Generative Type Abstraction and Type-level Computation (Extended Version)

Simon Peyton Jones Dimitrios Vytiniotis
Microsoft Research
{simonpj,dimitris}@microsoft.com

Stephanie Weirich Steve Zdancewic
University of Pennsylvania
{sweirich,stevez}@cis.upenn.edu

Abstract

Modular languages support *generative type abstraction*, ensuring that an abstract type is distinct from its representation, except inside the implementation where the two are synonymous. We show that this well-established feature is in tension with the *non-parametric features* of newer type systems, such as indexed type families and GADTs. In this paper we solve the problem by using kinds to distinguish between parametric and non-parametric contexts. The result is directly applicable to Haskell, which is rapidly developing support for type-level computation, but the same issues should arise whenever generativity and non-parametric features are combined.

1. Introduction

Generative type abstraction allows programmers to introduce new type constants in their programs that are *isomorphic* to existing types; examples include ML's module system [Milner et al. 1997; Pierce 2005, Ch. 8], and Haskell's **`newtype`** construct [Peyton Jones et al. 2003]. Type generativity is very important because it supports modularity by enforcing *abstraction*: the *implementor* of a module can move freely between the abstract and representation types, whereas to the *client* of the module the two types are completely distinct.

There is growing interest in languages that support some form of *type-level computation*, including Haskell's type classes [Hall et al. 1996] and indexed type families [Kiselyov et al. 2010]. However, as we show in Section 2, there is a fundamental tension between type-level computation and generative type abstraction, at least in the latter's more flexible forms. To summarize very briefly, the conflict is this:

- To maximize re-use and convenience, it is very desirable for the implementor to be able to treat the abstract type A and its concrete representation type C as synonymous – we call this *flexible type generativity*.
- However, given type-level function F the result of $(F\,A)$ and $(F\,C)$ may differ, so A and C cannot be synonymous.

Resolving this conflict is the subject of this paper. Specifically our contributions are:

- We show in Section 2 that the naive combination of type generativity and non-parametric type-level features can violate soundness; a problem that already manifests in the Glasgow Haskell Compiler, and affects not only type-level non-parametric functions, but also other forms of non-parametric constructs, such as *generalized algebraic datatypes* (GADTs) [Cheney and Hinze 2003; Hinze et al. 2002; Peyton Jones et al. 2006; Xi et al. 2003].
- We formalize a solution to this problem that reconciles flexible type generativity and non-parametric type functions in Section 3. Our language, FC_2, builds on GHC's existing core language, System FC [Sulzmann et al. 2007], which supports erasable type-level coercions. The key ingredient in our solution is to employ kinds decorated with *roles* to distinguish possibly non-parametric type contexts and to refine the admissible coercions of System FC.
- We prove that FC_2 programs are type safe, provided that user axioms and definitions give rise to consistent axiom sets (Section 4).
- We give sufficient conditions for showing the consistency of an axiom set. For our proofs, we introduce a rewrite system for types that is novel in two dimensions: rewriting (i) is *role-sensitive*, and (ii) introduces a new (to our knowledge) notion of parallel reduction that does not require termination of the rewrite system in the consistency conditions (Section 4.2).
- We present a Haskell-specific result: we show how Haskell source programs that may involve non-parametric type contexts and flexible type generativity can be translated to yield provably consistent FC_2 axiom sets. (Section 5)
- Our core language is an *improvement* of System FC since it permits safe flexible type generativity, but also *unsaturated* type functions. Perhaps surprisingly, our language is additionally a significant *simplification* of the original System FC, which *removes* several of the original coercion constructs that we have identified to be encodable (even in the original System FC). We discuss these differences in Section 6.2.

For the sake of concreteness we build our presentation around Haskell and System FC, since this setting allows us to demonstrate our points with real code, instead of using a hypothetical λ-calculus. However, we stress that our work is applicable whenever flexible type generativity and non-parametric type-level features are combined. For example, the very same issues could arise in extensions of the ML module system. We discuss related work in Section 7.

