mathsf{sel}[A](v,v')\ \mathsf{in}\ e]\!] &=\\
&\quad \mathsf{let}\ x=\mathsf{sel}[A](\mathcal{C}_{\text{val}}[\![v]\!],\mathcal{C}_{\text{val}}[\![v']\!])\ \mathsf{in}\ \mathcal{C}_{\text{exp}}[\![e]\!]\\
\mathcal{C}_{\text{exp}}[\![\mathsf{let}\ \langle X,\ x\rangle=\mathsf{open}\ v\ \mathsf{in}\ e]\!] &=\\
&\quad \mathsf{let}\ \langle X,\ x\rangle=\mathsf{open}\ \mathcal{C}_{\text{val}}[\![v]\!]\ \mathsf{in}\ \mathcal{C}_{\text{exp}}[\![e]\!]\\
\mathcal{C}_{\text{exp}}[\![\mathsf{let}\ x=v_1+v_2\ \mathsf{in}\ e]\!] &= \mathsf{let}\ x=\mathcal{C}_{\text{val}}[\![v_1]\!]+\mathcal{C}_{\text{val}}[\![v_2]\!]\ \mathsf{in}\ \mathcal{C}_{\text{exp}}[\![e]\!]\\
\mathcal{C}_{\text{exp}}[\![\mathsf{let}\ x=v_1<v_2\ \mathsf{in}\ e]\!] &= \mathsf{let}\ x=\mathcal{C}_{\text{val}}[\![v_1]\!]<\mathcal{C}_{\text{val}}[\![v_2]\!]\ \mathsf{in}\ \mathcal{C}_{\text{exp}}[\![e]\!]\\
\mathcal{C}_{\text{exp}}[\![\mathsf{if}[B,A](v,\ X_1.\,e_1,\ X_2.\,e_2)]\!] &=\\
&\quad \mathsf{if}[B,A](\mathcal{C}_{\text{val}}[\![v]\!],\ X_1.\,\mathcal{C}_{\text{exp}}[\![e_1]\!],\ X_2.\,\mathcal{C}_{\text{exp}}[\![e_2]\!])
\end{aligned}
$$

Figure 7: Closure conversion: from λ_K to λ_C.

2. $\Pi Y : B.\, C'$, where $Y \neq X$, X is not free in B, and C' is a well-formed constructor kind for X; or

3. $A \to C'$, where A is strictly positive in X and C' is a well-formed constructor kind for X.

Note that in the definition of $wfc_X(C)$, the second clause covers the case where C is of the form $A \to C'$, and X does not occur free in A. Therefore, we only allow the occurrence of X in the non-dependent case.

In the rest of this paper we often write the well-formed constructor kind for X as $\Pi \vec{Y} : \vec{B}.\, X$. We also denote terms that are strictly positive in X by $\Pi \vec{Y} : \vec{B}.\, X$, where X is not free in $\vec{B}$.

Definition 6 Let C be a well-formed constructor kind for X. Then C is of the form $\Pi \vec{Y} : \vec{A}.\, X$. If all the Y's are t's, that is, C is of the form $\Pi \vec{t} : \vec{A}.\, X$, then we say that C is a small constructor kind (or just small constructor when there is no ambiguity) and denote it as $small(C)$.

Our inductive definitions reside in Kind, whereas a small constructor does not make universal quantification over objects of type Kind. Therefore, an inductive definition with small constructors is a predicative definition. While dealing with impredicative inductive definitions, we must forbid projections on universes equal to or bigger than the one inhabited by the definition. In particular, we restrict large elimination to inductive definitions with only small constructors.

Next, we define the set of reductions on our terms. The definition of β- and η-reduction is standard. The ι-reduction defines primitive recursion over inductive objects.

Definition 7 Let C be a well-formed constructor kind for X and let A', B', and I be pseudoterms. We define $\Phi_{X,I,B'}(C, A')$ recursively based on the structure of C:

$$\begin{array}{ll}
\Phi_{X,I,B'}(X, A') & \stackrel{\text{def}}{=} A' \\
\Phi_{X,I,B'}(\Pi Y : B.\, C', A') & \stackrel{\text{def}}{=} \lambda Y : B.\, \Phi_{X,I,B'}(C', A'\ Y) \\
\Phi_{X,I,B'}((\Pi \vec{Y} : \vec{B}.\, X) \to C', A') & \stackrel{\text{def}}{=} \\
\quad \lambda Z : (\Pi \vec{Y} : \vec{B}.\, I).\, \Phi_{X,I,B'}(C', A'\ Z\ (\lambda \vec{Y} : \vec{B}.\, B'\ (Z\ \vec{Y}))) &
\end{array}$$

Definition 8 The reduction relations on our terms are defined as:

$$\begin{array}{rcl}
(\lambda X : A.\, B)\ A' & \leadsto_\beta & [A'/X]B \\
\lambda X : A.\, (B\ X) & \leadsto_\eta & B, \quad \text{if } X \notin FV(B) \\
\mathsf{Elim}[I, A'']([\mathsf{Ctor}\,(i, I)\ \vec{A}]\{\vec{B}\} & \leadsto_\iota & (\Phi_{X,I,B'}(C_i, B_i))\ \vec{A} \\
\text{where } \begin{array}{r} I \\ B' \end{array} & \begin{array}{l} = \mathsf{Ind}(X : \mathsf{Kind})\{\vec{C}\} \\ = \lambda Y : I.\, (\mathsf{Elim}[I, A''](Y)\{\vec{B}\}) \end{array} &
\end{array}$$

By $\rhd_\beta$, $\rhd_\eta$, and $\rhd_\iota$ we denote the relations that correspond to the rewriting of subterms using the relations $\leadsto_\beta$, $\leadsto_\eta$, and $\leadsto_\iota$ respectively. We use $\leadsto$ and $\rhd$ for the unions of the above relations. We also write $\rhd^*$ and $\rhd^+$ (respectively $\rhd^*_\beta$ etc.) for the reflexive-transitive and transitive closures of $\rhd$ (respectively $\rhd_\beta$ etc.) and $=_{\beta\eta\iota}$ for the reflexive-symmetric-transitive closure of $\rhd$. We say that a sequence of terms $A_1, \ldots, A_n$, such that $A \rhd A_1 \rhd A_2 \ldots \rhd A_n$, is a chain of reductions starting from A.

Let us examine the ι-reduction in detail. In $\mathsf{Elim}[I, A''](A)\{\vec{B}\}$, the term A of type I is being analyzed. The sequence $\vec{B}$ contains the set of branches for Elim, one for each constructor of I. In the case when $C_i = X$, which implies that A is of the form $\mathsf{Ctor}\,(i, I)$, the Elim just selects the B_i branch:

$$\mathsf{Elim}[I, A''](\mathsf{Ctor}\,(i, I))\{\vec{B}\} \quad \leadsto_\iota \quad B_i$$

In the case when $C_i = \Pi \vec{Y} : \vec{B}.\, X$ where X does not occur free in $\vec{B}$, then A must be in the form $\mathsf{Ctor}\,(i, I)\ \vec{A}$ with A_i of type B_i. None of the arguments are recursive. Therefore, the Elim should just select the B_i branch and pass the constructor arguments to it. Accordingly, the reduction yields (by expanding the Φ macro):

$$\mathsf{Elim}[I, A''](\mathsf{Ctor}\,(i, I)\ \vec{A})\{\vec{B}\} \quad \leadsto_\iota \quad B_i\ \vec{A}$$

The recursive case is the most interesting. For simplicity assume that the i-th constructor has the form $\Pi \vec{Y} : \vec{B'}.\, X \to \Pi \vec{Y'} : \vec{B''}.\, X$. Therefore, A is of the form $\mathsf{Ctor}\,(i, I)\ \vec{A}$ with A_1 being the recursive component of type $\Pi \vec{Y} : \vec{B'}.\, X$, and $A_2 \ldots A_n$ being non-recursive. The reduction rule then yields:

$$\begin{array}{l}
\mathsf{Elim}[I, A''](\mathsf{Ctor}\,(i, I)\ \vec{A})\{\vec{B}\} \\
\quad \leadsto_\iota B_i\ A_1\ (\lambda \vec{Y} : \vec{B'}.\, \mathsf{Elim}[I, A''](A_1\ \vec{Y})\{\vec{B}\})\ A_2 \ldots A_n
\end{array}$$

The Elim construct selects the B_i branch and passes the arguments $A_1, \ldots, A_n$, and the result of recursively processing A_1. In the general case, it would process each recursive argument.

Definition 9 defines the Ψ macro which represents the type of the large Elim branches. Definition 10 defines the ζ macro which represents the type of the small elimination branches. The different cases follow from the ι-reduction rule in Definition 8.

Definition 9 Let C be a well-formed constructor kind for X and let A' and I be two terms. We define $\Psi_{X,I}(C, A')$ recursively based on the structure of C:

$$\begin{array}{ll}
\Psi_{X,I}(X, A') & \stackrel{\text{def}}{=} A' \\
\Psi_{X,I}(\Pi Y : B.\, C', A') & \stackrel{\text{def}}{=} \Pi Y : B.\, \Psi_{X,I}(C', A') \\
\Psi_{X,I}(A \to C', A') & \stackrel{\text{def}}{=} [I/X]A \to [A'/X]A \to \Psi_{X,I}(C', A')
\end{array}$$

where X is not free in B and A is strictly positive in X.

Definition 10 Let C be a well-formed constructor kind for X and let A', I, and B' be terms. We define $\zeta_{X,I}(C, A', B')$ recursively based on the structure of C:

$$\begin{array}{ll}
\zeta_{X,I}(X, A', B') & \stackrel{\text{def}}{=} A'\ B' \\
\zeta_{X,I}(\Pi Y : B.\, C', A', B') & \stackrel{\text{def}}{=} \Pi Y : B.\, \zeta_{X,I}(C', A', B'\ Y) \\
\zeta_{X,I}(\Pi \vec{Y} : \vec{B}.\, X \to C', A', B') & \stackrel{\text{def}}{=} \\
\quad \Pi Z : (\Pi \vec{Y} : \vec{B}.\, I).\, \Pi \vec{Y} : \vec{B}.\, (A'\ (Z\ \vec{Y})) \to \zeta_{X,I}(C', A', B'\ Z) &
\end{array}$$

where X is not free in B and $\vec{B}$.

Definition 11 We use $\Delta|_{t,k}$ to denote that the environment does not contain any z variables.

Here are the complete typing rules for TL. The three weakening rules make sure that all variables are bound to the right classes of terms in the context. There are no separate context-formation rules; a context Δ is well-formed if we can derive the judgment $\Delta \vdash \mathsf{Kind} : \mathsf{Kscm}$ (notice we can only add new variables to the context via the weakening rules).

$$\cdot \vdash \mathsf{Kind} : \mathsf{Kscm} \qquad (\text{AX1})$$

$$\cdot \vdash \mathsf{Kscm} : \mathsf{Ext} \qquad (\text{AX2})$$

$$\frac{\Delta \vdash C : \mathsf{Kind} \quad \Delta \vdash A : B \quad t \notin Dom(\Delta)}{\Delta, t : C \vdash A : B} \qquad (\text{WEAK1})$$

$$\frac{\Delta \vdash C : \mathsf{Kscm} \quad \Delta \vdash A : B \quad k \notin Dom(\Delta)}{\Delta, k{:}C \vdash A : B} \quad (\text{WEAK2})$$

$$\frac{\Delta \vdash C : \mathsf{Ext} \quad \Delta \vdash A : B \quad z \notin Dom(\Delta)}{\Delta, z{:}C \vdash A : B} \quad (\text{WEAK3})$$

$$\frac{\Delta \vdash \mathsf{Kind} : \mathsf{Kscm} \qquad X \in Dom(\Delta)}{\Delta \vdash X : \Delta(X)} \quad (\text{VAR})$$

$$\frac{\Delta, X{:}A \vdash B : B' \qquad \Delta \vdash \Pi X{:}A.\, B' : s}{\Delta \vdash \lambda X{:}A.\, B : \Pi X{:}A.\, B'} \quad (\text{FUN})$$

$$\frac{\Delta \vdash A : \Pi X{:}B'.\, A' \quad \Delta \vdash B : B'}{\Delta \vdash A\ B : [B/X]A'} \quad (\text{APP})$$

$$\frac{\Delta \vdash A : s_1 \quad \Delta, X{:}A \vdash B : s_2 \quad (s_1, s_2) \in \mathcal{R}}{\Delta \vdash \Pi X{:}A.\, B : s_2} \quad (\text{PROD})$$

$$\frac{\textit{for all } i \qquad \Delta, X{:}\mathsf{Kind} \vdash C_i : \mathsf{Kind} \qquad wfc_X(C_i)}{\Delta \vdash \mathsf{Ind}(X{:}\mathsf{Kind})\{\vec{C}\} : \mathsf{Kind}} \quad (\text{IND})$$

$$\frac{\Delta \vdash I : \mathsf{Kind} \textit{ where } I = \mathsf{Ind}(X{:}\mathsf{Kind})\{\vec{C}\}}{\Delta \vdash \mathsf{Ctor}\,(i, I) : [I/X]C_i} \quad (\text{CON})$$

$$\frac{\begin{array}{c}\Delta \vdash A : I \qquad \Delta \vdash A' : I \to \mathsf{Kind} \\ \textit{for all } i \qquad \Delta \vdash B_i : \zeta_{X,I}(C_i, A', \mathsf{Ctor}\,(i, I))\end{array}}{\begin{array}{c}\Delta \vdash \mathsf{Elim}[I, A'](A)\{\vec{B}\} : A'\ A \\ \textit{where } I = \mathsf{Ind}(X{:}\mathsf{Kind})\{\vec{C}\}\end{array}} \quad (\text{ELIM})$$

$$\frac{\begin{array}{c}\Delta \vdash A : I \qquad \Delta|_{t,k} \vdash A' : \mathsf{Kscm} \\ \textit{for all } i \quad small(C_i) \quad \Delta \vdash B_i : \Psi_{X,I}(C_i, A')\end{array}}{\begin{array}{c}\Delta \vdash \mathsf{Elim}[I, A'](A)\{\vec{B}\} : A' \\ \textit{where } I = \mathsf{Ind}(X{:}\mathsf{Kind})\{\vec{C}\}\end{array}} \quad (\text{L-ELIM})$$

$$\frac{\begin{array}{c}\Delta \vdash A : B \\ \Delta \vdash B' : s \qquad \Delta \vdash B : s \qquad B =_{\beta\eta\iota} B'\end{array}}{\Delta \vdash A : B'} \quad (\text{CONV})$$

D.2 Subject Reduction

The proof is structured as follows:

- We first define a calculus of unmarked terms. These are terms with no annotations at lambda abstractions. We show that this language is confluent.
- We then prove Geuvers' lemma – a weak form of confluence. It says that a term that is equal to one in head normal form can be reduced to an η-expanded version of this head normal form.
- From Geuvers' lemma, we are able to prove the inversion lemma which relates the structure of a term to its typing derivation.
- We are then able to prove the uniqueness of types and subject reduction for $\beta\iota$ reduction.
- We are then able to prove that the system preserves sorts – that is, if two terms are convertible and well sorted, then they have the same sort.
- Finally, we prove the strengthening lemma and then subject reduction for η reduction.

D.2.1 Unmarked terms

The PTS language is non-confluent. Nederpelt gave the following counterexample – let A be the term defined by $\lambda X : A_1.\, (\lambda Y : A_2.\, Y)X$. Then we have that $A \rhd_\beta \lambda X : A_1.\, X$ and $A \rhd_\eta \lambda Y : A_2.\, Y$. For our proofs we want to operate in a language that is confluent. We will therefore introduce the notion of unmarked terms. As non-confluence is due to the presence of type annotations in λ abstractions, the unmarked terms are obtained by erasing the type annotations.

The set of unmarked terms $\| A \|$ are defined below. We are given a marked variable _ that can not be used elsewhere.

$$\begin{array}{rl}
\| s \| &= s \\
\| X \| &= X \\
\| A_1\ A_2 \| &= \| A_1 \|\ \| A_2 \| \\
\| \lambda X : A_1.\, A_2 \| &= \lambda X : _.\, \| A_2 \| \\
\| \Pi X : A_1.\, A_2 \| &= \Pi X : \| A_1 \|\, .\, \| A_2 \| \\
\| \mathsf{Ind}(X{:}\mathsf{Kind})\{\vec{A}\} \| &= \mathsf{Ind}(X{:}\mathsf{Kind})\{\overrightarrow{\| A \|}\} \\
\| \mathsf{Ctor}\,(i, A_1) \| &= \mathsf{Ctor}\,(i, \| A_1 \|) \\
\| \mathsf{Elim}[I, A_2](A_1)\{\vec{A}\} \| &= \mathsf{Elim}[\| I \|, \| A_2 \|](\| A_1 \|)\{\overrightarrow{\| A \|}\}
\end{array}$$

Lemma 6 For all terms A, B, A', B', and for all variables X and Y, we have that $[\lambda Y : A'.\, B/X]A =_{\beta\eta\iota} [\lambda Y : B'.\, B/X]A$.

Proof Consider $A_2 = [\lambda Z : A'.\, (\lambda Y : B'.\, B)\ Z/X]A$. Then $A_2 \rhd_\beta [(\lambda Z : A'.\, [Z/Y]B)/X]A$ and $A_2 \rhd_\eta [\lambda Y : B'.\, B/X]A$. Alpha converting the first reduct leads to the required result. □

Lemma 7 For all terms A, we have $A =_{\beta\eta} \| A \|$.

Proof Follows from lemma 6. □

Definition 12 (ι_0 reduction) We say that $A \rhd_{\iota_0} \| A' \|$ iff $A \rhd_\iota A'$ and $\| A \| \neq \| A' \|$.

Proposition 13 For all terms A and A', if $A \rhd_\beta A'$, then $\| A \| \rhd_\beta \| A' \|$ or $\| A \| = \| A' \|$. Similarly, if we have that $A \rhd_\iota A'$, then $\| A \| \rhd_{\iota_0} \| A' \|$ or $\| A \| = \| A' \|$. Moreover, if $\| A \| \rhd_{\beta\iota_0} \| A' \|$, then there exists a A'' such that $A \rhd_{\beta\iota} A''$ and $\| A'' \| = \| A' \|$.

Lemma 8 (Confluence for unmarked terms) For all unmarked terms $\| A \|$, the $\beta\eta\iota_0$ reduction is confluent.

The proof is based on the method of parallel reductions due to Tait and Martin-Löf.

Definition 14 (Parallel reduction) Define $\twoheadrightarrow$ on unmarked terms as below, in which we assume that $A \twoheadrightarrow A'$, $B \twoheadrightarrow B'$, etc:

$$\begin{array}{rl}
A &\twoheadrightarrow A \\
A\ B &\twoheadrightarrow A'\ B' \\
\lambda X : _.\, A &\twoheadrightarrow \lambda X : _.\, A' \\
\Pi X : A.\, B &\twoheadrightarrow \Pi X : A'.\, B' \\
\mathsf{Ind}(X{:}\mathsf{Kind})\{\vec{A}\} &\twoheadrightarrow \mathsf{Ind}(X{:}\mathsf{Kind})\{\vec{A'}\} \\
\mathsf{Ctor}\,(i, I) &\twoheadrightarrow \mathsf{Ctor}\,(i, I') \\
\mathsf{Elim}[A, C](I)\{\vec{A}\} &\twoheadrightarrow \mathsf{Elim}[A', C'](I')\{\vec{A'}\} \\
(\lambda X : _.\, A)\ B &\twoheadrightarrow [B'/X]A' \\
\lambda X : _.\, A\ X &\twoheadrightarrow A' \text{ if } X \notin FV(A) \\
\mathsf{Elim}[I, C]((\mathsf{Ctor}\,(i, I)\ \vec{B}))\{\vec{A}\} &\twoheadrightarrow (\Phi_{X,I',B'}(C'_i, A'_i))\ \vec{B'} \\
\textit{where}\quad I &= \mathsf{Ind}(X{:}\mathsf{Kind})\{\vec{C}\} \\
B' &= \lambda Y : _.\, (\mathsf{Elim}[I', C'](Y)\{\vec{A'}\})
\end{array}$$

The parallel reduction commutes with respect to substitution.