2. The problems with generative type abstraction

Generative type abstraction is an extremely useful mechanism for enforcing abstraction barriers and for refining interfaces. To see this, let us consider the Haskell incarnation of type generativity, namely **newtype** definitions. In Haskell the programmer may declare a **newtype** `Age`, with concrete representation type `Int`, thus:

```
newtype Age = MkAge Int
```

The implementor uses the "data constructor" `MkAge` to coerce an `Int` to an `Age`, and pattern matching to effect the inverse coercion. For example:

```
addAge :: Age → Int → Age
addAge (MkAge a) n = MkAge (a+n)
```

The client, in contrast, can be prevented from making such conversions, by using the module system to hide the `MkAge` constructor:

```
module AgeModule( Age, addAge, ... ) where
  -- Age definition and implementation
```

2.1 Coercion lifting

In describing `MkAge`, we wrote "data constructor" in quotes because although it behaves in many ways like a data constructor, its cost model is different. Specifically, a **newtype** definition guarantees that the abstract type really is represented by the concrete type, so the runtime conversion cost is zero. That would not be true if `Age` were instead declared with **data** instead of **newtype**.

So `Age` can be coerced to an `Int`, and vice versa, for free—i.e. without runtime cost—because it *is* an `Int`. Notationally, we say that `Int` $\sim$ `Age`, where we use $\sim$ for type equality[1]. But what about, say, `Maybe Age`?

```
data Maybe a = Nothing | Just a
```

Obviously, `Maybe Age` should be freely coercible to `Maybe Int`, because the two are represented identically. Alas, in Haskell 98 one would have to write

```
cvt :: Maybe Age → Maybe Int
cvt t = mapMaybe (λ MkAge a → a) t
-- mapMaybe :: (a→b) → Maybe a → Maybe b
```

This is unsavory for several reasons: (a) it is tedious for the programmer; (b) it is hard for the compiler to eliminate a runtime call to `mapMaybe` (let alone to guarantee to do so) especially if it is recursive; and (c) it may be difficult to implement the necessary "map" function. As an example of (c) consider the mapping function for the type `T` shown below, with co- and contra-variance, and higher kinds:

```
data T a f = T1 a
           | T2 (a → Int)
           | T3 (f (T a f) (T a f))
```

These difficulties are frustrating, because we know that, say, `T Age Maybe` is represented identically to `T Int Maybe`. So, let us imagine a hypothetical extension of Haskell that provides lifted coercions; that is, it implements the following rule:

> *Coercion lifting:* if for two types φ and ψ we have $\varphi \sim \psi$ (for example, if they are the abstract and concrete types of a **newtype** declaration), then $T\,\varphi \sim T\,\psi$ for any type constructor T.

[1] There are too many sorts of "="!

In fact this extension is not so hypothetical, because such a rule is the basis of the so-called "newtype deriving" feature implemented by GHC, but we do not want to get distracted by Haskell-specific details here.

ML supports coercion lifting even more directly: within a structure the abstract and the representation types are considered entirely interchangeable. For example in ML one might say

```
signature AgeSig = sig {
  type age
  addAge : age → int → age
  ... }

structure AgeModule : AgeSig = struct {
  type age = int
  addAge a n = a+n
  ... }
```

Inside `AgeModule` the two types are synonymous, and so `addAge` need not convert in either direction. Similarly, `cvt` would simply be the identity function, as indeed it should be.

However, the point of this paper is that the innocuous and obvious-seeming "lifting" of type identities becomes unsound when combined with type-level computation, as we show in the next section.

2.2 Type-level computation

One very popular extension to Haskell is that of Generalized Algebraic Data Types (GADTs) [Peyton Jones et al. 2006], with which we assume the reader is somewhat familiar. In GHC one could declare a GADT with three nullary constructors like this:

```
data K a where
  KAge :: K Age
  KInt :: K Int
  KAny :: K a
```

Now, consider these functions:

```
kint :: K Int
kint = KInt

get :: K Age → String
get KAge = "Age"
get KAny = "Any"
```

Since `get`'s type signature declares that its argument is of type `K Age`, it follows that the patterns in `get` are exhaustive. But consider the call `(get kint)`. By coercion lifting, `K Int` and `K Age` are coercible, so the call is well typed—yet the pattern match in `get` will fail.

In the last few years we have gone beyond GADTs, by extending GHC with type-level functions [Chakravarty et al. 2005a,b; Kiselyov et al. 2010]. The reader is urged to consult these papers for motivated examples of type functions, but for the purposes of this paper we content ourselves with a small but contrived example:

```
type family F a :: *
type instance F Age = Char
type instance F Int = Bool
```

Here the type function `F` maps the type `Age` to the type `Char`, but it maps `Int` to `Bool`.

However, the existence of such a type-level function threatens not just pattern exhaustiveness but type soundness itself. Consider the type `Bool`. This type is equivalent to `F Int` by the equation for `F`; and by coercion lifting that should be equivalent to `F Age`; and that is equivalent to `Char` by the other equation for `F`. Altogether we can coerce `Bool` to `Char`, which is obvious nonsense.

What went wrong? Maybe it should be illegal for a type function to behave differently on two coercible types, such as `Age` and `Int`? But in fact Haskell programmers often use **newtype** precisely so

that they can give a different type-class instance (for comparison, say) for `Age` than for the underlying `Int`. Type functions are no different; indeed, they are often introduced as an "associated type" of a type class [Kiselyov et al. 2010], and hence, just as the type class distinguishes between the abstract and concrete type, so must the type function.

How else might we fix the problem? Perhaps, in the definition of coercion lifting we should not allow T to range over type functions such as `F`? Indeed we should not, but that is not enough. Consider

```
data TF a = MkTF (F a)
```

Now, should coercion lifting allow us to coerce `TF Age` to `TF Int`? Obviously not! Otherwise we could write

```
to :: Bool → TF Int      from :: TF Age → Char
to b = MkTF b            from (MkTF c) = c
```

and now the composition `from ∘ to` is well-typed (via coercion lifting) but obviously unsound.

2.3 Summary

At this point it should be clear that a naive combination of:

- type-level dispatch, whether by GADTs or by type functions
- unrestricted coercion lifting

simply does not work. This interaction was far from obvious to us initially, and indeed GHC has a well-documented type-soundness bug[2] that arises *directly* from this unforeseen interaction. Yet both type-level dispatch and coercion lifting (suitably restricted) are valuable. The purpose of this paper is to show how they may be soundly combined.

We urge the reader not to be distracted by the question of whether the coercion between abstract and concrete types is explicit (as in Haskell) or implicit (as in ML). This is a property of the *surface language*, and one that is intimately connected with type inference. Instead, for most of the paper we will focus our attention on the *intermediate language*, in which (runtime-erasable) coercions are explicit. Whether they come directly from the source program, or from elaboration by the type checker, is secondary.

This problem is important not only because it arises in GHC, but also because the same issues will arise in *any* type system that combines type-level dispatch and coercion lifting. Haskell is the first programming language that has pushed the type system far enough for these problems to arise in practice, but others (such as ML) may well do so in the future, although their particularities may affect the applicability of our solution.

3. The FC_2 language: codes versus types

As shown above, the fundamental issue is that there is a tension between *generative types*, which allow programmers to express the intent that two types have identical representations, and *type functions*, which can distinguish two types even if they have the same underlying representation.

The key idea of our solution is to separate types that can be analyzed by type functions from those that must be used parametrically. We call the former *codes*, as in "codes for types," [Benke et al. 2003; Dybjer 2000] since type functions can branch on them and thus treat them as a form of data. Codes are themselves valid *types*, which, as usual, classify program expressions and indicate the representation of data structures. This distinction also gives rise to two different notions of equality—code equality is used to reason about the meaning of type-indexed functions and is finer-grained than type equality, which is used for determining which type coercions are safe.

To see why these distinctions matter, reconsider the `Age` example from above. The **`newtype`** declaration introduces a new code, `Age`, that is distinct (as a code) from the code `Int`. On the other hand `Age` and `Int` *are* equal when considered as types, since, in fact, they have identical representations and it is safe to coerce between them.

3.1 FC_2: an overview

These ideas are best explained in terms of an intermediate language that exposes the differences between codes and types and makes explicit the uses of the two kinds of equality mentioned above. Thus, the remainder of this section describes FC_2, our new variant of System FC [Sulzmann et al. 2007]—a model of the intermediate language used in GHC. As such, it is expressive enough to capture indexed type functions, **`newtype`** and **`newtype deriving`**, GADTs, existential and nested datatypes, and much more.