Lemma 9 If $A \twoheadrightarrow A'$ and $B \twoheadrightarrow B'$, then $[B/X]A \twoheadrightarrow [B'/X]A'$.

Proof By induction over the fact that $A \twoheadrightarrow A'$. □

The parallel reduction also has the following properties with respect to terms such as products and inductive definitions. The proof in each case is immediate and follows by induction over the structure of the term.

Proposition 15 Suppose $A = \Pi X : \vec{B}.\, Y\ \vec{C}$. If A can be reduced to A' through a reduction relation ($\twoheadrightarrow$, $\rhd_\beta$, etc.), then $A' = \Pi X : \vec{B'}.\, Y\ \vec{C'}$ where all the $\vec{B}$ and $\vec{C}$ can be reduced to $\vec{B'}$ and $\vec{C'}$ by the same reduction relation.

Proposition 16 Suppose $A = \Pi X : \vec{B}.\, Y\ \vec{C}$ and $A' = \Pi X : \vec{B'}.\, Y\ \vec{C'}$ be two terms such that both can be reduced to A'' through a reduction relation ($\twoheadrightarrow$, $\rhd_\beta$, etc.). Then $A'' = \Pi X : \vec{B''}.\, Y\ \vec{C''}$ where $\vec{B}$ and $\vec{B'}$ can be reduced to $\vec{B''}$ by the same relation and $\vec{C}$ and $\vec{C'}$ can be reduced to $\vec{C''}$ by the same relation.

The parallel reduction is important because it subsumes the single step reduction; that is, if $A \rhd A'$, then we have that $A \twoheadrightarrow A'$ which also implies that $A \rhd^* A'$. From here, to show the confluence of $\rhd$, it suffices to show the confluence of parallel reduction.

Lemma 10 For all unmarked terms D, D', D'', we have that if $D \twoheadrightarrow D'$ and $D \twoheadrightarrow D''$, then there exists a D''' such that $D' \twoheadrightarrow D'''$ and $D'' \twoheadrightarrow D'''$.

Proof The proof is by induction over the structure of D. We will only show one case here.

- Suppose $D = \mathsf{Elim}[I, C]((\mathsf{Ctor}\,(i, I)\ \vec{B}))\{\vec{A}\}$.
  - We can then have $D' = (\Phi_{X,I',B'}(C_i', A_i'))\ \vec{B'}$ and $D'' = (\Phi_{X,I'',B'}(C_i'', A_i''))\ \vec{B''}$. We have that $I' = \mathsf{Ind}(X : \mathsf{Kind})\{\vec{C'}\}$ and $I'' = \mathsf{Ind}(X : \mathsf{Kind})\{\vec{C''}\}$. This implies that $C_i \twoheadrightarrow C_i'$ and $C_i \twoheadrightarrow C_i''$. By applying the induction hypothesis to the subterms, we get that $I' \twoheadrightarrow I'''$ and $I'' \twoheadrightarrow I'''$ and so on for the other subterms. From here and proposition 16, it follows that we can take $D''' = (\Phi_{X,I''',B'}(C_i''', A_i'''))\ \vec{B'''}$.
  - Suppose $D' = \mathsf{Elim}[I', C']((\mathsf{Ctor}\,(i, I')\ \vec{B'}))\{\vec{A'}\}$ and $D'' = (\Phi_{X,I'',B'}(C_i'', A_i''))\ \vec{B''}$. As above we can again define I''', C_i''', etc. and take $D''' = (\Phi_{X,I''',B'}(C_i''', A_i'''))\ \vec{B'''}$.
  - Also $D' = \mathsf{Elim}[I', C']((\mathsf{Ctor}\,(i, I')\ \vec{B'}))\{\vec{A'}\}$ and $D'' = \mathsf{Elim}[I'', C'']((\mathsf{Ctor}\,(i, I'')\ \vec{B''}))\{\vec{A''}\}$. In this case, we can again take that $D''' = \mathsf{Elim}[I''', C''']((\mathsf{Ctor}\,(i, I''')\ \vec{B'''}))\{\vec{A'''}\}$.

□

As a corollary of the confluence of unmarked terms we get the following:

Corollary 17 If A and B are two distinct sorts or two distinct variables or a variable and a sort, then we have that $A \neq B$.

We will need another lemma – that of the delay of η reduction. But before that, we have to define another variant of the ι reduction. This essentially says that a ι reduction that would appear only after a series of eta reductions can be reduced straightaway without going through the eta reductions. For well typed terms, this is equivalent to ι reduction, but it also allows us to retain the property of delay of η reduction for ill-typed terms.

$$\mathsf{Elim}[I, A''](\lambda \vec{X} : \vec{A'}.\, (\mathsf{Ctor}\,(i, I)\ \vec{A})\vec{C'})\{\vec{B}\} \rhd_{\iota'} (\Phi_{X,I,B'}(C_i, B_i))\ \vec{A}$$

where $I = \mathsf{Ind}(X : \mathsf{Kind})\{\vec{C}\}$
$B' = \lambda Y : I.\, (\mathsf{Elim}[I, A''](Y)\{\vec{B}\})$
$C_i' \rhd_\eta X_i$ and $X_i \notin FV(\vec{A}) \cup FV(I)$

Proposition 18 For all terms A_1 and A_2, we have that $A_1 =_{\beta\eta\iota} A_2$ if and only if $A_1 =_{\beta\eta\iota'} A_2$.

Lemma 11 If $A \rhd_\eta A' \rhd_{\beta\iota'} A''$, then either $A \rhd^*_{\beta\iota'} A''$, or there exists a A''' such that $A \rhd_{\beta\iota'} A''' \rhd^*_\eta A''$.

Proof The proof is by induction over the structure of A. We will consider only the cases that do not follow directly from the induction hypothesis.

- $A = C\ D$. There are two cases.
  - If $C \rhd_\eta C'$, then it follows immediately from the induction hypothesis.
  - If $D \rhd_\eta D'$ and $C = \lambda X : B.\, B'$ and $A'' = [D'/X]B'$, then take $A''' = [D/X]B'$. The other cases follow from the induction hypothesis.
- $A = \lambda X : C.\, B\ X$. Suppose $A'' = B'$ where $B \rhd_{\beta\iota'} B'$. But then we also have that $A \rhd_{\beta\iota'} \lambda X : C.\, B'\ X$. Since the reduction does not introduce new free variables, this term can now η-reduce to B'.

□

Lemma 12 (Delay of η reduction) For all terms A and A', if $A \rhd^* A'$, then there exists a term A'' such that $A \rhd^*_{\beta\iota'} A'' \rhd^*_\eta A'$.

Proof Follows from lemma 11. □

We will next prove Geuvers' lemma which is essentially a weak form of confluence. This is enough to prove the uniqueness of types and subject reduction. But before that we need to define the counterpart of the ι' reduction for unmarked terms. We define it in the obvious way

Definition 19 (ι'_0 reduction) We say that $A \rhd_{\iota'_0} \| A' \|$ iff $A \rhd_{\iota'} A'$ and $\| A \| \neq \| A' \|$.

As before it has the following property:

Proposition 20 Suppose $A \rhd_{\iota'} A'$. Then either $\| A \| = \| A' \|$, or $\| A \| \rhd_{\iota'_0} \| A' \|$. Moreover, if $\| A \| \rhd_{\iota'_0} \| A' \|$, then $A \rhd_{\iota'} A'$.

Lemma 13 (Geuvers lemma)

- If $A =_{\beta\eta\iota} X\ \vec{A}$, then
$$A \rhd^*_{\beta\iota'} \lambda \vec{Y} : \vec{A'}.\, (X\ \vec{B}\ \vec{C})$$
where for all i, $A_i =_{\beta\eta\iota} B_i$ and for all j, $C_j \rhd^*_\eta Y_j$.
- If $A =_{\beta\eta\iota} \Pi X : A_1.\, A_2$, then
$$A \rhd^*_{\beta\iota'} \lambda \vec{Y} : \vec{A'}.\, ((\Pi X : A_3.\, A_4)\ \vec{B})$$
where $A_1 =_{\beta\eta\iota} A_3$ and $A_2 =_{\beta\eta\iota} A_4$ and for all i, $B_i \rhd^*_\eta Y_i$.

- If $A =_{\beta\eta\iota} \mathsf{Ctor}\ (i, I)\ \vec{C}$, then

$$A \rhd^*_{\beta\iota'} \lambda\vec{Y} : \vec{A'}.\ ((\mathsf{Ctor}\ (i, I')\ \vec{C'})\ \vec{B})$$

where for all i, $C_i =_{\beta\eta\iota} C'_i$ and for all j, $B_j \rhd^*_\eta Y_j$, and $I =_{\beta\eta\iota} I'$.

- If $A =_{\beta\eta\iota} \mathsf{Ind}(X : \mathsf{Kind})\{\vec{A}\}\ \vec{C}$, then

$$A \rhd^*_{\beta\iota'} \lambda\vec{Y} : \vec{A'}.\ ((\mathsf{Ind}(X : \mathsf{Kind})\{\vec{A''}\})\ \vec{C'})\ \vec{B}$$

where for all i, $A_i =_{\beta\eta\iota} A''_i$ and for all j, $C_j =_{\beta\eta\iota} C'_j$, and for all k, $B_k \rhd^*_\eta Y_k$.

- If $A =_{\beta\eta\iota} \mathsf{Elim}[I, A_2](A_1)\{\vec{A''}\}\ \vec{C}$, then

$$A \rhd^*_{\beta\iota'} \lambda\vec{Y} : \vec{A'}.\ (\mathsf{Elim}[I', B'](B)\{\vec{B}\}\ \vec{C'})\ \vec{B'}$$

where $A_1 =_{\beta\eta\iota} B$, and $A_2 =_{\beta\eta\iota} B'$, and $I =_{\beta\eta\iota} I'$, and for all i, $A''_i =_{\beta\eta\iota} B_i$ and for all j, $C_j =_{\beta\eta\iota} C'_j$ and for all k, $B'_k \rhd^*_\eta Y_k$.

Proof The proof for each of the cases is similar and is by induction over the length of the equivalence relation. We will show only one case here.

- Suppose $A =_{\beta\eta\iota} X\ \vec{A}$. By the induction hypothesis, there exists an A'' such that

$$A'' \rhd^*_{\beta\iota'} \lambda\vec{Y} : \vec{A'}.\ (X\ \vec{B}\ \vec{C})$$

and $A\ \rhd_{\beta\iota}\ A''$ or $A''\ \rhd_{\beta\iota}\ A$.

  - The case where $A\ \rhd_{\beta\iota}\ A''$ is immediate.
  - The case where $A\ \rhd_\eta\ A''$ follows from the lemma of delay of η-reduction.
  - If $A''\ \rhd_{\beta\iota}\ A$, then the required result follows from the confluence of $\beta\iota'$ reduction.
  - Suppose $A''\ \rhd_\eta\ A$. Then from the confluence of $\beta\eta\iota'_0$ reduction on unmarked terms, we get that $\| A \| \rhd^* X\ \vec{D}$ where $\| B_i \|\ \rhd_{\beta\eta\iota'_0} D_i$. From the lemma of delay of η-reduction, we get that

$$\| A \| \rhd^*_{\beta\iota'_0} \lambda\vec{Y} : _.\ X\ \vec{D'}\vec{F} \rhd^*_\eta X\ \vec{D}$$

From proposition 20 we can deduce the existence of a term A_1 such that $A \rhd^*_{\beta\iota'} A_1$ and $\| A_1 \| = \lambda\vec{Y} : _.\ X\ \vec{D'}\vec{F}$. The required result follows from here.

□

D.2.2 Classification of terms

Definition 21 We partition the set of terms into four classes: the set of types Ty, the set of kinds Ki, the set of kind schemas Sc, and Ex. The class of a term is defined as follows:

$$\begin{aligned}
\mathsf{Cls}(\mathsf{Kind}) &= \mathsf{Sc} \\
\mathsf{Cls}(\mathsf{Kscm}) &= \mathsf{Ex} \\
\mathsf{Cls}(t) &= \mathsf{Ty} \\
\mathsf{Cls}(k) &= \mathsf{Ki} \\
\mathsf{Cls}(z) &= \mathsf{Sc} \\
\mathsf{Cls}(A_1\ A_2) &= \mathsf{Cls}(A_1) \\
\mathsf{Cls}(\lambda X : A_1.\ A_2) &= \mathsf{Cls}(A_2) \\
\mathsf{Cls}(\Pi X : A_1.\ A_2) &= \mathsf{Cls}(A_2) \\
\mathsf{Cls}(\mathsf{Ind}(X : \mathsf{Kind})\{\vec{A}\}) &= \mathsf{Ki} \\
\mathsf{Cls}(\mathsf{Ctor}\ (i, A_1)) &= \mathsf{Ty} \\
\mathsf{Cls}(\mathsf{Elim}[I, A_2](A_1)\{\vec{A}\}) &= \mathsf{Ty} \quad \text{if } \mathsf{Cls}(A_2) = \mathsf{Ki}, \text{ else Ki}
\end{aligned}$$

We also define the following function:

$$\begin{aligned}
\mathsf{lift}(\mathsf{Ty}) &= \mathsf{Ki} \\
\mathsf{lift}(\mathsf{Ki}) &= \mathsf{Sc} \\
\mathsf{lift}(\mathsf{Sc}) &= \mathsf{Ex}
\end{aligned}$$

Lemma 14 If $\Delta \vdash A_1 : A_2$ is derivable, then we have $\mathsf{lift}(\mathsf{Cls}(A_1)) = \mathsf{Cls}(A_2)$. In particular, $A_1 \neq \mathsf{Ext}$. Moreover, for all pairs (X, A) in Δ, we have $\mathsf{Cls}(A) = \mathsf{lift}(\mathsf{Cls}(X))$.

Proof Immediate by induction over the derivation of the judgment. □

D.2.3 Well typed terms

We now consider the well typed terms. The following lemmas are proved easily by induction over the typing derivations.

Lemma 15 (Substitution) If we can derive $\Delta_1, (X, A), \Delta_2 \vdash B : C$ and $\Delta_1 \vdash A_2 : A$, then we can derive $\Delta_1, ([A_2/X]\Delta_2) \vdash [A_2/X]B : [A_2/X]C$.

Proof Straightforward induction over the structure of the derivation. □

Lemma 16 If we can derive $\Delta_1, (X, A), \Delta_2 \vdash B : C$, then we also have that $\Delta_1 \vdash A : s$ for some sort s. Moreover, we also have that $\Delta_1, (X, A), \Delta_2 \vdash A : s$.

Proof The proof is by induction over the structure of the derivation. □

Lemma 17 If we have that $\Delta \vdash \Pi X : A.\ B : s$, then we have that $\Delta, X : A \vdash B : s$.

Proof The only interesting case is for the CONV case which follows from Corollary 17. □

Lemma 18 If the judgment $\Delta \vdash A : B$ is derivable, then either $B = \mathsf{Ext}$, or $\Delta \vdash B : s$ for some sort s.

Proof The proof is a straightforward induction over the structure of the derivation. □

Lemma 19 (Inversion) If the judgment $\Delta \vdash A : B$ is derivable,

then

$$
\begin{array}{lll}
A = t & \Rightarrow & t \in \Delta \\
 & & B =_{\beta\eta\iota} \Delta(t) \\
 & & \Delta \vdash B : \mathsf{Kind} \\
A = k & \Rightarrow & k \in \Delta \\
 & & B =_{\beta\eta\iota} \Delta(k) \\
 & & \Delta \vdash B : \mathsf{Kscm} \\
A = z & \Rightarrow & z \in \Delta \\
 & & B =_{\beta\eta\iota} \Delta(z) \\
 & & \Delta \vdash B : \mathsf{Ext} \\
A = \mathsf{Kind} & \Rightarrow & B =_{\beta\eta\iota} \mathsf{Kscm} \\
A = \mathsf{Kscm} & \Rightarrow & B = \mathsf{Ext} \\
A = \Pi X\!:\!A_1.\, A_2 & \Rightarrow & \Delta \vdash A_1 : s_1 \\
 & & \Delta, X\!:\!A_1 \vdash A_2 : s_2 \\
 & & B =_{\beta\eta\iota} s_2 \\
 & & \text{where } s_1 \text{ is any sort and} \\
 & & s_2 = \mathsf{Kind}, \text{ or} \\
 & & s_1 \in \{\mathsf{Kind}, \mathsf{Kscm}\} \text{ and} \\
 & & s_2 = \mathsf{Kscm} \\
A = \lambda X\!:\!A_1.\, A_2 & \Rightarrow & \Delta \vdash A_1 : s_1 \\
 & & \Delta, X\!:\!A_1 \vdash A_2 : A_3 \\
 & & \Delta \vdash A_3 : s_2 \\
 & & B =_{\beta\eta\iota} \Pi X\!:\!A_1.\, A_3 \\
 & & \Delta \vdash B : s_2 \\
A = A_1\ A_2 & \Rightarrow & \Delta \vdash A_1 : \Pi X\!:\!B'.\, A' \\
 & & \Delta \vdash A_2 : B' \\
 & & B =_{\beta\eta\iota} [A_2/X]A' \\
A = \mathsf{Ind}(X\!:\!\mathsf{Kind})\{\vec{A}\} & \Rightarrow & \Delta, X\!:\!\mathsf{Kind} \vdash A_i : \mathsf{Kind} \\
 & & wfc_X(A_i) \\
 & & B =_{\beta\eta\iota} \mathsf{Kind} \\
A = \mathsf{Ctor}\,(i, I) & \Rightarrow & I = \mathsf{Ind}(X\!:\!\mathsf{Kind})\{\vec{A}\} \\
 & & \text{same conditions on } I \\
 & & B =_{\beta\eta\iota} [I/X]A_i \\
A = \mathsf{Elim}[I, A'](A)\{\vec{B}\} & \Rightarrow & I = \mathsf{Ind}(X\!:\!\mathsf{Kind})\{\vec{A}\} \\
 & & \text{same conditions on } I \\
 & & \Delta \vdash A : I \\
 & & \Delta \vdash A' : I \to \mathsf{Kind} \\
 & & \Delta \vdash B : \mathsf{Kind}\ \ B =_{\beta\eta\iota} A'\ A \\
 & & \Delta \vdash B_i : \\
 & & \qquad \zeta_{X,I}(A_i, A', \mathsf{Ctor}\,(i, I)) \\
A = \mathsf{Elim}[I, A'](A)\{\vec{B}\} & \Rightarrow & I = \mathsf{Ind}(X\!:\!\mathsf{Kind})\{\vec{A}\} \\
 & & \text{same conditions on } I \\
 & & \Delta \vdash A : I \\
 & & \Delta \vdash A' : \mathsf{Kscm} \\
 & & \Delta \vdash B : \mathsf{Kscm} \text{ and } B =_{\beta\eta\iota} A' \\
 & & \Delta \vdash B_i : \Psi_{X,I}(A_i, A') \\
 & & \mathit{for\ all}\ i\ \ \mathit{small}(A_i)
\end{array}
$$

Proof By induction over the structure of the derivation. For every case we consider the set of possible typing derivations. □

Lemma 20 (Uniqueness of types) If $\Delta \vdash A : A_1$ and $\Delta \vdash A : A_2$, then $A_1 =_{\beta\eta\iota} A_2$.

Proof By induction over the structure of A. We use the fact that if $A_1 =_{\beta\eta\iota} B$ and $A_2 =_{\beta\eta\iota} B$, then $A_1 =_{\beta\eta\iota} A_2$. For every case, we use the corresponding clause from lemma 19. □

Corollary 22 Suppose A is a well typed term. If $A \rhd_{\iota'} A'$, then $A \rhd_{\iota} A'$.

D.2.4 Reductions on well typed terms

Lemma 21 (Subject reduction for $\beta\iota$ reduction) If the judgment $\Delta \vdash A : B$ is derivable, and if $A \rhd_{\beta\iota} A'$ and $\Delta \rhd_{\beta\iota} \Delta'$, then we have that

$$\Delta \vdash A' : B \qquad \Delta' \vdash A : B$$

Proof The interesting cases are the APP and ELIM.

- APP When only the sub-terms reduce without a reduction at the head, the lemma follows by using the induction hypothesis on the sub-terms. Suppose that

  $$A = \lambda X\!:\!A_1.\, A_2 \qquad \frac{\Delta \vdash A : \Pi X\!:\!B'.\, A' \quad \Delta \vdash B : B'}{\Delta \vdash A\ B : [B/X]A'}$$

  and $A\ B \rhd_{\beta} [B/X]A_2$. We know from lemma 19 that

  $$\begin{array}{l} \Delta, X\!:\!A_1 \vdash A_2 : A_3 \\ \Pi X\!:\!A_1.\, A_3 =_{\beta\eta\iota} \Pi X\!:\!B'.\, A' \\ \Delta \vdash A_1 : s_1 \\ \Delta \vdash B' : s_2 \end{array}$$

  This implies that $A_1 =_{\beta\eta\iota} B'$ and $A_3 =_{\beta\eta\iota} A'$. Moreover,

  $$\mathsf{Cls}(B') = \mathsf{Cls}(A_1) = \mathsf{lift}(\mathsf{Cls}(X))$$

  Therefore, we get from lemma 14 that

  $$\mathsf{Cls}(s_2) = \mathsf{Cls}(s_1) \quad \Rightarrow s_2 = s_1$$

  Applying the CONV rule we get that $\Delta \vdash B : A_1$. By lemma 15 we get that $\Delta \vdash [B/X]A_2 : [B/X]A_3$. We can show in a similar manner as before that $\mathsf{Cls}(A_3) = \mathsf{Cls}(A')$. This allows us to apply the CONV rule again which leads to the required result.

- L-ELIM We will only consider the case when an ι reduction takes place at the head. The other cases follow easily by structural induction.

  $$\frac{\Delta \vdash A : I \quad \Delta \vdash A' : \mathsf{Kscm} \quad \mathit{for\ all}\ i \quad \Delta \vdash B_i : \Psi_{X,I}(C_i, A')}{\Delta \vdash \mathsf{Elim}[I, A'](A)\{\vec{B}\} : A'}$$
  $$\mathit{where}\ I = \mathsf{Ind}(X\!:\!\mathsf{Kind})\{\vec{C}\} \mathit{and}\ \forall i.\ \mathit{small}(C_i)$$

  The interesting case is when we consider the reduction

  $$\begin{array}{l} \mathsf{Elim}[I, A'](\mathsf{Ctor}\,(i, I)\ \vec{A})\{\vec{B}\}\ \rhd_{\iota}\ (\Phi_{X,I,B'}(C_i, B_i))\ \vec{A} \\ \mathit{where}\ \ I = \mathsf{Ind}(X\!:\!\mathsf{Kind})\{\vec{C}\} \\ \qquad B' = \lambda Y\!:\!I.\, (\mathsf{Elim}[I, A'](Y)\{\vec{B}\}) \end{array}$$

  Suppose $A'' = (\Phi_{X,I,B'}(C_i, B_i))\ \vec{A}$. Suppose that $\vec{A} = A_{1\ldots n}$. We have that $\Delta \vdash B_i : \Psi_{X,I}(C_i, A')$. The proof is by induction on the fact that C_i is a kind of a constructor and the length of $\vec{A}$. We consider the different cases by which C_i is a kind of a constructor.

  - If $C_i = X$, then $A'' = B_i$. From definition 9 we can see that in this case, B_i has the type A'.
  - If $C_i = \Pi Y\!:\!B.\, C$, then $A'' = (\Phi_{X,I,B'}([A_1/Y]C, B_i\ A_1))\ A_{2\ldots n}$. We have that $\Delta \vdash B_i\ A_1 : \Psi_{X,I}([A_1/Y]C, A')$. By the induction hypothesis, the reduct has type A'.
  - If $C_i = \Pi \vec{Y} : \vec{B}.\, X \to C$, then

    $$A'' = \Phi_{X,I,B'}(C, B_i\ A_1\ (\lambda \vec{Y} : \vec{B}.\, B'\ (A_1\ \vec{Y})))\ A_{2\ldots n}$$

    From Definition 9 we have that $\Delta \vdash B_i : [I/X]A \to [A'/X]A \to \Psi_{X,I}(C', A')$. We also know that $\Delta \vdash A_1 : [I/X]A$. From here, we can apply the induction hypothesis and show that the reduct has type A'.

- ELIM We will only consider the case when an ι reduction takes place at the head. The other cases follow easily by structural induction.

$$\frac{\begin{array}{c}\Delta \vdash A : I \quad \Delta \vdash A' : I \to \mathsf{Kind} \\ \textit{for all } i \quad \Delta \vdash B_i : \zeta_{X,I}(C_i, A', \mathsf{Ctor}\,(i, I))\end{array}}{\begin{array}{c}\Delta \vdash \mathsf{Elim}[I, A'](A)\{\vec{B}\} : A'\ A' \\ \textit{where } I = \mathsf{Ind}(X : \mathsf{Kind})\{\vec{C}\}\end{array}}$$

The interesting case is when we consider the reduction

$$\begin{array}{l}\mathsf{Elim}[I, A'](\mathsf{Ctor}\,(i, I)\ \vec{A})\{\vec{B}\} \ \rhd_\iota \ (\Phi_{X,I,B'}(C_i, B_i))\ \vec{A} \\ \textit{where} \quad I = \mathsf{Ind}(X : \mathsf{Kind})\{\vec{C}\} \\ \qquad B' = \lambda Y : I.\, (\mathsf{Elim}[I, A'](Y)\{\vec{B}\})\end{array}$$

Suppose $A'' = (\Phi_{X,I,B'}(C_i, B_i))\ \vec{A}$. Suppose that $\vec{A} = A_{1\ldots n}$. We have that $\Delta \vdash B_i : \zeta_{X,I}(C_i, A', \mathsf{Ctor}\,(i, I))$. By using the inversion lemma we can get that $\Delta \vdash B' : \Pi X : I.\, A'\ X$. By induction on the structure of C_i (where C_i is a kind of a constructor), we can show that if $C_i = \Pi \vec{Y} : \vec{B}.\, X$, then $\Delta \vdash \Phi_{X,I,B'}(C_i, B_i) : \Pi \vec{Y} : \vec{B}.\, A'\ \mathsf{Ctor}\,(i, I)\ \vec{Y}$. The required result follows from here.

□

Corollary 23 Suppose A is a well formed term. If $A \rhd^*_{\beta\iota'} A'$, then $A \rhd^*_{\beta\iota} A'$ and A' is well formed.

Corollary 24 Suppose A is a well formed term. If $A \rhd^* A'$, then there exists a well formed term A'' such that $A \rhd^*_{\beta\iota} A'' \rhd^*_\eta A'$.

Lemma 22 Let $\Delta \vdash A : B$ and $\Delta \vdash A' : B'$ be two derivable judgments. If $A =_{\beta\eta\iota} A'$, then $\mathsf{Cls}(A) = \mathsf{Cls}(A')$.

Proof We know that $\| A \|$ and $\| A' \|$ have a common reduct, say A_2. This implies that

$$\| A \| \rhd^*_{\beta\iota'_0} B \rhd^*_\eta A_2 \qquad \text{and} \qquad \| A' \| \rhd^*_{\beta\iota'_0} B' \rhd^*_\eta A_2$$

From here we get that

$$A \rhd^*_{\beta\iota} B_0 \text{ and } A' \rhd^*_{\beta\iota} B'_0 \text{ where } \| B_0 \| = B \text{ and } \| B'_0 \| = B'$$

Eta reduction does not change the class of a term. Moving from marked to unmarked terms also does not change the class of a term. Therefore, we get that

$$\begin{array}{l}\mathsf{Cls}(A) = \mathsf{Cls}(B_0) = \mathsf{Cls}(B) = \mathsf{Cls}(A_2) \quad \text{and} \\ \mathsf{Cls}(A_2) = \mathsf{Cls}(B') = \mathsf{Cls}(B'_0) = \mathsf{Cls}(A')\end{array}$$

□

Corollary 25 Let $\Delta \vdash A : s_1$ and $\Delta \vdash B : s_2$ be two derivable judgments. If $A =_{\beta\eta\iota} B$, then $s_1 = s_2$.

Lemma 23 If $\Delta_1, Y : C, \Delta_2 \vdash A : B$ and $Y \notin FV(\Delta_2) \cup FV(A)$, then there exists a B' such that $\Delta_1\Delta_2 \vdash A : B'$. (This also implies that $B =_{\beta\eta\iota} B'$).

Proof The proof is by induction on the structure of the derivation. We will consider only the important cases.

- case FUN. We know that

$$\frac{\begin{array}{c}\Delta_1, Y : C, \Delta_2, X : A \vdash B : B' \\ \Delta_1, Y : C, \Delta_2 \vdash \Pi X : A.\, B' : s\end{array}}{\Delta_1, Y : C, \Delta_2 \vdash \lambda X : A.\, B : \Pi X : A.\, B'}$$

Applying the induction hypothesis to the formation of B

$$\Delta_1\Delta_2, X : A \vdash B : C' \qquad B' =_{\beta\eta\iota} C'$$

By lemma 18 we have that

$$\begin{array}{l}\Delta_1\Delta_2, X : A \vdash C' : s \text{ which implies} \\ \Delta_1\Delta_2 \vdash \Pi X : A.\, C' : s\end{array}$$

Therefore we get that

$$\Delta_1\Delta_2 \vdash \lambda X : A.\, B : \Pi X : A.\, C'$$

- case APP We know that

$$\frac{\begin{array}{c}\Delta_1, Y : C, \Delta_2 \vdash A : \Pi X : B'.\, A' \\ \Delta_1, Y : C, \Delta_2 \vdash B : B'\end{array}}{\Delta_1, Y : C, \Delta_2 \vdash A\ B : [B/X]A'}$$

By applying the induction hypothesis we get that

$$\begin{array}{l}\Delta_1\Delta_2 \vdash A : A_2 \text{ and } \Delta_1\Delta_2 \vdash B : A_3 \text{ where} \\ A_2 =_{\beta\eta\iota} \Pi X : B'.\, A' \text{ and } A_3 =_{\beta\eta\iota} B'\end{array}$$

From lemma 13, $A_2 \ \rhd_{\beta\iota} \ \lambda \vec{Y} : \vec{A}.\, (\Pi X : B''.\, A'')\ \vec{B}$. Since $\beta\iota$ reduction preserves type, and A_2 is well formed, we have that $A_2 \ \rhd_{\beta\iota} \ \Pi X : B''.\, A''$. This implies that $A'' =_{\beta\eta\iota} A'$ and $B'' =_{\beta\eta\iota} B'$. We also get that $A_3 =_{\beta\eta\iota} B''$. From corollary 25 we get that A_3 and B'' have the same sort. By applying the CONV rule we get that

$$\Delta_1\Delta_2 \vdash A : \Pi X : B''.\, A'' \text{ and } \Delta_1\Delta_2 \vdash B : B''$$

Therefore, we get that

$$\Delta_1\Delta_2 \vdash A\ B : [B/X]A''$$

□

As a corollary we now get that

Lemma 24 (Strengthening) If $\Delta_1, Y : C, \Delta_2 \vdash A : B$ and $Y \notin FV(\Delta_2) \cup FV(A) \cup FV(B)$, then $\Delta_1\Delta_2 \vdash A : B$.

Lemma 25 (Subject reduction for η reduction) If $\Delta \vdash A : B$, and $A \ \rhd_\eta \ A'$ and $\Delta \ \rhd_\eta \ \Delta'$, then we have that

$$\Delta \vdash A' : B \qquad \Delta' \vdash A : B$$

Proof The interesting case is that of functions. Suppose that

$$\Delta \vdash \lambda X : A_1.\, A_2\ X : B \quad X \notin FV(A_2) \quad \lambda X : A_1.\, A_2\ X \rhd_\eta A_2$$

From lemma 19 we know that

$$\Delta, X : A_1 \vdash A_2\ X : A_3 \quad B =_{\beta\eta\iota} \Pi X : A_1.\, A_3 \quad \Delta \vdash B : s$$

Again applying lemma 19 we get that

$$\Delta, X : A_1 \vdash A_2 : \Pi Y : B'.\, A' \ \ B' =_{\beta\eta\iota} A_1 \ \ A_3 =_{\beta\eta\iota} [X/Y]A'$$

By applying the CONV rule now, we get that $\Delta, X : A_1 \vdash A_2 : B$. By applying lemma 24 we get that $\Delta \vdash A_2 : B$. □

Theorem 26 (Subject reduction) If $\Delta \vdash A : B$, and $A \rhd A'$ and $\Delta \rhd \Delta'$, then we have that: $\Delta \vdash A' : B$ and $\Delta' \vdash A : B$.

Proof Follows from lemma 21 and 25. □

D.3 Strong Normalization

The proof is structured as follows:

- We introduce a calculus of pure terms. This is just the pure λ calculus extended with a recursive filtering operator. We do this so that we can operate in a confluent calculus.
- We define a notion of reducibility candidates. Every schema gives rise to a reducibility candidate. We also show how these candidates can be constructed inductively.
- We then define a notion of well constructed kinds which is a weak form of typing.
- We associate an interpretation to each well formed kind. We show that under adequate conditions, this interpretation is a candidate.
- We show that type level constructs such as abstractions and constructors belong to the candidate associated with their kind.
- We show that the interpretation of a kind remains the same under $\beta\eta$ reduction.
- We define a notion of kinds that are invariant on their domain – these are kinds whose interpretation remains the same upon reduction.
- We show that kinds formed with large elimination are invariant on their domain.
- From here we can show the strong normalization of the calculus of pure terms. We show that if a type is well formed, then the pure term derived from it is strongly normalizing.
- We then reduce the strong normalization of all well formed terms to the strong normalization of pure terms.

D.3.1 Notation

The syntax for the language is:

$$
\begin{array}{lll}
(\textit{ctxt}) & \Delta & ::= \cdot \mid \Delta, X : A \\
(\textit{sort}) & s & ::= \mathsf{Kind} \mid \mathsf{Kscm} \mid \mathsf{Ext} \\
(\textit{var}) & X & ::= z \mid k \mid t \\
(\textit{ptm}) & A, B & ::= s \mid X \mid \lambda X : A.\, B \mid A\ B \mid \Pi X : A.\, B \\
 & & \quad \mid \mathsf{Ind}(X : \mathsf{Kind})\{\vec{A}\} \mid \mathsf{Ctor}\,(i, A) \\
 & & \quad \mid \mathsf{Elim}[A', B'](A)\{\vec{B}\}
\end{array}
$$

The proof of strong normalization uses the stratification in the language shown below.

$$
\begin{array}{lll}
(\textit{ctxt}) & \Delta & ::= \cdot \mid \Delta, z : \mathsf{Kscm} \mid \Delta, k : u \mid \Delta, t : \kappa \\
(\textit{kscm}) & u & ::= z \mid \Pi t : \kappa.\, u \mid \Pi k : u_1.\, u_2 \mid \mathsf{Kind} \\
(\textit{kind}) & \kappa & ::= k \mid \lambda t : \kappa_1.\, \kappa_2 \mid \kappa[\tau] \mid \lambda k : u.\, \kappa \mid \kappa_1\ \kappa_2 \\
 & & \quad \mid \Pi t : \kappa_1.\, \kappa_2 \mid \Pi k : u.\, \kappa \mid \Pi z : \mathsf{Kscm}.\, \kappa \\
 & & \quad \mid \mathsf{Ind}(k : \mathsf{Kind})\{\vec{\kappa}\} \mid \mathsf{Elim}[\kappa', u](\tau)\{\vec{\kappa}\} \\
(\textit{type}) & \tau & ::= t \mid \lambda t : \kappa.\, \tau \mid \tau_1\ \tau_2 \mid \lambda k : u.\, \tau \mid \tau[\kappa] \\
 & & \quad \mid \lambda z : \mathsf{Kscm}.\, \tau \mid \tau[u] \mid \mathsf{Ctor}\,(i, \kappa) \\
 & & \quad \mid \mathsf{Elim}[\kappa', \kappa](\tau')\{\vec{\tau}\} \mid \mathsf{Elim}[\kappa', \kappa](\tau')\{\vec{\tau}\}
\end{array}
$$

In this section, the types are also referred to as proof terms. We sometimes use I to refer to an inductive definition.

D.3.2 Pure terms

The pure terms are defined as:

$$(\Lambda) \quad a, b, c ::= t \mid a\ b \mid \lambda t.a \mid \mathsf{Co}(n) \mid \mathsf{match}\, t.\{\vec{a}\}$$

The set of reductions on the pure terms are defined as:

$$
\begin{array}{l}
(\lambda t.a)\ b \rhd_\beta [b/t]a \\
\lambda t.(a\ t) \rhd_\eta a \qquad \text{if } t \notin FV(a) \\
\mathsf{match}\, t.\{\vec{a}\}\ (\mathsf{Co}(i)\ \vec{b}) \rhd_\iota ([\mathsf{match}\, t.\{\vec{a}\}/t]a_i)\ \vec{b}
\end{array}
$$

The translation from types to pure terms is defined as:

$$
\begin{array}{rl}
|\, t \,| &= t \\
|\, \tau_1\ \tau_2 \,| &= |\, \tau_1 \,|\ |\, \tau_2 \,| \\
|\, \tau[\kappa] \,| &= |\, \tau \,| \\
|\, \tau[u] \,| &= |\, \tau \,| \\
|\, \lambda t : \kappa.\, \tau \,| &= \lambda t.|\, \tau \,| \\
|\, \lambda k : u.\, \tau \,| &= |\, \tau \,| \\
|\, \lambda z : \mathsf{Kscm}.\, \tau \,| &= |\, \tau \,| \\
|\, \mathsf{Ctor}\,(n, \kappa) \,| &= \mathsf{Co}(n) \\
|\, \mathsf{Elim}[\kappa, \kappa'](\tau)\{\vec{\tau}\} \,| &= \\
\multicolumn{2}{c}{(\mathsf{match}\, t.\{\overrightarrow{\Upsilon(\kappa_i, |\, \tau_i \,|, \lambda t_2.t\ t_2)}\})\ \ |\, \tau \,|} \\
\multicolumn{2}{c}{\text{where } \kappa = \mathsf{Ind}(k : \mathsf{Kind})\{\vec{\kappa}\} \text{ and}}
\end{array}
$$

$$
\begin{array}{rl}
\Upsilon(k, a_1, a_2) &= a_1 \\
\Upsilon(\Pi t : \kappa_1.\, \kappa_2, a_1, a_2) &= \lambda t.\Upsilon(\kappa_2, a_1\ t, a_2) \\
\Upsilon(\Pi k : u.\, \kappa, a_1, a_2) &= \Upsilon(\kappa, a_1, a_2) \\
\Upsilon(\Pi z : \mathsf{Kscm}.\, \kappa, a_1, a_2) &= \Upsilon(\kappa, a_1, a_2) \\
\Upsilon(\Pi \vec{X} : \vec{A}.\, k \to \kappa, a_1, a_2) &= \\
\multicolumn{2}{c}{\lambda t.\Upsilon(\kappa, a_1\ t\ (\lambda |\, \vec{X} \,|.a_2\ (t\ \ |\, \vec{X} \,|)), a_2)}
\end{array}
$$

Lemma 26 Let τ and τ' be two well formed types and let t be a type variable. Then $|\, [\tau'/t]\tau \,| = [|\, \tau' \,|\ /t]\ |\, \tau \,|$.