Figure 1 summarizes the syntax of FC_2, which, at the term level (e), is just the polymorphic lambda calculus with two extensions. First, FC_2 provides polymorphic datatypes, introduced by data constructors K. These datatypes are eliminated using a **`case`** construct that should be familiar from Haskell or ML-style functional programming—we describe how datatypes and **`case`** are typechecked in Section 3.5.

Second, FC_2 includes first-class proofs of type equality that witness safe coercions introduced during compilation. These explicit coercions, written γ, make typechecking FC_2 programs *syntax-directed*—every expression is annotated with enough information to determine whether it is well-typed (and with what type) using just an inductive walk over the expression. Programs in FC_2 can abstract over coercions reflecting a particular type equality (written $\Lambda c{:}\varphi_1 \sim \varphi_2.e$), pass a coercion as an argument to such a function (written $e\,\gamma$), and use a coercion to cast a term from one type to another (written $e \triangleright \gamma$).

Figure 2 shows the typing rules for the terms of FC_2. The first five rules, ETVAR through ETAPP, are completely standard. We defer explanation of the remaining rules until we build up some more technical machinery having to do with FC_2's kind-level distinction between codes and types and the rules by which explicit coercions can themselves be combined. We describe these aspects of FC_2 next.

3.2 FC_2 types and kinds

Types in FC_2 are classified by pairs κ of the form η/R, where the *kind* η ensures (as usual) that types are well-formed structurally, and the *role* R determines whether the type can be analyzed. Codes have role C, whereas types that must be used parametrically have role T. This syntax is summarized at the top of Figure 1. There is an inclusion relation $\mathsf{C} \preceq \mathsf{T}$ on roles that makes explicit the fact that any code can play the role of a type but not vice-versa (see the top of Figure 3). For example, both $\texttt{Int} : \star/\mathsf{C}$ and $\texttt{Int} : \star/\mathsf{T}$ hold; that is, `Int` can play both roles.

The distinction between codes and types allows us to give informative kinds to type constructors:

- The `Maybe` type (Section 2.1) has kind $\star/\mathsf{T} \to \star$, indicating that `Maybe` treats its argument *parametrically*.
- The types `K`, `F`, and `TF` (Section 2.2) all use *type indexing* and therefore have kind $\star/\mathsf{C} \to \star$.

It is only safe to lift coercions through functions with parametric kinds, as we discuss in more detail below. So, for example, `Maybe Age` $\sim$ `Maybe Int` holds but `TF Age` $\not\sim$ `TF Int`.

Despite these non-standard kinds, the types of FC_2 are mostly standard: codes φ and types σ are drawn from the same syntax (see

[2] `http://hackage.haskell.org/trac/ghc/ticket/1496`

η	$::=$	$\star \mid \kappa \to \eta$	kind
R	$::=$	$\mathsf{C} \mid \mathsf{T}$	role
κ	$::=$	η / R	kind and role
H	$::=$		type constants
	$\mid$	T	datatypes
	$\mid$	F	functions/newtypes
	$\mid$	$(\to)$	arrow
	$\mid$	$(\sim_\eta)$	equality
$\varphi, \sigma, \psi, \upsilon$	$::=$		codes and types
	$\mid$	a	variables
	$\mid$	H	constants
	$\mid$	$\varphi_1\, \varphi_2$	application
	$\mid$	$\forall a{:}\kappa.\varphi$	polymorphism
γ	$::=$		coercion proof
	$\mid$	$c\, \overline{\varphi}$	assumption
	$\mid$	$\langle \varphi \rangle$	reflexivity
	$\mid$	$\mathbf{sym}\, \gamma$	symmetry
	$\mid$	$\gamma_1\, ;\, \gamma_2$	transitivity
	$\mid$	$\gamma_1\, \gamma_2$	application
	$\mid$	$\mathbf{nth}\, k\, \gamma$	injectivity
	$\mid$	$\forall a{:}\kappa.\gamma_2$	polymorphism
	$\mid$	$\gamma @ \varphi$	instantiation
$e,\ v$	$::=$		expressions
	$\mid$	x	variable
	$\mid$	$\lambda x{:}\sigma.e$	abstraction
	$\mid$	$e_1\, e_2$	application
	$\mid$	$\Lambda a{:}\kappa.e$	type abstraction
	$\mid$	$e\, \varphi$	type application
	$\mid$	K	data constructor
	$\mid$	$\mathbf{case}_\sigma\ e\ \mathbf{of}\ brs$	case analysis
	$\mid$	$\Lambda c{:}\varphi_1 \sim \varphi_2.e$	proof abstraction
	$\mid$	$e\, \gamma$	proof application
	$\mid$	$e \triangleright \gamma$	coercion
brs	$::=$	$\overline{K_i \Rightarrow e_i}^{\,i \in 1..n}$	branches
bnd	$::=$		binding
	$\mid$	$a{:}\kappa$	type variable
	$\mid$	$H{:}\eta$	type constant
	$\mid$	$c{:}\Delta.\, \varphi_1 \sim \varphi_2 / R$	coercion
	$\mid$	$x{:}\sigma$	term variable
	$\mid$	$K{:}\Delta.\sigma$	data constructor
Γ	$::=$	$\cdot \mid \Gamma, bnd$	context
Δ	$::=$	$\cdot \mid a{:}\kappa, \Delta$	type context
ρ	$::=$	$e \mid \varphi \mid \gamma$	datacon argument
Θ	$::=$		telescopes
	$\mid$	$\cdot$	empty
	$\mid$	σ, Θ	expression type
	$\mid$	$a{:}\kappa, \Theta$	type variable
	$\mid$	$\varphi_1 \sim \varphi_2, \Theta$	equality