Proof It is a straightforward proof by induction over the structure of τ. □

The following lemma uses Definitions 9 and 7 in Section D.2 and also the definition of Υ from above.

Lemma 27 $|\, \Phi_{X,I,B}(\kappa, \tau) \,| =$
$[\mathsf{match}\, t.\{\overrightarrow{\Upsilon(\kappa_i, |\, \tau_i \,|, \lambda t_2.t\ t_2)}\}/t]\Upsilon(\kappa, |\, \tau \,|, \lambda t_2.t\ t_2)$

Proof The proof is by induction on the fact that κ is the kind of a constructor. □

Lemma 28 For all well formed proof terms τ_1 and τ_2, if $\tau_1\ \rhd^i\ \tau_2$, then $|\, \tau_1 \,|\ \rhd^j\ |\, \tau_2 \,|$ where $j \leq i$.

Proof Follows from lemmas 26 and 27. □

D.3.3 Interpretation of schemas

Definition 27 (Arity) We call ground kind schemas arities denoted as $\mathsf{arity}(u, \mathsf{Kind})$. The arities are defined with the following grammar:

$$(\textit{kscm}) \quad u ::= \mathsf{Kind} \mid \Pi k : u_1.\, u_2 \mid \Pi t : \kappa.\, u$$

Definition 28 (Schema map) We define a kind schema mapping $\mathcal{K}$ as a function mapping kind schema variables z to arities. We also use $\mathcal{K}, z : u$ to say that $\mathcal{K}$ has been augmented with the mapping $z \mapsto u$.

Definition 29 We define the function $\rho(u)_{\mathcal{K}}$ as:

$$\rho(u)_{\mathcal{K}} = \rho_0(\mathcal{K}(u)) \quad \text{where}$$

- $\rho_0(\mathsf{Kind})$ is the set of sets of pure terms;
- $\rho_0(\Pi k\!:\!u_1.\,u_2)$ is the set of functions from $\rho_0(u_1)$ to $\rho_0(u_2)$; and
- $\rho_0(\Pi t\!:\!\kappa.\,u)$ is the set of functions from Λ to $\rho_0(u)$.

Definition 30 For each kind schema u and mapping $\mathcal{K}$, we define in $\rho(u)_{\mathcal{K}}$ the relation of partial equivalence written as $\simeq_{\mathcal{K}(u)}$ as follows:

- for all C and C' in $\rho_0(\mathsf{Kind})$, we have that $C \simeq_{\mathsf{Kind}} C' \iff C = C'$;
- for all C and C' in $\rho_0(\Pi k\!:\!u_1.\,u_2)$, we have $C \simeq_{\Pi k u_1.\,u_2} C' \iff$ for all C_1 and C_2 in $\rho_0(u_1)$ with $C_1 \simeq_{u_1} C_2$ we get that $C\ C_1 \simeq_{u_2} C'\ C_2$; and
- for all C and C' in $\rho_0(\Pi t\!:\!\kappa.\,u)$, we have that $C \simeq_{\Pi t\kappa.\,u} C' \iff$ for all a and b in Λ such that $a =_{\beta\eta\iota} b$, we get that $C\ a \simeq_u C' b$.

Definition 31 (Invariant) Given C in $\rho(u)_{\mathcal{K}}$, we say that C is invariant $\iff C \simeq_{\mathcal{K}(u)} C$.

Definition 32 (Neutral terms) A term is called neutral if it has neither of the following forms – $\lambda t.a$, $\mathsf{Co}(i)\ \vec{a}$, or $\mathsf{match}\ t.\{\vec{a}\}$.

Definition 33 We define $\mathcal{CR}_0(\mathsf{Kind})$ as consisting of all sets C such that:

- if $a \in C$, then a is strongly normalizing;
- if $a_1 \rhd a_2$ and $a_1 \in C$, then $a_2 \in C$; and
- if a is neutral and for all terms a' such that $a \rhd a'$ and $a' \in C$, then $a \in C$.

Definition 34 (Candidates) We define $\mathcal{CR}(u)_{\mathcal{K}}$ as a subset of $\rho(u)_{\mathcal{K}}$ as:

$$\mathcal{CR}(u)_{\mathcal{K}} = \mathcal{CR}_0(\mathcal{K}(u)) \quad \text{where}$$

- $\mathcal{CR}_0(\mathsf{Kind})$ is defined as in Definition 33;
- $\mathcal{CR}_0(\Pi t : \kappa.\,u)$ is the set of invariant elements C belonging to $\rho_0(\Pi t\!:\!\kappa.\,u)$ such that $C\ \Lambda \subset \mathcal{CR}_0(u)$; and
- $\mathcal{CR}_0(\Pi k\!:\!u_1.\,u_2)$ is the set of invariant elements C belonging to $\rho_0(\Pi k\!:\!u_1.\,u_2)$ such that $C\ (\mathcal{CR}_0(u_1)) \subset \mathcal{CR}_0(u_2)$.

Proposition 35 All reducibility candidates are invariant.

Proposition 36 Let $(C_i)_{i\in I}$ be a family of reducibility candidates of Kind indexed by a set I. Then $\cap_{i\in I} C_i$ is a reducibility candidate of schema Kind.

Lemma 29 Let $C \in \rho(u)_{\mathcal{K}}$. If C is invariant, then

$$C \in \mathcal{CR}(u)_{\mathcal{K}} \iff \forall C' \in Dom(\mathcal{CR}(u)_{\mathcal{K}}).C\ C' \in \mathcal{CR}(\mathsf{Kind})_{\mathcal{K}}$$

Proof Straightforward induction over the structure of $\mathcal{K}(u)$. □

Definition 37 Let a_1 be a strongly normalizing term. Then the length of the longest sequence of reductions to a normal form is denoted as $\nu(a_1)$.

Lemma 30 Let a_1 and a_2 be two terms and let $C \in \mathcal{CR}_0(\mathsf{Kind})$ be a reducibility candidate. If a_2 is strongly normalizing, and if $[a_2/t]a_1 \in C$, then $(\lambda t.a_1)\ a_2 \in C$.

Proof By induction over $\nu(a_1) + \nu(a_2)$. □

Corollary 38 Let a_1 be a pure term and let C be a reducibility candidate of schema Kind. Let $\vec{t}$ and $\vec{a'}$ be respectively a sequence of variables and terms of the same length. If for all i, a'_i is strongly normalizing, and if $[\vec{a'}/\vec{t}]a_1 \in C$, then $(\lambda \vec{t}.a_1)\ \vec{a'} \in C$.

Lemma 31 For all reducibility candidates C of kind Kind, for all sequences of strongly normalizing $\vec{a}$ and $\vec{b}$ and for all i less than the length of $\vec{a}$, we have that

$$\mathsf{match}\ t.\{\vec{a}\}\ (\mathsf{Co}(i)\ \vec{b}) \in C \iff ([\mathsf{match}\ t.\{\vec{a}\}/t]a_i)\ \vec{b} \in C$$

Proof Follows by induction over $\nu(a_i) + \nu(b_i)$ (for all i). □

Definition 39 (Canonical candidates) Define $\mathsf{Can}(u)_{\mathcal{K}}$ as:

$$\mathsf{Can}(u)_{\mathcal{K}} = \mathsf{Can}_0(\mathcal{K}(u)) \quad \text{where}$$

- $\mathsf{Can}_0(\mathsf{Kind})$ is the set of all strongly normalizing terms;
- $\mathsf{Can}_0(\Pi t : \kappa.\,u)$ is the function mapping all pure terms to $\mathsf{Can}_0(u)$; and
- $\mathsf{Can}_0(\Pi k : u_1.\,u_2)$ is the function mapping all elements of $\rho_0(u_1)$ to $\mathsf{Can}_0(u_2)$.

D.3.4 Properties of candidates

In this section, we state some properties of the reducibility candidates. The properties with respect to the union and the intersection of a family of candidates will be used for the inductive constructions of candidates.

Definition 40 (Order over candidates) For each kind schema u and mapping $\mathcal{K}$, we define in $\rho(u)_{\mathcal{K}}$ the relation $<_{\mathcal{K}(u)}$ as follows:

- for all C and C' in $\rho_0(\mathsf{Kind})$, we have that $C <_{\mathsf{Kind}} C' \iff C \subset C'$;
- for all C and C' in $\rho_0(\Pi k\!:\!u_1.\,u_2)$, we have $C <_{\Pi k u_1.\,u_2} C' \iff$ for all C_1 in $\rho_0(u_1)$, we get that $C\ C_1 <_{u_2} C'\ C_1$; and
- for all C and C' in $\rho_0(\Pi t\!:\!\kappa.\,u)$, we have that $C <_{\Pi t\kappa.\,u} C' \iff$ for all a in Λ, we get that $C\ a <_u C'\ a$.

Definition 41 For all schemas u and mapping $\mathcal{K}$, for all families of elements in $\rho(u)_{\mathcal{K}}$, we define $\bigwedge_{i\in I} C_i$ as:

- for all $C_i \in \rho_0(\mathsf{Kind})$, $\bigwedge_{i\in I} C_i = \cap_{i\in I} C_i$;
- for all $C_i \in \rho_0(\Pi t\!:\!\kappa.\,u)$, $\bigwedge_{i\in I} C_i = b \in \Lambda \mapsto \bigwedge_{i\in I} C_i\ b$; and
- for all $C_i \in \rho_0(\Pi k : u_1.\,u_2)$, $\bigwedge_{i\in I} C_i = C' \in \rho_0(u_1) \mapsto \bigwedge_{i\in I} C_i\ C'$.

Lemma 32 Let u be a schema and $\mathcal{K}$ a mapping and C_i a family of elements of $\rho(u)_{\mathcal{K}}$. Then $\forall j \in I$, $\bigwedge_{i\in I} C_i <_{\mathcal{K}(u)} C_j$.

Proof It follows in a straightforward way by induction over the structure of $\mathcal{K}(u)$. □

The following two propositions also follow easily by induction over the structure of $\mathcal{K}(u)$.

Proposition 42 Let u be a schema and $\mathcal{K}$ a mapping and C_i a family of elements of $\rho(u)_{\mathcal{K}}$. If all C_i are invariants, then the same holds for $\bigwedge_{i\in I} C_i$.

Proposition 43 Let u be a schema and $\mathcal{K}$ a mapping and C_i a family of elements of $\mathcal{CR}(u)_{\mathcal{K}}$. Then we also have that $\bigwedge_{i\in I} C_i \in \mathcal{CR}(u)_{\mathcal{K}}$.

Corollary 44 We get that $(\mathcal{CR}(u)_{\mathcal{K}}, <_{\mathcal{K}(u)})$ is an inf-semi-lattice for all schema u and mapping $\mathcal{K}$. We use $min(\mathcal{K}(u))$ to denote the smallest element.

Definition 45 For all schemas u and mapping $\mathcal{K}$, for all families of elements in $\rho(u)_{\mathcal{K}}$, we define $\bigvee_{i\in I} C_i$ as:

- for all $C_i \in \rho_0(\mathsf{Kind})$, $\bigvee_{i\in I} C_i = \cup_{i\in I} C_i$;
- for all $C_i \in \rho_0(\Pi t : \kappa.\, u)$, $\bigvee_{i\in I} C_i = b \in \Lambda \mapsto \bigvee_{i\in I} C_i\ b$; and
- for all $C_i \in \rho_0(\Pi k : u_1.\, u_2)$, $\bigvee_{i\in I} C_i = C' \in \rho_0(u_1) \mapsto \bigvee_{i\in I} C_i\ C'$.

Lemma 33 Let u be a schema and $\mathcal{K}$ be a mapping. Let $(C_i)_{i\in I}$ and $(C'_i)_{i\in I}$ be two families of elements of $\rho(u)_{\mathcal{K}}$. If for all elements i of I we have that $C_i \simeq_{\mathcal{K}(u)} C'_i$, then we also have that $\bigvee_{i\in I} C_i \simeq_{\mathcal{K}(u)} \bigvee_{i\in I} C'_i$.

Proof Straightforward induction over the structure of $\mathcal{K}(u)$. □

Corollary 46 Let u be a schema and $\mathcal{K}$ be a mapping. Let $(C_i)_{i\in I}$ be a family of elements of $\rho(u)_{\mathcal{K}}$. If all C_i are invariant, then $\bigvee_{i\in I} C_i$ is also invariant.

Lemma 34 Let u be a schema and $\mathcal{K}$ be a mapping. Let $(C_i)_{i\in I}$ be a family of elements of $\rho(u)_{\mathcal{K}}$ and $C \in \rho(u)_{\mathcal{K}}$. If for all i, $C_i <_{\mathcal{K}(u)} C$, then $\bigvee_{i\in I} C_i <_{\mathcal{K}(u)} C$.

Proof The proof is by induction over the structure of $\mathcal{K}(u)$. □

Lemma 35 Let $(C_i)_{i\in I}$ be a totally ordered family of elements of $\mathcal{CR}(u)_{\mathcal{K}}$. Then $\bigvee_{i\in I} C_i \in \mathcal{CR}(u)_{\mathcal{K}}$.

Proof The proof is by induction over the structure of $\mathcal{K}(u)$. Suppose $\bigvee_{i\in I} C_i = C'$.

- $\mathcal{K}(u) = \mathsf{Kind}$. We have to make sure that all three conditions in Definition 33 are satisfied. The first two conditions follow obviously. For the third case, assume that a is neutral and for all terms a_i such that $a \rhd a_i$, we have that $a_i \in C'$. This implies that $a_i \in C_j$ for some j. Since there are finitely many such C_j and they are totally ordered, we can choose a C_k among them that contains all the C_js. Since this C_k is also a candidate, it contains a. Therefore, $a \in \bigvee_{i\in I} C_i$.
- $\mathcal{K}(u) = \Pi t : \kappa.\, u$. Since all the C_i are invariant, it follows from Definitions 30 and 31 that for a term $a \in \Lambda$, we have that $C_i\ a$ is invariant. Again from Definition 40, it is clear that the $C_i\ a$ are totally ordered. Also from Corollary 46 we get that $\bigvee_{i\in I} C_i\ a$ is invariant. Applying the induction hypothesis we get that $\bigvee_{i\in I} C_i\ a \in \mathcal{CR}_0(u)$. From Definition 34, it follows that $\bigvee_{i\in I} C_i \in \mathcal{CR}_0(\Pi t : \kappa.\, u)$.
- $\mathcal{K}(u) = \Pi k : u_1.\, u_2$. Similar to the previous case.

□

Definition 47 (Schema interpretation) A schema interpretation $\mathcal{U}$ is a function that maps a kind variable k to an element of $\rho(u)_{\mathcal{K}}$. We also use $\mathcal{U}, k : C$ to say that $\mathcal{U}$ has been augmented with the mapping $k \mapsto C$.

Definition 48 (Well formed kinds) Let u be a schema, κ be a kind, $\mathcal{K}$ be a mapping, and $\mathcal{U}$ be an interpretation. We say that κ is a well formed kind of schema $\mathcal{K}(u)$ under $\mathcal{K}$ and $\mathcal{U}$ *iff*:

1. $\kappa = k$ and $\mathcal{U}(k) = \rho(u)_{\mathcal{K}}$;
2. $\kappa = \Pi t : \kappa_1.\, \kappa_2$ with $\mathcal{K}(u) =_{\beta\eta\iota} \mathsf{Kind}$ and κ_1 and κ_2 are both well constructed of schema Kind under $\mathcal{K}$ and $\mathcal{U}$;
3. $\kappa = \Pi k : u'.\, \kappa'$ with $\mathcal{K}(u) =_{\beta\eta\iota} \mathsf{Kind}$ and κ' is well constructed of schema Kind under $\mathcal{K}$ and $\mathcal{U}, k : \rho(u')_{\mathcal{K}}$;
4. $\kappa = \Pi z : \mathsf{Kscm}.\, \kappa'$ with $\mathcal{K}(u) =_{\beta\eta\iota} \mathsf{Kind}$ and for all u' such that $u' \in \mathsf{arity}(u_1, \mathsf{Kind})$, we have that κ' is well constructed of schema Kind under $\mathcal{K}, z : u'$ and $\mathcal{U}$;
5. $\kappa = \kappa_1\ \kappa_2$ if there exists two schemas u_1 and u_2 with κ_2 well constructed of schema $\mathcal{K}(u_2)$ under $\mathcal{K}$ and $\mathcal{U}$, also κ_1 well constructed of schema $\mathcal{K}(\Pi k : u_2.\, u_1)$ under $\mathcal{K}$ and $\mathcal{U}$, and $\rho(u)_{\mathcal{K}} = \rho([\kappa_2/k]u_1)_{\mathcal{K}}$;
6. $\kappa = \kappa_1\ \tau_1$ if there exists a schema u_2 and kind κ_2 such that κ_1 is well constructed of schema $\mathcal{K}(\Pi t : \kappa_2.\, u_2)$ under $\mathcal{K}$ and $\mathcal{U}$ and $\rho(u)_{\mathcal{K}} = \rho([\tau_1/t]u_2)_{\mathcal{K}}$;
7. $\kappa = \lambda k : u_1.\, \kappa_1$ if there exists a u_2 such that κ_1 is well constructed of schema $\mathcal{K}(u_2)$ under $\mathcal{K}$ and $\mathcal{U}, k : \rho(u_1)_{\mathcal{K}}$ and $\rho(u)_{\mathcal{K}} = \rho(\Pi k : u_1.\, u_2)_{\mathcal{K}}$;
8. $\kappa = \lambda t : \kappa_1.\, \kappa_2$ if there exists a u_2 such that κ_2 is well constructed of schema $\mathcal{K}(u_2)$ under $\mathcal{K}$ and $\mathcal{U}$ and $\rho(u)_{\mathcal{K}} = \rho(\Pi t : \kappa_1.\, u_2)_{\mathcal{K}}$;
9. $\kappa = \mathsf{Ind}(k : \mathsf{Kind})\{\vec{\kappa}\}$ if all κ_i are kinds of constructors and well constructed of schema Kind under $\mathcal{K}$ and $\mathcal{U}, k : \rho_0(\mathsf{Kind})$, and $\rho(u)_{\mathcal{K}} = \rho_0(\mathsf{Kind})$; and
10. $\kappa = \mathsf{Elim}[\kappa', u'](\tau)\{\vec{\kappa}\}$ if $\kappa' = \mathsf{Ind}(k : \mathsf{Kind})\{\vec{\kappa'}\}$, and κ' is well constructed of schema Kind under $\mathcal{K}$ and $\mathcal{U}$, also u' is a schema and $\mathcal{K}(u) =_{\beta\eta\iota} u'$, and κ_i is well constructed of schema $\mathcal{K}(\Psi_{k,\kappa'}(\kappa'_i, u'))$ under $\mathcal{K}$ and $\mathcal{U}$.

Definition 49 We define compatible mappings and interpretation as:

1. A mapping $\mathcal{K}$ is compatible with a context Δ if for all $z \in \Delta$, we have $\mathcal{K}(z) = \mathsf{arity}(u, \mathsf{Kind})$.
2. An interpretation $\mathcal{U}$ is compatible with a context Δ and a compatible mapping $\mathcal{K}$ if for all pairs $(k, u) \in \Delta$, we have $\mathcal{U}(k) \in \rho(u)_{\mathcal{K}}$.

Lemma 36 If $\Delta \vdash \kappa : u$, then for all compatible $\mathcal{K}$ and $\mathcal{U}$, we have that κ is well constructed of schema $\mathcal{K}(u)$.

Proof By induction over the structure of κ. □

D.3.5 Inductive constructions

Consider an increasing function F in $\rho_0(\mathsf{Kind})$ for the order $<_{\mathsf{Kind}}$. Denote the smallest element of $\rho_0(\mathsf{Kind})$ as $\bot$. Since $\rho_0(\mathsf{Kind})$ is closed under $\cap$, and $(\rho_0(\mathsf{Kind}), <_{\mathsf{Kind}})$ is an inf-semi-lattice, the function F has a least fixed point (lfp). We will construct this least fixed point inductively. We first define the transfinite iteration of F.

Definition 50 Let $C \in \rho_0(\mathsf{Kind})$ and o be an ordinal. We define the iteration of order o of F over C as:

- $F^0(C) = C$;
- $F^{o+1}(C) = F(F^o(C))$; and
- $F^{lim(U)} = \cup_{o \in U} F^o(C)$.

Lemma 37 Let o be an ordinal; we have $F^o(\bot) <_{\mathsf{Kind}} lfp(F)$.

Proof The proof is by induction over o. If $o = 0$, then it follows immediately. Otherwise,

- $o = o' + 1$ Then we have that $F^o(\bot) = F(F^{o'}(\bot))$. By the induction hypothesis, we get that $F(F^{o'}(\bot)) <_{\mathsf{Kind}} F(lfp(F))$. This implies that $F(F^{o'}(\bot)) <_{\mathsf{Kind}} lfp(F)$.
- $o = lim(U)$ Follows immediately from the induction hypothesis and lemma 34.

□

Remark 51 Since we do not consider the degenerate case of $F(\bot) = \bot$, it follows from lemma 37 that for some ordinal o, we have that $lfp(F) = F^o(\bot)$.

Lemma 38 Suppose $\mathcal{S}$ is a subset of $\rho_0(\mathsf{Kind})$ satisfying:

- if $(C_i)_{i \in I}$ is a totally ordered family of elements of $\mathcal{S}$, then $\cup_{i \in I} C_i \in \mathcal{S}$;
- $F(\bot) \in \mathcal{S}$; and
- for all C in $\mathcal{S}$, $F(C) \in \mathcal{S}$.

Then $lfp(F) \in \mathcal{S}$.

Proof Follows from the fact that $lfp(F) = F^o(\bot)$ for some ordinal o. □

Definition 52 Let $a \in lfp(F)$. We define $\mathsf{deg}(a)$ as the smallest ordinal such that $a \in F^{\mathsf{deg}(a)}(\bot)$.

Definition 53 To all $a \in lfp(F)$, we associate $\mathsf{pred}(a)$ defined as $F^{\mathsf{deg}(a)-1}(\bot)$.

Lemma 39 For all a, $\mathsf{deg}(a)$ is an ordinal successor.

Proof Suppose it is the limit of the set U. From Definition 50, there exists some $o \in U$ for which $a \in F^o(\bot)$. This leads to a contradiction. □

Definition 54 (Partial order) Suppose C and C' are two elements of $\mathcal{CR}_0(\mathsf{Kind})$. We say that $C <_F C'$ if $C = F^o(\bot)$ and $C' = F^{o'}(\bot)$, and $o < o'$.

D.3.6 Interpretation of kinds

In this section we interpret kinds as members of reducibility candidates. First we augment the schema interpretation

Definition 55 We augment $\mathcal{U}$ so that it maps a kind variable to an element of $\rho(u)_{\mathcal{K}}$, and a type variable to a pure term a.

Definition 56 We denote the interpretation of a type τ as $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau)$. To form this, we first construct the corresponding pure term $|\tau|$ and then substitute the type variables by the corresponding pure terms in $\mathcal{U}$. This is equivalent to $\mathcal{U}(|\tau|)$.

Definition 57 (Interpreting kinds) Consider a kind κ, a schema u, a mapping $\mathcal{K}$, and an interpretation $\mathcal{U}$. Suppose κ is well constructed of schema $\mathcal{K}(u)$ under $\mathcal{K}$ and $\mathcal{U}$. We define by recursion on κ:

1. $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(k) = \mathcal{U}(k)$
2. $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\Pi t : \kappa_1 . \kappa_2) = \{a \in \Lambda, \forall a_1 \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_1), a\ a_1 \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U},t:a_1}(\kappa_2)\}$
3. $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\Pi k : u_1 . \kappa_1) = \cap_{C \in \mathcal{CR}(u_1)_{\mathcal{K}}} \mathcal{C}^{\mathcal{K}}_{\mathcal{U},k:C}(\kappa_1)$
4. $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\Pi z : \mathsf{Kscm} . \kappa_1) = \cap_{u_1 \in \mathsf{arity}(u,\mathsf{Kind})} \mathcal{C}^{\mathcal{K},z:u_1}_{\mathcal{U}}(\kappa_1)$
5. $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_1\ \tau) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_1)\ \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau)$
6. $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_1\ \kappa_2) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_1)\ \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_2)$
7. $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\lambda t : \kappa_1 . \kappa_2) = a \in \Lambda \longmapsto \mathcal{C}^{\mathcal{K}}_{\mathcal{U},t:a}(\kappa_2)$
8. $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\lambda k : u_1 . \kappa_1) = C \in \mathcal{CR}(u_1)_{\mathcal{K}} \longmapsto \mathcal{C}^{\mathcal{K}}_{\mathcal{U},k:C}(\kappa_1)$
9. $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\mathsf{Ind}(k : \mathsf{Kind})\{\vec{\kappa}\}) =$ the least fixed point of the function F from $\rho_0(\mathsf{Kind})$ to $\rho_0(\mathsf{Kind})$ defined as :

   for all $\mathcal{S} \in \rho_0(\mathsf{Kind})$, for all C' in $\mathcal{CR}(I \to \mathsf{Kind})_{\mathcal{K}}$ (where $I = \mathsf{Ind}(k : \mathsf{Kind})\{\vec{\kappa}\}$), for all sequences of pure terms b_i, with for all i,

   $$b_i \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U},k:\mathcal{S},A':C',B':\mathsf{Co}(i)}(\zeta_{k,I}(\kappa_i, A', B'))$$

   $F(\mathcal{S})$ is the union of $min(\mathsf{Kind})$ with the set of pure terms a such that

   $$(\mathsf{match}\ t . \{\overrightarrow{\mathcal{C}^{\mathcal{K}}_{\mathcal{U},a_i:b_i}(\Upsilon(\kappa_i, a_i, \lambda t_2 . t\ t_2))}\})\ a \in C'\ a$$

10. $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\mathsf{Elim}[\kappa, u](\tau)\{\vec{\kappa'}\}) = G(\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa))$

    where $\kappa = \mathsf{Ind}(k : \mathsf{Kind})\{\vec{\kappa}\}$ is well constructed of schema Kind under $\mathcal{K}$ and $\mathcal{U}$ and $G(C) \in \rho(u)_{\mathcal{K}}$ is defined for all $C \in dom(<_\kappa)$ as follows ($<_\kappa$ is the order induced by the inductive definition κ):

    - If $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau)$ has a normal form $b = \mathsf{Co}(i)\ \vec{a}$ such that $b \in C$

      $$G(C) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U},t_1:G(\mathsf{pred}(b))}(\Phi_{k,I,t_1}(\kappa_i, \kappa'_i))\ (\vec{a})$$

    - $\mathsf{Can}(u)_{\mathcal{K}}$ otherwise

Lemma 40 The function F in Definition 57.9 is monotonic.

Proof We must prove that if $C_1 <_{\mathsf{Kind}} C_2$, then

$$\mathcal{C}^{\mathcal{K}}_{\mathcal{U},k:C_2,A':C',B':\mathsf{Co}(i)}(\zeta_{k,I}(\kappa_i, A', B')) <_{\mathsf{Kind}} \mathcal{C}^{\mathcal{K}}_{\mathcal{U},k:C_1,A':C',B':\mathsf{Co}(i)}(\zeta_{k,I}(\kappa_i, A', B'))$$

The proof is by induction on the fact that κ_i is the kind of a constructor.

- If $\kappa_i = k$, then both sides reduce to $C'\ \mathsf{Co}(i)$.
- If $\kappa_i = \Pi X : A_1.\, A_2$, then it follows directly from the induction hypothesis and because k does not occur in A_1.
- If $\kappa_i = \Pi \vec{X} : \vec{A}.\, k \to A_2$, then

$$\zeta_{k,I}(\kappa_i, A', B') = \Pi Z : (\Pi \vec{X} : \vec{A}.\, k).\, \Pi \vec{X'} : \vec{A}.\, (A'\ (Z\ \vec{X'})) \to \zeta_{k,I}(A_2, A', B'\ Z)$$

  Suppose $\mathcal{U}' = \mathcal{U}, k : C'', A' : C', B' : \mathsf{Co}(i)$ where C'' is either C_1 or C_2. The required set is then

$$\begin{array}{c} a \in \Lambda, \text{ such that } \forall a_1 \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U}'}(\Pi \vec{X} : \vec{A}.\, k), \\ \forall a_2 \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U}',Z:a_1}(\Pi \vec{X'} : \vec{A}.\, A'\ (Z\ \vec{X'})) \\ a\ a_1\ a_2 \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U}',Z:a_1}(\zeta_{k,I}(A_2, A', B'\ Z)) \end{array}$$

  The set of a_1 and a_2 is larger for the LHS. By the induction hypothesis, the result $a\ a_1\ a_2$ must occur in a smaller set for the LHS. The required result follows from this.

□

Remark 58 The previous lemma ensures that the interpretation of an inductive type sets up a well defined order. This ensures that the interpretation of large elimination (Definition 57.10) is well formed.

We get a bunch of substitution lemmas. The proof for each of these is similar and follows directly by induction over the structure of κ. We state them below:

Proposition 59 Let κ be a well constructed kind of schema u under $\mathcal{K}$ and $\mathcal{U}$. Let t be a type variable, and τ a type. We have that

$$\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}([\tau/t]\kappa) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U},t:\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau)}(\kappa)$$

Proposition 60 Let κ be a well constructed kind of schema u under $\mathcal{K}$ and $\mathcal{U}$. Let k be a kind variable and κ_1 a kind such that κ_1 is well constructed under $\mathcal{K}$ and $\mathcal{U}$ of the same schema as $\mathcal{U}(k)$. We have that

$$\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}([\kappa_1/k]\kappa) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U},k:\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_1)}(\kappa)$$

Proposition 61 Let κ be a well constructed kind of schema u under $\mathcal{K}$ and $\mathcal{U}$. Let z be a schema variable, and u_1 be a schema such that $\mathcal{K}(u_1)$ is an arity. We have that

$$\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}([u_1/z]\kappa) = \mathcal{C}^{\mathcal{K},z:\mathcal{K}(u_1)}_{\mathcal{U}}(\kappa)$$

D.3.7 Candidate interpretation of kinds

Definition 62 We say that $\mathcal{U}$ and $\mathcal{U}'$ are equivalent interpretations if for all k, we have that $\mathcal{U}(k) \simeq \mathcal{U}'(k)$ and for all t we have that $\mathcal{U}(t) =_{\beta\eta\iota} \mathcal{U}'(t)$.

Lemma 41 Let u be a schema, $\mathcal{K}$ be a mapping, and $\mathcal{U}$ and $\mathcal{U}'$ be two equivalent interpretations. Suppose κ is well constructed of schema $\mathcal{K}(u)$ under $\mathcal{K}$ and both $\mathcal{U}$ and $\mathcal{U}'$. Then $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa) \simeq_{\mathcal{K}(u)} \mathcal{C}^{\mathcal{K}}_{\mathcal{U}'}(\kappa)$.

Proof The proof is by induction over the structure of κ. Most of the cases follow directly from the induction hypothesis.

- $\kappa = \mathsf{Elim}[\kappa', u](\tau)\{\vec{\kappa'}\}$. Here $\kappa' = \mathsf{Ind}(k : \mathsf{Kind})\{\vec{\kappa}\}$. First note that $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa') = \mathcal{C}^{\mathcal{K}}_{\mathcal{U}'}(\kappa')$. Therefore, the function F whose lfp generates the inductive definition is the same. Moreover, $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau) =_{\beta\eta\iota} \mathcal{C}^{\mathcal{K}}_{\mathcal{U}'}(\tau)$. Since the set of pure terms is confluent, $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau)$ and $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}'}(\tau)$ have the same normal form. We can now do induction on the structure of κ_i to prove that

$$\mathcal{C}^{\mathcal{K}}_{\mathcal{U},t_1:G(\mathsf{pred}(b))}(\Phi_{k,I,t_1}(\kappa_i, \kappa_i')) \simeq \mathcal{C}^{\mathcal{K}}_{\mathcal{U}',t_1:G(\mathsf{pred}(b))}(\Phi_{k,I,t_1}(\kappa_i, \kappa_i'))$$

□

Lemma 42 Let $\mathcal{K}$ be a mapping, $\mathcal{U}$ a candidate interpretation, κ be a kind and u be a schema such that κ is a well constructed kind of schema $\mathcal{K}(u)$. Then $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa) \in \mathcal{CR}(u)_{\mathcal{K}}$.

Proof The proof is by induction over the structure of κ. Most of the cases follow in a direct way.

- $\kappa = \mathsf{Ind}(k : \mathsf{Kind})\{\vec{\kappa}\}$. We will use lemma 38 to prove this. For $\mathcal{S} \in \mathcal{CR}_0(\mathsf{Kind})$, the first condition is satisfied by lemma 35.
  - Suppose $\mathcal{S} = \bot$. If none of the branches is recursive then the function F is a constant function and the proof is similar to the non-bottom case. Suppose the ith branch is recursive. Then it is easy to see that the b_i defined as:

$$b_i \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U},k:\bot,A':C,B':\mathsf{Co}(i)}(\zeta_{k,I}(\kappa_i, A', B'))$$

    includes the set of all terms, including non-normalizing ones. Therefore, there are no terms a that would satisfy the condition that:

$$(\mathsf{match}\ t.\{\overrightarrow{\mathcal{C}^{\mathcal{K}}_{\mathcal{U},a_i:b_i}(\Upsilon(\kappa_i, a_i, \lambda t_2.t\ t_2))}\})\ a \in C\ a$$

    This implies that $F(\bot) = \bot$ and we know that $\bot \in \mathcal{CR}_0(\mathsf{Kind})$.
  - Consider any other $\mathcal{S}$. We will show that $F(\mathcal{S})$ satisfies the conditions in Definition 33 and hence belongs to $\mathcal{CR}_0(\mathsf{Kind})$. $F(\mathcal{S})$ is defined as the union of $min(\mathsf{Kind})$ with the set of pure terms a such that

$$(\mathsf{match}\ t.\{\overrightarrow{\mathcal{C}^{\mathcal{K}}_{\mathcal{U},a_i:b_i}(\Upsilon(\kappa_i, a_i, \lambda t_2.t\ t_2))}\})\ a \in C\ a$$

    Since C is a candidate, the terms a must be strongly normalizing.
    To see that the set is closed under reduction, suppose $a \rhd a'$. Since C is a candidate we have that $(\mathsf{match}\ t.\{\dots\})\ a' \in C\ a$. Moreover, we have that $C\ a = C\ a'$. Therefore, a' is also in the generated set. Suppose a is a neutral term and for all a' such that $a \rhd a'$, we have that a' belongs to this set. We have to prove that a belongs to this set. This implies that we must prove:

$$(\mathsf{match}\ t.\{\overrightarrow{\mathcal{C}^{\mathcal{K}}_{\mathcal{U},a_i:b_i}(\Upsilon(\kappa_i, a_i, \lambda t_2.t\ t_2))}\})\ a \in C\ a$$

    Since a is a neutral term, the above term does not have a redex at the head. From the induction hypothesis, we get that $\mathcal{C}^{\mathcal{K}}_{\mathcal{U},k:\mathcal{S},A':C,B':\mathsf{Co}(i)}(\zeta_{k,I}(\kappa_i, A', B'))$ is a candidate and therefore closed under reduction. Moreover, the b_i are strongly normalizing. We can now consider all possible redices and prove by induction over $\nu(b_i)$ that the above condition is satisfied.

- $\kappa = \mathsf{Elim}[\kappa', u](\tau)\{\vec{\kappa'}\}$ where $\kappa' = \mathsf{Ind}(k:\mathsf{Kind})\{\vec{\kappa}\}$. First note that $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa')$ is a candidate by induction and gives rise to a well founded order on $\mathcal{CR}_0(\mathsf{Kind})$. We will do induction on this order. Suppose $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa) = G(\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa'))$. We will show that for all sets $\mathcal{S}$ belonging to the order generated by κ', and for all pure terms b, we have that $G(\mathcal{S}) \in \mathcal{CR}(u)_{\mathcal{K}}$. For the non-recursive case, the proof is immediate. For the recursive case, consider $\mathcal{C}^{\mathcal{K}}_{\mathcal{U},t_1:G(\mathsf{pred}(b))}(\Phi_{k,\kappa',t_1}(\kappa_i, \kappa'_i))$. Note that $\mathsf{pred}(b)$ belongs to the same order. The required result follows now by doing induction over the structure of κ_i and applying the induction hypothesis to $G(\mathsf{pred}(b))$.

□

Definition 63 Suppose Δ is a context and $\mathcal{K}$ and $\mathcal{U}$ are a mapping and an interpretation. We say that $\mathcal{K}$ and $\mathcal{U}$ are adapted to Δ if:

- $\forall z \in \Delta$, we have that $\mathcal{K}(z)$ is an arity and $\cdot \vdash \mathcal{K}(z) : \mathsf{Kscm}$.
- $\forall k \in \Delta$, we have that $\mathcal{U}(k) \in \mathcal{CR}(\Delta(k))_{\mathcal{K}}$.
- $\forall t \in \Delta$, we have that $\mathcal{U}(t) \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\Delta(t))$.

D.3.8 Interpretation of abstractions

We get a bunch of lemmas that state that an abstraction at the type level belongs to the corresponding kind. The proof of each of these lemmas is straightforward and follows in a similar way. We will show the proof for only one of the lemmas.

Lemma 43 Let $\Delta \vdash \lambda t:\kappa.\,\tau : \Pi t:\kappa.\,\kappa_1$ be a judgment and $\mathcal{K}$ and $\mathcal{U}$ be a mapping and a candidate interpretation adapted to Δ. We have $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\lambda t:\kappa.\,\tau) \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\Pi t:\kappa.\,\kappa_1)$ if and only if for all pure terms $a \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa)$, we have that $\mathcal{C}^{\mathcal{K}}_{\mathcal{U},t:a}(\tau) \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U},t:a}(\kappa_1)$.

Lemma 44 Let $\Delta \vdash \lambda k:u.\,\tau : \Pi k:u.\,\kappa$ be a judgment and $\mathcal{K}$ and $\mathcal{U}$ be a mapping and a candidate interpretation adapted to Δ. We have $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\lambda k:u.\,\tau) \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\Pi k:u.\,\kappa)$ if and only if for all reducibility candidates $C \in \mathcal{CR}(u)_{\mathcal{K}}$ we have that $\mathcal{C}^{\mathcal{K}}_{\mathcal{U},k:C}(\tau) \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U},k:C}(\kappa)$.