Figure 1. Syntax

$\boxed{\Gamma \vdash e : \sigma}$

$$\frac{x{:}\sigma \in \Gamma \quad \vdash \Gamma}{\Gamma \vdash x : \sigma}\ \textsc{ETVar}$$

$$\frac{\Gamma, x{:}\sigma_1 \vdash e : \sigma_2}{\Gamma \vdash \lambda x{:}\sigma_1.e : \sigma_1 \to \sigma_2}\ \textsc{EEAbs}$$

$$\frac{\Gamma \vdash e_1 : \sigma_1 \to \sigma_2 \quad \Gamma \vdash e_2 : \sigma_1}{\Gamma \vdash e_1\, e_2 : \sigma_2}\ \textsc{EEApp}$$

$$\frac{\Gamma, a{:}\kappa \vdash e : \sigma}{\Gamma \vdash \Lambda a{:}\kappa.e : \forall a{:}\kappa.\sigma}\ \textsc{ETAbs}$$

$$\frac{\Gamma \vdash e : \forall a{:}\kappa.\sigma \quad \Gamma \vdash \varphi : \kappa}{\Gamma \vdash e\, \varphi : \sigma[a \mapsto \varphi]}\ \textsc{ETApp}$$

$$\frac{K{:}\Delta.\sigma \in \Gamma \quad \vdash \Gamma}{\Gamma \vdash K : \forall \Delta.\sigma}\ \textsc{EDataCon}$$

$$\frac{\begin{array}{l}\Gamma \vdash e : T\, \overline{\varphi} \quad \Gamma \vdash \sigma : \star/\mathsf{T} \\ \text{for each } K_i \in \mathrm{Constr}_\Gamma(T) \\ \quad K_i{:}\Delta.\psi_i \in \Gamma \\ \quad \psi_i[\Delta \mapsto \overline{\varphi}] = \forall \Theta_i.T\, \overline{\varphi} \\ \quad \Gamma \vdash e_i : \forall \Theta_i.\sigma\end{array}}{\Gamma \vdash \mathbf{case}_\sigma\ e\ \mathbf{of}\ \overline{K_i \Rightarrow e_i}^{\,i} : \sigma}\ \textsc{ECase}$$

$$\frac{\Gamma, c{:}\varphi_1 \sim \varphi_2/\mathsf{C} \vdash e : \sigma}{\Gamma \vdash \Lambda c{:}\varphi_1 \sim \varphi_2.e : (\varphi_1 \sim \varphi_2) \Rightarrow \sigma}\ \textsc{ECAbs}$$

$$\frac{\begin{array}{l}\Gamma \vdash e : (\varphi_1 \sim \varphi_2) \Rightarrow \sigma \\ \Gamma \vdash \gamma : \varphi_1 \sim \varphi_2 \in \eta/\mathsf{C}\end{array}}{\Gamma \vdash e\, \gamma : \sigma}\ \textsc{ECApp}$$

$$\frac{\Gamma \vdash e : \sigma_1 \quad \Gamma \vdash \gamma : \sigma_1 \sim \sigma_2 \in \star/\mathsf{T}}{\Gamma \vdash e \triangleright \gamma : \sigma_2}\ \textsc{ECoerce}$$