Lemma 45 Let $\Delta \vdash \lambda z:\mathsf{Kscm}.\,\tau : \Pi z:\mathsf{Kscm}.\,\kappa$ be a judgment and $\mathcal{K}$ and $\mathcal{U}$ be a mapping and a candidate interpretation adapted to Δ. We have $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\lambda z:\mathsf{Kscm}.\,\tau) \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\Pi z:\mathsf{Kscm}.\,\kappa)$ if and only if for all $u \in \mathsf{arity}(u', \mathsf{Kind})$ we have that $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau) \in \mathcal{C}^{\mathcal{K},z:u}_{\mathcal{U}}(\kappa)$.

Proof By definition $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\lambda z : \mathsf{Kscm}.\,\tau) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau)$. Similarly $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\Pi z:\mathsf{Kscm}.\,\kappa) = \cap_{u_1 \in \mathsf{arity}(u,\mathsf{Kind})}\mathcal{C}^{\mathcal{K},z:u_1}_{\mathcal{U}}(\kappa)$. The *if* part follows directly from the definition.

For the *only if*, suppose that $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau) \in \mathcal{C}^{\mathcal{K},z:u}_{\mathcal{U}}(\kappa)$ for all arities u. This implies that $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau) \in \cap_{u_1 \in \mathsf{arity}(u,\mathsf{Kind})}\mathcal{C}^{\mathcal{K},z:u_1}_{\mathcal{U}}(\kappa)$. This implies that $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau) \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\Pi z:\mathsf{Kscm}.\,\kappa)$. □

D.3.9 Interpretation of weak elimination

For this section $\kappa = \mathsf{Ind}(k : \mathsf{Kind})\{\vec{\kappa}\}$. Suppose also that $C \in \mathcal{CR}(\kappa \to \mathsf{Kind})_{\mathcal{K}}$ and $\tau_i \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U},A':C,B':\mathsf{Co}(i)}(\zeta_{k,I}(\kappa_i, A', B'))$.

Lemma 46 Suppose $a \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa)$. We have then

$$(\mathsf{match}\, t.\{\overrightarrow{\Upsilon(\kappa_i, \tau_i, \lambda t_2.t\, t_2)}\})\ a \in C\ a$$

Proof Follows immediately from the definition of $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa)$. □

Lemma 47 Let $\Delta \vdash \mathsf{Elim}[\kappa, \kappa_1](\tau)\{\vec{\tau'}\} : \kappa_1$ be a derivable judgment where κ_1 is a kind. Suppose $\mathcal{K}$ is a mapping and $\mathcal{U}$ is a candidate interpretation adapted to Δ. If $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau) \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa)$ and $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau'_i) \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\zeta_{k,I}(\kappa_i, \kappa_1, \mathsf{Ctor}\,(i, \kappa)))$, then we have

$$\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\mathsf{Elim}[\kappa, \kappa_1](\tau)\{\vec{\tau'}\}) \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_1)$$

Proof Follows now from the previous lemma. □

D.3.10 Interpretation of constructors

For this section, suppose $I = \kappa = \mathsf{Ind}(k : \mathsf{Kind})\{\vec{\kappa}\}$. Also, suppose $C \in \mathcal{CR}(I \to \mathsf{Kind})_{\mathcal{K}}$.

Lemma 48 For all i, $\mathsf{Co}(i) \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_i)$.

Proof We know that κ_i is of the form $\Pi\vec{X} : \vec{A}.\,k$. Suppose $\vec{B} \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U},k:\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(I)}(\vec{X} : \vec{A})$. Then we need to prove that $\mathsf{Co}(i)\ \vec{B} \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(I)$. This means that we need to prove that

$$(\mathsf{match}\, t.\{\overrightarrow{\Upsilon(\kappa_i, a_i, \lambda t_2.t\, t_2)}\})\ (\mathsf{Co}(i)\ \vec{B}) \in C\ (\mathsf{Co}(i)\ \vec{B})$$

where a_i belongs to the appropriate candidate. This implies that we need to prove that

$$\Upsilon(\kappa_i, a_i, \lambda t_2.\mathsf{match}\, t.\{\dots\}\, t_2)\ \vec{B} \in C\ (\mathsf{Co}(i)\ \vec{B})$$

This follows directly by an induction over the structure of κ_i. □

D.3.11 Invariance under β reduction

In this section, we show that the interpretation of kinds remains invariant under β reduction.

Lemma 49 Let κ be a well constructed kind of schema u under a mapping $\mathcal{K}$ and candidate interpretation $\mathcal{U}$. If $\kappa \rhd_\beta \kappa'$, then κ' is well constructed of schema u under $\mathcal{K}$ and $\mathcal{U}$, and $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa')$.

Proof The proof is by induction over the structure of κ. Most of the cases follow directly from the induction hypothesis. We will only consider β reductions at the head.

- $\kappa = (\lambda t:\kappa_1.\,\kappa_2)\ \tau$. By definition,

  $$\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}((\lambda t:\kappa_1.\,\kappa_2)\ \tau) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\lambda t:\kappa_1.\,\kappa_2)\ \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau)$$

  Again by definition this is equal to $\mathcal{C}^{\mathcal{K}}_{\mathcal{U},t:\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau)}(\kappa_2)$. By proposition 59 this is equal to $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}([\tau/t]\kappa_2)$
- $\kappa = (\lambda k:u_1.\,\kappa_1)\ \kappa_2$. By definition,

  $$\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}((\lambda k:u_1.\,\kappa_1)\ \kappa_2) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\lambda k:u_1.\,\kappa_1)\ \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_2)$$

  By lemma 42 we have that $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_2) \in \mathcal{CR}(u_1)_{\mathcal{K}}$. Therefore, we get that

  $$\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}((\lambda k:u_1.\,\kappa_1)\ \kappa_2) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U},k:\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_2)}(\kappa_1)$$

  By proposition 60 this is equal to $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}([\kappa_2/k]\kappa_1)$.

□

D.3.12 Invariance under η reduction

In this section, we show that the interpretation remains the same under η reduction. The unmarked terms $\| \kappa \|$ are defined in Section D.2.1.

Lemma 50 Let κ be a well constructed kind of schema u under a mapping $\mathcal{K}$ and candidate interpretation $\mathcal{U}$. If $\kappa \rhd_\eta \kappa'$, then κ' is well constructed of schema u under $\mathcal{K}$ and $\mathcal{U}$, and $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa')$.

Proof The proof is again by induction over the structure of κ. We will consider only the cases where the reduction occurs at the head.

- $\kappa = \lambda t\!:\!\kappa_1.\ (\kappa_2\ t)$. By definition $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa)$ is equal to:

  $$a \in \Lambda \longmapsto \mathcal{C}^{\mathcal{K}}_{\mathcal{U},t:a}(\kappa_2)\ \mathcal{C}^{\mathcal{K}}_{\mathcal{U},t:a}(t)$$

  Since t does not occur free in κ_2, this is equivalent to

  $$a \in \Lambda \longmapsto \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_2)\ a$$

  Since a does not occur free now in $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_2)$, we get that this is equivalent to $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_2)$. Note from Definition 34 that the domain of $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_2)$ is Λ.

- $\kappa = \lambda k\!:\!u_1.\ (\kappa_2\ k)$. By definition $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa)$ is equal to:

  $$C \in \mathcal{CR}(u_1)_{\mathcal{K}} \longmapsto \mathcal{C}^{\mathcal{K}}_{\mathcal{U},k:C}(\kappa_2)\ \mathcal{C}^{\mathcal{K}}_{\mathcal{U},k:C}(k)$$

  Since k does not occur free in κ_2, this is equivalent to

  $$C \in \mathcal{CR}(u_1)_{\mathcal{K}} \longmapsto \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_2)\ C$$

  Since C does not occur free now in $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_2)$, we get that this is equivalent to $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_2)$. Note from Definition 34 that the domain of $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_2)$ is $\mathcal{CR}(u_1)_{\mathcal{K}}$.

□

Lemma 51 For all well constructed kinds κ of schema u under $\mathcal{K}$ and $\mathcal{U}$, we have $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\| \kappa \|)$.

Proof Follows from the fact that $\kappa =_{\beta\eta} \| \kappa \|$. □

D.3.13 Invariance under ι reduction

In this section we essentially show that interpretation remains the same under large elimination.

Lemma 52 Let $\mathsf{Elim}[\kappa, u](\tau)\{\vec{\kappa'}\}$ be well constructed of schema $\mathcal{K}(u)$ under $\mathcal{K}$ and $\mathcal{U}$. Suppose $\kappa = \mathsf{Ind}(k\!:\!\mathsf{Kind})\{\vec{\kappa}\}$. Suppose G is the function used for the interpretation of the large elimination. If $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau) \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa)$, then for all $C \in \mathcal{CR}_0(\mathsf{Kind})$ with $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau) \in C$, we have that $G(\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa)) = G(C)$.

Proof The proof is immediate. □

Lemma 53 Suppose $I = \kappa = \mathsf{Ind}(k\!:\!\mathsf{Kind})\{\vec{\kappa}\}$. Suppose the constructors of I are all small. Suppose the mth constructor of I has the form $\Pi\vec{Y}\!:\!\vec{B}.\ k$ and we have a sequence of terms $\vec{b}$ such that $\mathsf{Co}(m)\ \vec{b} \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(I)$. Then we have that $b_i \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U},\forall k<i.Y_k:b_k,k:\mathsf{pred}(\mathsf{Co}(m)\ \vec{b})}(B_i)$.

Proof We can have two cases.

- $\mathsf{pred}(\mathsf{Co}(m)\ \vec{b}) \neq \bot$
  This implies that $\mathsf{pred}(\mathsf{Co}(m)\ \vec{b}) \in \mathcal{CR}_0(\mathsf{Kind})$. Suppose $\mathcal{S} = \mathcal{C}^{\mathcal{K}}_{\mathcal{U},\forall k<i.Y_k:b_k,k:\mathsf{pred}(\mathsf{Co}(m)\ \vec{b})}(B_i)$. Then we have that $\mathcal{S}$ is a candidate of schema Kind. Suppose also that C' belongs to $\mathcal{CR}(I \to \mathsf{Kind})_{\mathcal{K}}$ and maps elements in the domain of $I \to \mathsf{Kind}$ to $\mathcal{S}$. Then for all indices i', we have that $\mathcal{C}^{\mathcal{K}}_{\mathcal{U},k:\mathsf{pred}(\mathsf{Co}(m)\ \vec{b}),A':C'}(\zeta_{k,I}(\kappa_{i'}, A', \mathsf{Ctor}\,(i', I)))$ is a reducibility candidate of Kind.

  To prove the lemma we need to show that if for all indices i

  $$\tau_i \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U},k:\mathsf{pred}(\mathsf{Co}(m)\ \vec{b}),A':C'}(\zeta_{k,I}(\kappa_i, A', \mathsf{Ctor}\,(i, I)))$$

  then we have that $\Phi_{k,I,B'}(\kappa_m, \tau_m)$ can reduce to b_i by a head reduction. To have this, for the indices $i \neq m$ choose τ_i as some variable. For τ_m choose the term that returns the ith argument of the constructor.

- $\mathsf{pred}(\mathsf{Co}(m)\ \vec{b}) = \bot$ We can show that the constructors now are not recursive. Hence k does not occur free in any of the B_is. The proof for the previous case can be reused here.

□

Lemma 54 Let $\Delta \vdash \mathsf{Elim}[\kappa, u](\tau)\{\vec{\kappa'}\} : u$ be a derivable judgment. Let $\mathcal{K}$ be a mapping and $\mathcal{U}$ be an interpretation adapted to Δ. Suppose $I = \kappa = \mathsf{Ind}(k\!:\!\mathsf{Kind})\{\vec{\kappa}\}$. Suppose $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau) \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa)$ and $\tau \rhd^*\ \mathsf{Ctor}\,(i, \kappa)\ \vec{A}$. Also suppose $B' = \lambda t\!:\!I.\,\mathsf{Elim}[\kappa, u](t)\{\vec{\kappa'}\}$. We then have that $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\mathsf{Elim}[\kappa, u](\tau)\{\vec{\kappa'}\}) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\Phi_{k,I,B'}(\kappa_i, \kappa'_i)\ (\vec{A}))$.

Proof Let G be the function used for interpreting large elimination. Suppose $\mathsf{Co}(i)\ \vec{a}$ is the normal form of $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau)$. Then given the assumptions we have that:

$$\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\mathsf{Elim}[\kappa, u](\tau)\{\vec{\kappa'}\}) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U},B':G(\mathsf{pred}(\mathsf{Co}(i)\ \vec{a}))}(\Phi_{k,I,B'}(\kappa_i, \kappa'_i))\ (\vec{a})$$

We therefore have to prove that

$$\mathcal{C}^{\mathcal{K}}_{\mathcal{U},B':G(\mathsf{pred}(\mathsf{Co}(i)\ \vec{a}))}(\Phi_{k,I,B'}(\kappa_i, \kappa'_i))\ (\vec{a}) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\Phi_{k,I,B'}(\kappa_i, \kappa'_i)\ (\vec{A}))$$

- $\kappa_i = k$ it follows directly.
- $\kappa_i = \Pi t\!:\!\kappa_1.\ \kappa_2$ We have to prove that

  $$\mathcal{C}^{\mathcal{K}}_{\mathcal{U},B':G(\mathsf{pred}(\mathsf{Co}(i)\ \vec{a})),t:a_1}(\Phi_{k,I,B'}(\kappa_2, \kappa'_i\ t))\ (a_{2..n}) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U},t:a_1}(\Phi_{k,I,B'}(\kappa_2, \kappa'_i\ t)\ (A_{2..n}))$$

  Applying the induction hypothesis leads to the result.

- $\kappa_i = \Pi\vec{t}\!:\!\vec{\kappa}.\ k \to \kappa_2$ The LHS becomes

  $$\mathcal{C}^{\mathcal{K}}_{\mathcal{U}'}(\Phi_{k,I,B'}(\kappa_2, \kappa'_i t(\lambda\vec{Y}\!:\!\vec{\kappa}.\ B'(t\vec{Y}))))\ (a_{2..n})$$
  $$\text{where } \mathcal{U}' = \mathcal{U}, B' : G(\mathsf{pred}(\mathsf{Co}(i)\ \vec{a})), t : a_1$$

  By lemma 53, a_1 belongs to $\mathcal{C}^{\mathcal{K}}_{\mathcal{U},k:\mathsf{pred}(\mathsf{Co}(i)\ \vec{a})}(\Pi\vec{t}\!:\!\vec{\kappa}.\ k)$. This implies that $a_1\ \vec{Y} \in \mathsf{pred}(\mathsf{Co}(i)\ \vec{a})$. Moreover, by lemma 52 $G(\mathsf{pred}(\mathsf{Co}(i)\ \vec{a}))(a_1\ \vec{Y})$ is equal to $G(\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa))(a_1\ \vec{Y})$ and which is in turn equal to $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\mathsf{Elim}[\kappa, u](A_1\ \vec{Y})\{\vec{\kappa'}\})$. The required result follows directly from here by performing one head reduction on the RHS and applying the induction hypothesis.

□

D.3.14 Kinds invariant on their domain

Definition 64 Let $\Delta \vdash \kappa : u$ be a derivable judgment and $\mathcal{K}$ and $\mathcal{U}$ be a mapping and an interpretation adapted to Δ. We say $(\kappa, u, \Delta, \mathcal{K}, \mathcal{U})$ is invariant if:

- $u = \mathsf{Kind}$ and for all κ' such that $\kappa \rhd^* \kappa'$, we have that $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa')$;
- $u = \Pi t\!:\!\kappa_1.\, u_1$ then for all derivable judgments $\Delta \vdash \tau : \kappa_1$ and $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau) \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_1)$, we have that $(\kappa\ \tau, [\tau/t]u_1, \Delta, \mathcal{K}, \mathcal{U})$ is invariant;
- $u = \Pi k : u_1.\, u_2$ then for all derivable judgments $\Delta \vdash \kappa_1 : u_1$, we have that $(\kappa\ \kappa_1, [\kappa_1/k]u_2, \Delta, \mathcal{K}, \mathcal{U})$ is invariant.
- $u = z$ and we have that $(\mathcal{K}(\kappa), \mathcal{K}(u), \mathcal{K}(\Delta), \mathcal{K}, \mathcal{U})$ is invariant.

Lemma 55 Let $\Delta \vdash \kappa_1 : \mathsf{Kind}$ and $\Delta \vdash \kappa_2 : \mathsf{Kind}$ be two derivable judgments and $\mathcal{K}$ and $\mathcal{U}$ be a mapping and an interpretation adapted to Δ. If $(\kappa_1, \mathsf{Kind}, \Delta, \mathcal{K}, \mathcal{U})$ and $(\kappa_2, \mathsf{Kind}, \Delta, \mathcal{K}, \mathcal{U})$ are invariant and $\kappa_1 =_{\beta\eta\iota} \kappa_2$, then $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_1) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_2)$.

Proof We know that there exists a B such that $\| \kappa_1 \| \rhd^* B$ and $\| \kappa_2 \| \rhd^* B$. This implies that there exists a κ_1' and a κ_2' (lemma 13 and 12) such that $\kappa_1 \rhd_{\beta\iota} \kappa_1'$ and $\| \kappa_1' \| \rhd^*_\eta B$. Similarly, $\kappa_2 \rhd_{\beta\iota} \kappa_2'$ and $\| \kappa_2' \| \rhd^*_\eta B$. From here we get that

$$\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_1) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_1') = \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(B) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_2') = \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_2)$$

□

Proposition 65 If $([\tau/t]\kappa, u, \Delta, \mathcal{K}, \mathcal{U})$ is invariant, and also $\Delta \vdash (\lambda t\!:\!\kappa_1.\, \kappa)\ \tau : u$, then $((\lambda t\!:\!\kappa_1.\, \kappa)\ \tau, u, \Delta, \mathcal{K}, \mathcal{U})$ is invariant.

D.3.15 Interpretation of large elimination

Lemma 56 Let $\Delta \vdash \mathsf{Elim}[\kappa, u](\tau)\{\vec{\kappa'}\} : u$ be a judgment. Suppose $I = \kappa = \mathsf{Ind}(k\!:\!\mathsf{Kind})\{\vec{\kappa}\}$. Let $\mathcal{K}$ and $\mathcal{U}$ be a mapping and an interpretation adapted to Δ. Suppose

1. $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau) \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa)$.
2. for all i, $(\kappa_i', \Psi_{k,I}(\kappa_i, u), \Delta, \mathcal{K}, \mathcal{U})$ is invariant.

Then we have that $(\mathsf{Elim}[\kappa, u](\tau)\{\vec{\kappa'}\}, u, \Delta, \mathcal{K}, \mathcal{U})$ is invariant.

Proof Suppose $\kappa_1 = \mathsf{Elim}[\kappa, u](\tau)\{\vec{\kappa'}\}$. Suppose we are given a sequence of terms $\vec{A}$ of the proper type so that $\kappa_1\ \vec{A}$ is in Kind. To show the invariance, we have to show that if $\kappa_1\ \vec{A} \rhd^* \kappa_2$, then $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_1\ \vec{A}) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_2)$. We will reason by induction on $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau)$ over the order defined by I.

- If the term $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau)$ can not be reduced to a term of the form $\mathsf{Co}(i)\vec{a}$, then it is minimal with respect to the order defined by I. Then κ_2 is necessarily of the form $\mathsf{Elim}[\kappa', u'](\tau')\{\vec{\kappa''}\}\ \vec{A'}$ and we have that the interpretation of both $\kappa_1\ \vec{A}$ and κ_2 is $\mathsf{Can}_0(\mathsf{Kind})$.
- Suppose the term $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau)$ can be reduced to a term of the form $\mathsf{Co}(i)\vec{a}$, but τ is not reduced to a term of the form $\mathsf{Ctor}\,(i, I)\vec{C}$. Then κ_2 is again of the form $\mathsf{Elim}[\kappa''', u'](\tau')\{\vec{\kappa''}\}\ \vec{A'}$. By definition, we have that

$$B_1 = \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_1\ \vec{A}) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U},\vec{t}:\vec{a}}(\Phi_{k,I,B'}(\kappa_i, \kappa_i')\ (\vec{t})\vec{A})$$
$$B_2 = \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_2) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U},\vec{t}:\vec{a}}(\Phi_{k,I',B''}(\kappa_i'', \kappa_i'')\ (\vec{t})\vec{A'})$$

  where $B' = \lambda Y : I.\, \mathsf{Elim}[\kappa, u](\tau)\{\vec{\kappa'}\}$, and $B'' = \lambda Y : I'.\, \mathsf{Elim}[\kappa''', u'](\tau')\{\vec{\kappa''}\}$. It is evident that B_2 is a reduct of B_1, and therefore we need to prove that $(B_1, \mathsf{Kind}, \Delta, \mathcal{K}, \mathcal{U})$ is invariant.

  This follows by an induction over the structure of κ_i and by using the condition 2. The non-recursive cases follow directly. For the recursive case, we use lemma 53 to show that B' is applied to a smaller argument with respect to the order defined by I.
- We are left with the case when τ reduces to a term of the form $\mathsf{Ctor}\,(i, I)\vec{C}$. In going from $\kappa_1\ \vec{A}$ to κ_2, we will now have a ι reduction. The sequence of reductions is now

$$\begin{aligned}\kappa_1\ \vec{A} &\rhd^* \mathsf{Elim}[\kappa, u](\mathsf{Ctor}\,(i, I)\vec{A})\{\vec{\kappa'}\} \\ &\rhd_\iota (\Phi_{k,I,\kappa_i'}(\kappa_i, B')\ (\vec{B}))\vec{A} \\ &\rhd^* \kappa_2\end{aligned}$$

  The first reduction does not change the interpretation since we are reducing only a type. By lemma 54, the second does not change the interpretation. Finally, as above, we can prove that the result of the ι reduction is invariant over Kind.

□

D.3.16 Instantiation of contexts

Definition 66 Let Δ be a well formed context. Let Θ be a context and ϕ be a mapping from variables to terms such that $\forall X \notin \Delta, \phi(X) = X$.

We say that (Θ, ϕ) is an instantiation of Δ if for all variables $X \in \Delta$, we have that $\Theta \vdash \phi(X) : \phi(\Delta(X))$.

Lemma 57 Let $\Delta \vdash A : B$ be a derivable judgment and (Θ, ϕ) an instantiation of Δ. Then $\Theta \vdash \phi(A) : \phi(B)$.

Proof By induction over the structure of A. □

Definition 67 (Adapted instantiation) We say that an instantiation (Θ, ϕ) is adapted to a context Δ if:

- for all $t \in \Delta$, $\phi(t) \in \mathcal{C}^{\emptyset}_{\mathsf{Can}_0(\Theta)}(\phi(\Delta(t)))$;
- for all $k \in \Delta$, $(\phi(k), \phi(\Delta(k)), \Theta, \emptyset, \mathsf{Can}_0(\Theta))$ is invariant;
- for all $z \in \Delta$, $(\phi(z), \mathsf{Kscm}, \Theta, \emptyset, \mathsf{Can}_0(\Theta))$ is invariant and $\phi(z)$ is an arity.

Definition 68 Suppose $\Delta \vdash \kappa : u$ is a derivable judgment. We say that all instantiations of (κ, u, Δ) are invariant if for all instantiations (Θ, ϕ) adapted to Δ and for all interpretations $\mathcal{U}$ adapted to Θ, we have that $(\phi(\kappa), \phi(u), \Theta, \emptyset, \mathcal{U})$ is invariant.

D.3.17 Kind schema invariant on their domain

Definition 69 Let $\Delta \vdash u : \mathsf{Kscm}$ be a derivable judgment and $\mathcal{K}$ and $\mathcal{U}$ be a mapping and an interpretation adapted to Δ. We say that $(u, \mathsf{Kscm}, \Delta, \mathcal{K}, \mathcal{U})$ is invariant:

- if $u = \mathsf{Kind}$, then $(u, \mathsf{Kscm}, \Delta, \mathcal{K}, \mathcal{U})$ is invariant;
- if $u = \Pi t : \kappa_1.\, u_1$, then it is invariant if and only if $(\kappa_1, \mathsf{Kind}, \Delta, \mathcal{K}, \mathcal{U})$ is invariant and for all terms τ such that $\Delta \vdash \tau : \kappa_1$ is derivable and $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau) \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_1)$, we have that $([\tau/t]u_1, \mathsf{Kscm}, \Delta, \mathcal{K}, \mathcal{U})$ is invariant;

- if $u = \Pi k : u_1 . u_2$, then it is invariant if and only if $(u_1, \mathsf{Kscm}, \Delta, \mathcal{K}, \mathcal{U})$ is invariant, and for all kinds κ such that $\Delta \vdash \kappa : u_1$ is derivable and $(\kappa, u_1, \Delta, \mathcal{K}, \mathcal{U})$ is invariant, we have that $([\kappa/k]u_2, \mathsf{Kscm}, \Delta, \mathcal{K}, \mathcal{U})$ is invariant;
- if $u = z$, then it is invariant *iff* $(\mathcal{K}(z), \mathsf{Kscm}, \Delta, \mathcal{K}, \mathcal{U})$ is invariant.

Lemma 58 Let $\Delta \vdash \kappa : u$ and $\Delta \vdash u' : \mathsf{Kscm}$ be derivable judgments. Let $\mathcal{K}$ and $\mathcal{U}$ be a mapping and an interpretation adapted to Δ. Suppose $u =_{\beta\eta\iota} u'$, and $(u, \mathsf{Kscm}, \Delta, \mathcal{K}, \mathcal{U})$ and $(u', \mathsf{Kscm}, \Delta, \mathcal{K}, \mathcal{U})$ are invariant. If $(\kappa, u, \Delta, \mathcal{K}, \mathcal{U})$ is invariant, then $(\kappa, u', \Delta, \mathcal{K}, \mathcal{U})$ is also invariant.

Proof The proof is by induction over the structure of u and u'.

- if $u = u' = \mathsf{Kind}$, then it is trivially true.
- if $u = u' = z$, then again it is trivially true.
- if $u = \Pi t : \kappa_1 . u_1$ and $u' = \Pi t : \kappa_2 . u_2$, then we have that $\kappa_1 =_{\beta\eta\iota} \kappa_2$ and $u_1 =_{\beta\eta\iota} u_2$. By assumption, we know that $(\kappa_1, \mathsf{Kind}, \Delta, \mathcal{K}, \mathcal{U})$ and $(\kappa_2, \mathsf{Kind}, \Delta, \mathcal{K}, \mathcal{U})$ are invariant. This means that $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_1) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa_2)$. Moreover, $\Delta \vdash \tau : \kappa_1$ is true *iff* $\Delta \vdash \tau : \kappa_2$ is true. Applying the induction hypothesis now leads to the required result.
- if $u = \Pi k : u_1 . u_2$ and $u' = \Pi k : u_1' . u_2'$, the proof is similar to the previous case.

□

Definition 70 Suppose $\Delta \vdash u : \mathsf{Kscm}$ is a derivable judgment. We say that all instantiations of $(u, \mathsf{Kscm}, \Delta)$ are invariant if for all instantiations (Θ, ϕ) adapted to Δ and for all interpretations $\mathcal{U}$ adapted to Θ, we have that $(\phi(u), \mathsf{Kscm}, \Theta, \emptyset, \mathcal{U})$ is invariant.

D.3.18 Strong normalization of pure terms

Theorem 71 Let $\Delta \vdash \tau : \kappa$ be a derivable judgment and $\mathcal{K}$ and $\mathcal{U}$ be a mapping and an interpretation adapted to Δ. Then $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau) \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa)$.

Proof The proof is by induction over the length of the derivation. The induction hypothesis are as follows:

- if $\Delta \vdash \tau : \kappa$ and $\mathcal{K}$ and $\mathcal{U}$ be a mapping and an interpretation adapted to Δ, then $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau) \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\kappa)$;
- if $\Delta \vdash \kappa : u$, then all instantiations of (κ, u, Δ) are invariant;
- if $\Delta \vdash u : \mathsf{Kscm}$, then all instantiations of $(u, \mathsf{Kscm}, \Delta)$ are invariant;

type formation rules This paragraph deals with rules of the form $\Delta \vdash \tau : \kappa$.

- abstractions – Follows directly from the induction hypothesis and lemmas 43 and 44 and 45.
- var – Follows because the interpretation $\mathcal{U}$ is adapted to the context Δ.
- weak elimination – Follows from lemma 47.
- constructor – Follows from lemma 48.
- weakening – Follows directly from the induction hypothesis since the mapping and interpretation remain adapted for a smaller context.
- conv – Follows from the recursion hypothesis and lemma 55.
- app – All three cases of app are proved similarly. We will show only one case here.
  - $\Delta \vdash \tau[u'] : \kappa$. Then we know that $\Delta \vdash \tau : \Pi z : \mathsf{Kscm} . \kappa_1$ and $\Delta \vdash u' : \mathsf{Kscm}$ and $[u'/z]\kappa_1 = \kappa$. By the induction hypothesis
    $$\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau) \in \cap_{u_1 \in \mathsf{arity}(u, \mathsf{Kind})} \mathcal{C}^{\mathcal{K}, z:u_1}_{\mathcal{U}}(\kappa_1)$$
    Suppose $u_1' = \mathcal{K}(u')$. Then we know that $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau) \in \mathcal{C}^{\mathcal{K}, z:u_1'}_{\mathcal{U}}(\kappa_1)$. By proposition 61 we know that $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau) \in \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}([u'/z]\kappa_1)$. But $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau[u']) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau)$.

kind formation rules This paragraph deals with rules of the form $\Delta \vdash \kappa : u$.

- product – All the product formation rules are proved in the same way. We show only one case here.
  - Consider the following formation rule
    $$\frac{\Delta, z : \mathsf{Kscm} \vdash \kappa : \mathsf{Kind}}{\Delta \vdash \Pi z : \mathsf{Kscm} . \kappa : \mathsf{Kind}}$$
    We have to prove that for all instantiations (Θ, ϕ) we have that $(\Pi z : \mathsf{Kscm} . \phi(\kappa), \mathsf{Kind}, \Theta, \emptyset, \mathcal{U})$ is invariant. This implies that we must prove that if $\kappa \rhd \kappa'$, then $\mathcal{C}^{\emptyset}_{\mathcal{U}}(\Pi z : \mathsf{Kscm} . \phi(\kappa)) = \mathcal{C}^{\emptyset}_{\mathcal{U}}(\Pi z : \mathsf{Kscm} . \phi(\kappa'))$. By the induction hypothesis, for all instantiations $(\Theta, \phi; z : \mathsf{arity}(u, \mathsf{Kind}))$ we have that
    $$(\phi; z : \mathsf{arity}(u, \mathsf{Kind})(\kappa), \mathsf{Kind}, \Theta, \emptyset, \mathcal{U})$$
    is invariant. This implies that if $\kappa \rhd \kappa'$ then
    $$\mathcal{C}^{z:\mathsf{arity}(u, \mathsf{Kind})}_{\mathcal{U}}(\kappa) = \mathcal{C}^{z:\mathsf{arity}(u, \mathsf{Kind})}_{\mathcal{U}}(\kappa')$$
    The required result follows from here.
- var – follows since the instantiation is adapted.
- conv – follows from lemma 58.
- application – Both of the applications are proved similarly and follow directly from the induction hypothesis. We will show only one case here.
  - If $\Delta \vdash \kappa_1\ \kappa_2 : [\kappa_2/k]u$, then given Θ, ϕ, and $\mathcal{U}$, we must prove that $(\phi(\kappa_1\ \kappa_2), \phi([\kappa_2/k]u), \Theta, \emptyset, \mathcal{U})$ is invariant. But by the induction hypothesis we know that $(\phi(\kappa_1), \phi(\Pi k : u_1 . u), \Theta, \emptyset, \mathcal{U})$ is invariant and $\Delta \vdash \kappa_2 : u_1$. By lemma 57 $\Theta \vdash \phi(\kappa_2) : \phi(u_1)$. This leads to the required result.
- ind – Suppose $I = \mathsf{Ind}(k : \mathsf{Kind})\{\vec{\kappa}\}$. Note that $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(I)$ depends only on $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}, k:\mathcal{S}, A':C, B':\mathsf{Co}(i)}(\zeta_{k,I}(\kappa_i, A', B'))$ where $\mathcal{S} \in \rho_0(\mathsf{Kind})$ and $C \in \mathcal{CR}(I \to \mathsf{Kind})_{\mathcal{K}}$. By induction on the structure of κ_i, we can show that this is invariant. This implies that if $\kappa_i \rhd \kappa_i'$ then the interpretation remains the same. If $I \rhd I'$, then for some i, $\kappa_i \rhd \kappa_i'$. From here we can deduce that if $I \rhd I'$, then $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(I) = \mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(I')$.
- large elim – Follows from lemma 56.
- abstraction – Both of the abstractions are proved similarly. So we will show only one of the cases.

– $\Delta \vdash \lambda t : \kappa_1 . \kappa_2 : \Pi t : \kappa_1 . u$. We must prove that $(\phi(\lambda t : \kappa_1 . \kappa_2), \phi(\Pi t : \kappa_1 . u), \Theta, \emptyset, \mathcal{U})$ is invariant, given Θ, ϕ, and $\mathcal{U}$. This implies that if $\Theta \vdash \tau : \phi(\kappa_1)$ and τ belongs to the appropriate candidate, then we must have $(\phi(\lambda t : \kappa_1 . \kappa_2)\ \tau, [\tau/t]\phi(u), \Theta, \emptyset, \mathcal{U})$ is invariant. By proposition 65 we must prove that

$$([\tau/t]\phi(\kappa_2), [\tau/t]\phi(u), \Theta, \emptyset, \mathcal{U})$$

is invariant. But $(\phi, t : \tau)$ is an instantiation that is adapted to $(\Delta, t : \kappa_1)$. Applying the induction hypothesis now leads to the result.

schema formation rules This paragraph deals with rules of the form $\Delta \vdash u : \mathsf{Kscm}$.

- $u = \mathsf{Kind}$ follows directly.
- $u = z$ follows since the instantiation is adapted.
- $u = \Pi k : u_1 . u_2$ Given Θ, ϕ, and $\mathcal{U}$ we have to prove that $(\phi(\Pi k : u_1 . u_2), \mathsf{Kscm}, \Theta, \emptyset, \mathcal{U})$ is invariant. By the induction hypothesis, we know that $(\phi(u_1), \mathsf{Kscm}, \Theta, \emptyset, \mathcal{U})$ is invariant. The induction hypothesis also says that $([\phi, k : \kappa](u_2), \mathsf{Kscm}, \Theta, \emptyset, \mathcal{U})$ is invariant. We also know that $\Delta \vdash \kappa : \phi(u_1)$ and $(\kappa, \phi(u_1), \Theta, \emptyset, \mathcal{U})$ is invariant since the instantiation is adapted. This implies that $(\phi([\kappa/k]u_2), \mathsf{Kscm}, \Theta, \emptyset, \mathcal{U})$ is invariant.
- $u = \Pi t : \kappa_1 . u_1$ the proof is very similar to the above case.

□

Corollary 72 If τ is a well formed type, $|\tau|$ is strongly normalizing.

Proof Since τ is well formed we have that $\Delta \vdash \tau : \kappa$. We only need to construct an interpretation and a mapping. For the interpretation, let $\mathcal{U}(t) = t$ for every type variable. Then we get $\mathcal{C}^{\mathcal{K}}_{\mathcal{U}}(\tau) = |\tau|$.

We can build the rest of $\mathcal{U}$ and $\mathcal{K}$ as:

- if $\Delta = \cdot$ then $\mathcal{U}(k) = \mathsf{Can}_0(\mathsf{Kind})$ and $\mathcal{K}(z) = \mathsf{Kind}$ for all variables k and z;
- if $\Delta = \Delta', t : \kappa$ then return the $\mathcal{U}'$ and $\mathcal{K}'$ associated with Δ';
- if $\Delta = \Delta', k : u$ then $\mathcal{U} = \mathcal{U}', k : C$ and $\mathcal{K} = \mathcal{K}'$, where $C \in \mathcal{CR}(u)_{\mathcal{K}'}$ and $\mathcal{K}'$ and $\mathcal{U}'$ are associated with Δ';
- if $\Delta = \Delta', z : \mathsf{Kscm}$ then $\mathcal{K} = \mathcal{K}', z : \mathsf{Kind}$ and $\mathcal{U} = \mathcal{U}'$ where $\mathcal{K}'$ and $\mathcal{U}'$ are associated with Δ'.

□

D.3.19 Normalization of terms

In this section, we use an encoding that maps all well formed terms to types. This encoding preserves the number of reductions. The idea is similar to that of Harper *et al* [20].