Figure 2. Typing rules

$\boxed{R_1 \preceq R_2}$ $\quad \dfrac{}{\mathsf{C} \preceq \mathsf{T}}\ \textsc{RSub}$ $\quad \dfrac{}{R \preceq R}\ \textsc{RRefl}$

$\boxed{\Gamma \vdash \varphi : \kappa}$

$$\frac{a{:}\eta/R_1 \in \Gamma \quad R_1 \preceq R_2 \quad \vdash \Gamma}{\Gamma \vdash a : \eta/R_2}\ \textsc{PVar}$$

$$\frac{H{:}\eta \in \Gamma \quad \vdash \Gamma}{\Gamma \vdash H : \eta/R}\ \textsc{PConst}$$

$$\frac{\begin{array}{l}\Gamma \vdash \varphi_1 : (\eta_1/R_2 \to \eta_2)/R_1 \\ \Gamma \vdash \varphi_2 : \eta_1/min(R_1, R_2)\end{array}}{\Gamma \vdash \varphi_1\, \varphi_2 : \eta_2/R_1}\ \textsc{PApp}$$

$$\frac{\Gamma, a{:}\kappa \vdash \varphi : \star/R}{\Gamma \vdash \forall a{:}\kappa.\varphi : \star/R}\ \textsc{PAll}$$

$\boxed{\Gamma \vdash \overline{\varphi} : \Delta}$

$$\frac{}{\Gamma \vdash \cdot : \cdot}\ \textsc{PNil} \qquad \frac{\Gamma \vdash \varphi : \kappa \quad \Gamma \vdash \overline{\varphi} : \Delta}{\Gamma \vdash \varphi, \overline{\varphi} : (a{:}\kappa, \Delta)}\ \textsc{PCons}$$

Figure 3. Kinding

Figure 1)—we use two different metavariables as a reminder of the intended role. The type language includes type variables a, type constants H, applications $\varphi_1\ \varphi_2$, and polymorphic types $\forall a{:}\kappa.\sigma$.

Type constants, H, include datatypes T, and type functions F. For the most part, datatypes and type functions are treated uniformly, but there are two important distinctions:

- Datatypes must be injective, while type functions need not be. Injectivity is important because equalities between injective functions imply equalities between their arguments; see rule CNTHT in Section 3.3.
- Datatypes are inhabited by values, but type functions are not—there are no values v with types that are headed by F. This distinction is key to the definition of consistency in Section 4.1.

Newtypes are not inhabited by values, so we treat them like type functions, ranged over by F. Unlike type functions, however, newtypes *are* injective at role C—after all, the essence of generativity is that newtypes create a fresh constant—but for now we will not take advantage of that fact, leaving it for discussion in Section 6.1.

The set of type constants also includes the familiar arrow type constructor $(\rightarrow)$, and a kind-indexed family of constructors $(\sim_\eta)$, which construct functions that abstract over coercions. The kinds of these constants are:

$$\begin{array}{lcl}(\rightarrow) & : & \star/\mathsf{T} \rightarrow \star/\mathsf{T} \rightarrow \star \\ (\sim_\eta) & : & \eta/\mathsf{C} \rightarrow \eta/\mathsf{C} \rightarrow \star/\mathsf{T} \rightarrow \star\end{array}$$

(We discuss in Sections 3.3 and 3.6 why the kind of $(\sim_\eta)$ must require role C for its first two arguments.) Type constants are generally applied prefix, but for these two constants we define infix syntactic sugar:

$$\begin{array}{lcl}\sigma \rightarrow \sigma' & \equiv & (\rightarrow)\ \sigma\ \sigma' \\ (\varphi_1 \sim \varphi_2) \Rightarrow \sigma & \equiv & (\sim_\eta)\ \varphi_1\ \varphi_2\ \sigma\end{array}$$

In the latter case, because the syntactic sugar lacks the η annotation, we only use this notation in contexts where the kind of φ_1 and φ_2 is irrelevant. Rule ECABS follows this convention—it shows that this family of type constructors is used to give a type to terms of the form $\Lambda c : \varphi_1 \sim \varphi_2.e$, which abstracts over an equality proof in the body e. Note that this rule applies only to code equalities; abstraction over type equalities is not needed for compilation of Haskell and permitting it, while straightforward, would require extra syntactic complexity that we choose to omit for the sake of presentation.