The encoding uses two constants. $\mathcal{A}$ is a kind and $\mathcal{B}$ is a type. $*$ is a variable that is never used, it is a wild-card.

$$\begin{array}{ll} \mathcal{A} & : \mathsf{Kind} \\ \mathcal{B} & : \Pi k : \mathsf{Kind} . k \\ * & \text{unused variable} \end{array}$$

The encoding for Kscm is as follows:

$$\begin{array}{rcl} S(\mathsf{Kscm}) & = & \mathsf{Kscm} \\ U(\mathsf{Kscm}) & = & \mathsf{Kind} \\ K(\mathsf{Kscm}) & = & \mathcal{A} \end{array}$$

The encoding for schemas is as follows:

$$\begin{array}{rl} U(\mathsf{Kind}) = & \mathsf{Kind} \\ U(\Pi t : \kappa . u) = & \Pi t : K(\kappa) . U(u) \\ U(\Pi k : u_1 . u_2) = & \Pi k : U(u_1) . \Pi t_k : K(u_1) . U(u_2) \\ U(z) = & z \end{array}$$

$$\begin{array}{rl} K(\mathsf{Kind}) = & \mathcal{A} \\ K(\Pi t : \kappa . u) = & \Pi t : K(\kappa) . K(u) \\ K(\Pi k : u_1 . u_2) = & \Pi k : U(u_1) . \Pi t_k : K(u_1) . K(u_2) \\ K(z) = & k_z \end{array}$$

$$\begin{array}{rl} T(\mathsf{Kind}) = & \mathcal{B}\ \mathcal{A} \\ T(\Pi t : \kappa . u) = & \mathcal{B}[\mathcal{A} \to \Pi t : K(\kappa) . \mathcal{A} \to \mathcal{A}] \\ & \quad T(\kappa)(\lambda t : K(\kappa) . T(u)) \\ T(\Pi k : u_1 . u_2) = & \mathcal{B}[\mathcal{A} \to \Pi k : U(u_1) . \Pi t_k : K(u_1) . \mathcal{A} \to \mathcal{A}] \\ & \quad T(u_1)(\lambda k : U(u_1) . \lambda t_k : K(u_1) . T(u_2)) \\ T(z) = & t_z \end{array}$$

The encoding for kinds is as follows:

$$\begin{array}{rl} K(k) = & k \\ K(\Pi t : \kappa_1 . \kappa_2) = & \Pi t : K(\kappa_1) . K(\kappa_2) \\ K(\Pi k : u . \kappa) = & \Pi k : U(u) . \Pi t_k : K(u) . K(\kappa) \\ K(\Pi z : \mathsf{Kscm} . \kappa) = & \Pi z : \mathsf{Kscm} . \Pi k_z : \mathsf{Kind} . \Pi t_z : \mathcal{A} . K(\kappa) \\ K(\lambda k : u . \kappa) = & \lambda k : U(u) . \lambda t_k : K(u) . K(\kappa) \\ K(\lambda t : \kappa_1 . \kappa_2) = & \lambda t : K(\kappa_1) . K(\kappa_2) \\ K(\kappa\ \tau) = & K(\kappa)\ T(\tau) \\ K(\kappa_1\ \kappa_2) = & K(\kappa_1)\ K(\kappa_2) T(\kappa_2) \\ K(\mathsf{Ind}(k : \mathsf{Kind})\{\vec{\kappa}\}) = & \mathsf{Ind}(k : \mathsf{Kind})\{\overrightarrow{K(\kappa)}\} \\ K(\mathsf{Elim}[\kappa, u](\tau)\{\vec{\kappa'}\}) = & \mathsf{Elim}[K(\kappa), U(u)](T(\tau))\{\overrightarrow{K(\kappa')}\} \end{array}$$

$$\begin{array}{rl} T(k) = & t_k \\ T(\Pi t : \kappa_1 . \kappa_2) = & \mathcal{B}[\mathcal{A} \to \Pi t : K(\kappa_1) . \mathcal{A} \to \mathcal{A}] \\ & \quad T(\kappa_1)(\lambda t : K(\kappa_1) . T(\kappa_2)) \\ T(\Pi k : u . \kappa) = & \mathcal{B}[\mathcal{A} \to \Pi k : U(u) . \Pi t_k : K(u) . \mathcal{A} \to \mathcal{A}] \\ & \quad T(u)(\lambda k : U(u) . \lambda t_k : K(u) . T(\kappa)) \\ T(\Pi z : \mathsf{Kscm} . \kappa) = & \\ & \mathcal{B}[\Pi z : \mathsf{Kscm} . \Pi k_z : \mathsf{Kind} . \Pi t_z : \mathcal{A} . \mathcal{A} \to \mathcal{A}] \\ & \quad (\lambda z : \mathsf{Kscm} . \lambda k_z : \mathsf{Kind} . \lambda t_z : \mathcal{A} . T(\kappa)) \\ T(\lambda k : u . \kappa) = & \\ & \lambda k : U(u) . \lambda t_k : K(u) . (\lambda * : \mathcal{A} . T(\kappa)) T(u) \\ T(\lambda t : \kappa_1 . \kappa_2) = & \lambda t : K(\kappa_1) . (\lambda * : \mathcal{A} . T(\kappa_2)) T(\kappa_1) \\ T(\kappa\ \tau) = & T(\kappa)\ T(\tau) \\ T(\kappa_1\ \kappa_2) = & T(\kappa_1)[K(\kappa_2)] T(\kappa_2) \\ T(\mathsf{Ind}(k : \mathsf{Kind})\{\vec{\kappa}\}) = & \\ & \mathcal{B}[(\mathsf{Kind} \to \mathcal{A} \to (\mathcal{A} \to \ldots \to \mathcal{A}) \to \mathcal{A}) \to \mathcal{A}] \\ & \quad (\lambda k : \mathsf{Kind} . \lambda t_k : \mathcal{A} . \lambda Y : (\mathcal{A} \to \ldots \to \mathcal{A}) . (Y\ \overrightarrow{T(\kappa_i)})) \\ T(\mathsf{Elim}[\kappa, u](\tau)\{\vec{\kappa'}\}) = & \\ & \mathsf{Elim}[K(\kappa), (\lambda * : \underline{K(\kappa) . K(u))}](T(\tau)) \\ & \quad \{\overrightarrow{(\lambda * : \mathcal{A} . \lambda * : \mathcal{A} . T(\kappa_i'))T(\kappa)T(u)}\} \end{array}$$

The encoding for types is as follows:

$$
\begin{array}{rcl}
T(t) & = & t \\
T(\lambda t\!:\!\kappa.\,\tau) & = & \lambda t\!:\!K(\kappa).\,(\lambda *\!:\!\mathcal{A}.\,T(\tau))T(\kappa) \\
T(\tau_1\,\tau_2) & = & T(\tau_1)\,T(\tau_2) \\
T(\lambda k\!:\!u.\,\tau) & = & \lambda k\!:\!U(u).\,\lambda t_k\!:\!K(u).\,(\lambda *\!:\!\mathcal{A}.\,T(\tau))T(u) \\
T(\tau[\kappa]) & = & T(\tau)[K(\kappa)]T(\kappa) \\
T(\lambda z\!:\!\mathsf{Kscm}.\,\tau) & = & \lambda z\!:\!\mathsf{Kscm}.\,\lambda k_z\!:\!\mathsf{Kind}.\,\lambda t_z\!:\!\mathcal{A}.\,T(\tau) \\
T(\tau[u]) & = & T(\tau)[U(u)][K(u)]\,T(u) \\
T(\mathsf{Ctor}\,(i,\kappa)) & = & (\lambda *\!:\!\mathcal{A}.\,\mathsf{Ctor}\,(i,K(\kappa)))T(\kappa) \\
T(\mathsf{Elim}[\kappa,\kappa_1](\tau)\{\vec{\tau}\}) & = & \\
\mathsf{Elim}[K(\kappa),K(\kappa_1)](T(\tau))\{\overrightarrow{(\lambda *\!:\!\mathcal{A}.\,\lambda *\!:\!\mathcal{A}.\,T(\tau_i))T(\kappa)T(\kappa_1)}\} &&
\end{array}
$$

We have to define a similar transformation on contexts:

$$
\begin{array}{rcl}
\Gamma(\cdot) & = & \cdot, \mathcal{A}\!:\!\mathsf{Kind}, \mathcal{B}\!:\!\Pi k\!:\!\mathsf{Kind}.\,k \\
\Gamma(\Delta, t\!:\!\kappa) & = & \Gamma(\Delta), t\!:\!K(\kappa) \\
\Gamma(\Delta, k\!:\!u) & = & \Gamma(\Delta), k\!:\!U(u), t_k\!:\!K(u) \\
\Gamma(\Delta, z\!:\!\mathsf{Kscm}) & = & \Gamma(\Delta), z\!:\!\mathsf{Kscm}, k_z\!:\!\mathsf{Kind}, t_z\!:\!\mathcal{A}
\end{array}
$$

D.3.20 Coding and reduction

In this section we state lemmas that prove that the coding preserves the number of reductions. We omit the proofs since they follow by a straightforward induction over the structure of terms.

Lemma 59 For all well typed terms A, if $A \rhd_\beta A'$, then we have

$$
\begin{array}{l}
T(A) \rhd_\beta^{1+} T(A') \\
K(A) \rhd_\beta^{*} K(A') \\
U(A) \rhd_\beta^{*} U(A')
\end{array}
$$

Moreover, if $\| A \| \rhd_\beta A_1$, then there exists A_2 such that $\| A_2 \| = A_1$ and $|T(A)| \rhd^{1+} |T(A_2)|$.

Lemma 60 For all well typed terms A, if $A \rhd_\iota A'$, then we have

$$
\begin{array}{l}
T(A) \rhd_\iota^{1+} T(A') \\
K(A) \rhd_\iota^{*} K(A') \\
U(A) \rhd_\iota^{*} U(A')
\end{array}
$$

Moreover, if $\| A \| \rhd_{\iota_0} A_1$, then there exists A_2 such that $\| A_2 \| = A_1$ and $|T(A)| \rhd^{1+} |T(A_2)|$.

Lemma 61 For all well typed terms A, if $A \rhd_\eta A'$, then we have

$$
\begin{array}{l}
T(A) \rhd_{\beta\eta}^{1+} T(A') \\
K(A) \rhd_{\beta\eta}^{*} K(A') \\
U(A) \rhd_{\beta\eta}^{*} U(A')
\end{array}
$$

D.3.21 Coding and typing

In this section we show that the coding of a well typed term is also well typed. For this we need to prove that the coding preserves $\beta\eta\iota$ equality. This requires a confluent calculus. Therefore, we use the unmarked terms from Section D.2.1. We extend the coding to unmarked terms by defining:

$$
\begin{array}{rcl}
U(_) & = & _ \\
K(_) & = & _ \\
T(_) & = & _
\end{array}
$$

It is now easy to prove by a straightforward induction on the structure of terms that the following lemma holds:

Lemma 62 Suppose $\Delta \vdash A : B$ and $B \neq \mathsf{Ext}$. Then we have that

$$
\begin{array}{l}
\Gamma(\Delta) \vdash T(A) : K(B) \text{ and } \Gamma(\Delta) \vdash K(B) : \mathsf{Kind} \\
\Gamma(\Delta) \vdash K(A) : U(B) \text{ and } \Gamma(\Delta) \vdash U(B) : \mathsf{Kscm} \text{ if defined} \\
\Gamma(\Delta) \vdash U(A) : S(B) \text{ and } \Gamma(\Delta) \vdash S(B) : \mathsf{Ext} \text{ if defined}
\end{array}
$$

Corollary 73 Suppose $\Delta \vdash A : B$ and $B \neq \mathsf{Ext}$. Then $|T(A)|$ is strongly normalizing.

D.3.22 Normalization of unmarked terms

Lemma 63 For all well typed terms A, we have that $\| A \|$ is strongly normalizing for $\beta\eta\iota_0$ reduction.

Proof Since there can not be an infinite sequence of η reductions and we can delay η reductions, we need to prove the normalization for $\beta\iota_0$ reductions only. Suppose $\| A \|$ is not normalizing and there exists a sequence $A_1 \ldots A_i \ldots$ such that $A_i \rhd_{\beta\iota_0} A_{i+1}$ and $A_0 = \| A \|$. By lemma 59 and 60, we get that there exists a sequence of terms $A'_1 \ldots A'_i \ldots$ such that $\| A'_i \| = A_i$ and $|T(A'_i)| \rhd_{\beta\iota}^{1+} |T(A'_{i+1})|$ and also $|T(A)| \rhd_{\beta\iota}^{1+} |T(A'_1)|$. This implies that $|T(A)|$ is not strongly normalizing which is a contradiction. □

D.3.23 Normalization of all terms

Lemma 64 Suppose $A \rhd_{\beta\iota} B$. Then $\| T(A) \| \rhd_{\beta\iota}^{1+} \| T(B) \|$.

Proof By induction over the derivation of $A \rhd_{\beta\iota} B$. Note that in taking a term A to $T(A)$, all the terms C that appear as annotations at lambda abstractions are duplicated with the corresponding $T(C)$. □

Lemma 65 Suppose $\Delta \vdash A : B$. Then A is strongly normalizing.

Proof We only have to prove normalization for $\beta\iota$ reduction. By lemma 64, if A is not normalizing, then $\| T(A) \|$ is also not normalizing. But by lemma 62 we have that $\Gamma(\Delta) \vdash T(A) : K(B)$ which implies (lemma 63) that $\| T(A) \|$ is strongly normalizing. □

Theorem 74 (Strong normalization) All well typed terms are strongly normalizing.

Proof Follows from lemma 65. □

D.4 Church-Rosser Property

The proof is structured as follows:

- We first prove that a well typed term A in $\beta\iota$ normal form has the same η reductions as $\| A \|$.
- From here we know that if A and A' are in normal form, then $\| A \|$ and $\| A' \|$ are equal. We then show that the annotations in the λ-abstractions are equal.

D.4.1 Structure of normal forms

Lemma 66 All well typed $\beta\iota$ normal terms N have the following form:

1. $\lambda X\!:\!N_1.\,N_2$.
2. $\Pi X\!:\!N_1.\,N_2$.

3. $s \in \{\mathsf{Kind}, \mathsf{Kscm}, \mathsf{Ext}\}$.
4. $X\ \vec{N}$.
5. $\mathsf{Ind}(X:\mathsf{Kind})\{\vec{N}\}$.
6. $\mathsf{Ctor}\,(i, N)\ \vec{N}$ where N is of the form 5.
7. $\mathsf{Elim}[N, N_2](N_1)\{\vec{N}\}\ \vec{N'}$ where N is of the form 5 and N_1 is of the form 4.

Lemma 67 Let $\Delta, X:C, \Delta' \vdash A : B$ be a judgment and A in $\beta\iota$ normal form. If X does not occur in $FV(B) \cup FV(\Delta') \cup FV(\| A \|)$, then $X \notin FV(A)$.

Proof The proof is by induction over the size of A. We use lemma 66 to enumerate the different cases.

- The case where A is a variable or a sort is immediate.
- Suppose $\Delta, X : C, \Delta' \vdash \Pi Y : N_1. N_2 : B$. It follows directly from the induction hypothesis that X does not occur in N_1 and N_2.
- Suppose $\Delta, X : C, \Delta' \vdash \lambda Y : N_1. N_2 : B$ and $B = \Pi Y : N_1. A'$. We know that $\Delta, X : C, \Delta' \vdash N_1 : s$ and therefore $X \notin FV(N_1)$. Also $B \rhd^* \Pi Y : N_1'. A''$ and $\Delta, X : C, \Delta', Y : N_1 \vdash N_2 : A''$. Since $X \notin FV(A'') \cup FV(N_1)$, we can apply the induction hypothesis and therefore $X \notin FV(N_2)$.
- Suppose $\Delta, X : C, \Delta' \vdash Y\ \vec{N} : B$. This implies that $\Delta, X : C, \Delta' \vdash Y : \Pi Z : A_1. A_2$ and $\Delta, X : C, \Delta' \vdash N_1 : A_1$. From lemma 23 and 13 we have that $\Delta, X : C, \Delta' \vdash Y : \Pi Z : A_3. A_4$ where X does not occur free in A_3 and $A_3 =_{\beta\eta\iota} A_1$ and $A_4 =_{\beta\eta\iota} A_2$. From here we can show that $\Delta, X : C, \Delta' \vdash N_1 : A_3$. We can now apply the inductive hypothesis to show that $X \notin FV(N_1)$. Iterating in this way, we can show that $X \notin FV(N_i)$.
- Suppose $\Delta, X : C, \Delta' \vdash \mathsf{Ind}(Y : \mathsf{Kind})\{\vec{N}\} : B$. Follows directly from the induction hypothesis that $X \notin FV(N_i)$.
- Suppose $\Delta, X : C, \Delta' \vdash \mathsf{Ctor}\,(i, I)\ \vec{N} : B$. Follows directly from the induction hypothesis that $X \notin FV(I)$. We can then show as above that $X \notin FV(N_i)$.
- Suppose $\Delta, X : C, \Delta' \vdash \mathsf{Elim}[N, N_1](N_2)\{\vec{N}\}\ \vec{N'} : B$. Since $\Delta, X : C, \Delta' \vdash N : \mathsf{Kind}$, it follows from the induction hypothesis that $X \notin FV(N)$. Similarly, since $\Delta, X : C, \Delta' \vdash N_1 : \mathsf{Kscm}$, or $\Delta, X : C, \Delta' \vdash N_1 : N \to \mathsf{Kind}$, it follows that $X \notin FV(N_1)$. Similarly we can prove directly from the induction hypothesis that $X \notin FV(N_2) \cup FV(\vec{N})$. Finally, as above we can prove that $X \notin FV(\vec{N'})$. □

Corollary 75 Let $\Delta \vdash A : B$. If A is in normal form, then $\| A \|$ is also in normal form.

Proof We must show that $\| A \|$ does not contain any η reductions. The interesting case is when A is of the form $\lambda X : N_1. N_2\ X$. We want to show that if $X \notin FV(\| N_2 \|)$, then $X \notin FV(N_2)$. Since it is well typed we know that $\Delta \vdash \lambda X : N_1. N_2\ X : \Pi X : N_1. C$. We have that $X \notin FV(\Pi X : N_1. C)$. From here we get that $\Delta, X : N_1 \vdash N_2 : \Pi X : N_1. C$. This implies that if $X \notin FV(\| N_2 \|)$, then $X \notin FV(N_2)$. □

D.4.2 Church-Rosser

Theorem 76 (Church-Rosser) Let $\Delta \vdash A : B$ and $\Delta \vdash A' : B$ be two derivable judgments. If $A =_{\beta\eta\iota} A'$, and if A and A' are in normal form, then $A = A'$.

Proof We know that $\| A \|$ and $\| A' \|$ are in normal form. Since the unmarked terms are confluent we have that $\| A \| = \| A' \|$. The proof is by induction over the structures of A and A'.

- The case when $A = A' = s$ or $A = A' =$ a variable is immediate.
- Suppose $A = \lambda X : N_1. N_2$ and $A' = \lambda X : N_1'. N_2'$. We know that $B =_{\beta\eta\iota} \Pi X : N_1. A_3 =_{\beta\eta\iota} \Pi X : N_1'. A_3'$. This implies that $N_1 =_{\beta\eta\iota} N_1'$ which implies that both of them have the same sort. This implies that $N_1 = N_1'$. We can now apply the induction hypothesis to N_2 and N_2' to get that $N_2 = N_2'$.
- Suppose $A = \Pi X : N_1. N_2$ and $A' = \Pi X : N_1'. N_2'$. Follows directly from the induction hypothesis.
- Suppose $A = X\ \vec{N}$ and $A' = X\ \vec{N'}$. We know that in the context Δ, the variable X has the type $\Pi \vec{Y} : \vec{B}. A_3$. Therefore each of the N_i and N_i' have the same type. Applying the induction hypothesis to each of them leads to the required result.
- Suppose $A = \mathsf{Ind}(X : \mathsf{Kind})\{\vec{N}\}$ and $A' = \mathsf{Ind}(X : \mathsf{Kind})\{\vec{N'}\}$. By the typing rules we know that $\Delta, X : \mathsf{Kind} \vdash N_i : \mathsf{Kind}$ and $\Delta, X : \mathsf{Kind} \vdash N_i' : \mathsf{Kind}$. Applying the induction hypothesis leads to $N_i = N_i'$.
- Suppose $A = \mathsf{Ctor}\,(i, N)\ \vec{N}$ and $A' = \mathsf{Ctor}\,(i, N')\vec{N'}$. We know that both N and N' have type Kind. The induction hypothesis directly leads to $N = N'$. We can then show as above that $N_i = N_i'$.
- Suppose $A = \mathsf{Elim}[N, N_1](N_2)\{\vec{N}\}\ \vec{N_0}$ and $A' = \mathsf{Elim}[N', N_1'](N_2')\{\vec{N'}\}\ \vec{N'}_0$. Since N and N' are both of type Kind, it follows that $N = N'$. From here we get that $N_2 = N_2'$. Since both N_1 and N_1' have the type Kscm or have the type $N \to \mathsf{Kind}$, it follows that $N_1 = N_1'$. From this we can show that the N_i and N_i' are equal. Finally as above, we can show that the N_{0i} and the N'_{0i} are equal. □

Theorem 77 (Confluence) Let $\Delta \vdash A : B$ and $\Delta \vdash A' : B$ be two judgments. If $A =_{\beta\eta\iota} A'$, then A and A' have a common reduct – there exists a term C such that $A \rhd^* C$ and $A' \rhd^* C$.

Proof We know that both A and A' reduce to normal forms A_1 and A_1'. Due to subject reduction, both A_1 and A_1' have the same type B. By the previous lemma $A_1 = A_1'$. □

D.5 Consistency

Theorem 78 (Consistency of the logic) There exists no term A for which $\cdot \vdash A : \Pi X : \mathsf{Kind}. X$.

Proof Suppose there exists a term A for which $\cdot \vdash A : \Pi X : \mathsf{Kind}. X$. By theorem 74, there exists a normal form B for A. By the subject reduction $\cdot \vdash B : \Pi X : \mathsf{Kind}. X$. We can show now that this leads to a contradiction by case analysis of the possible normal forms for the types in the calculus. □