Figure 3 defines the kinding rules for FC_2 using judgments of the form $\Gamma \vdash \varphi : \kappa$. Here, the context Γ maps type variables to their kind/role pairs and type constants and type functions to their kinds.

Rule PVAR uses subsumption to allow a variable playing the role of a code to be treated as though its role is a type. Type constants introduce new codes but, again using subsumption, PCONST allows a type constant to play either role. (Although a type constant introduces a new code, its *kind* may well involve arguments with role T; for example, see the signature for $(\rightarrow)$ above.)

Rule PAPP says that the argument to an indexed type function must be a code (if R_2 is C then $min(\mathsf{C}, R_1)$ is C). Likewise, if an application is viewed as a code by the context (*i.e.* R_1 is C) the argument should be viewed as a code too. If neither R_1 nor R_2 is C, then the argument's role is effectively unconstrained. Together these kinding rules implement a subsumption relation that includes codes into the language of types:

LEMMA 1. *If* $\Gamma \vdash \varphi : \eta/\mathsf{C}$ *then* $\Gamma \vdash \varphi : \eta/\mathsf{T}$.

On the other hand, types have only one kind regardless of their role:

LEMMA 2. *If* $\Gamma \vdash \varphi : \eta_1/R_1$ *and* $\Gamma \vdash \varphi : \eta_2/R_2$ *then* $\eta_1 = \eta_2$.

$\boxed{\Gamma \vdash \gamma : \varphi_1 \sim \varphi_2 \in \kappa}$

$$\frac{(c{:}\Delta.\ \varphi_1 \sim \varphi_2/R_1) \in \Gamma \quad \Gamma \vdash \varphi_1 : \eta/R_1 \quad \Gamma \vdash \overline{\psi} : \Delta \quad R_1 \preceq R_2}{\Gamma \vdash c\,\overline{\psi} : \varphi_1[\Delta \mapsto \overline{\psi}] \sim \varphi_2[\Delta \mapsto \overline{\psi}] \in \eta/R_2}\ \textsc{CAssm}$$

$$\frac{\Gamma \vdash \varphi : \kappa}{\Gamma \vdash \langle\varphi\rangle : \varphi \sim \varphi \in \kappa}\ \textsc{CRefl}$$

$$\frac{\Gamma \vdash \gamma : \varphi_1 \sim \varphi_2 \in \kappa}{\Gamma \vdash \mathbf{sym}\,\gamma : \varphi_2 \sim \varphi_1 \in \kappa}\ \textsc{CSym}$$

$$\frac{\Gamma \vdash \gamma_1 : \varphi_1 \sim \varphi_2 \in \kappa \quad \Gamma \vdash \gamma_2 : \varphi_2 \sim \varphi_3 \in \kappa}{\Gamma \vdash \gamma_1\,;\,\gamma_2 : \varphi_1 \sim \varphi_3 \in \kappa}\ \textsc{CTrans}$$

$$\frac{\Gamma \vdash \gamma_1 : \varphi_1 \sim \varphi_2 \in (\eta_1/R_2 \rightarrow \eta_2)/R_1 \quad \Gamma \vdash \gamma_2 : \psi_1 \sim \psi_2 \in \eta_1/min(R_1, R_2)}{\Gamma \vdash \gamma_1\ \gamma_2 : \varphi_1\,\psi_1 \sim \varphi_2\,\psi_2 \in \eta_2/R_1}\ \textsc{CApp}$$

$$\frac{\Gamma \vdash \gamma : T\,\overline{\varphi} \sim T\,\overline{\psi} \in \eta/\mathsf{T} \quad T{:}\forall\,\Delta.\eta \in \Gamma \quad \eta'/R_1 = nth\ k\ \Delta \quad R_1 \preceq R_2}{\Gamma \vdash \mathbf{nth}\,k\,\gamma : nth\ k\ \overline{\varphi} \sim nth\ k\ \overline{\psi} \in \eta'/R_2}\ \textsc{CNthT}$$

$$\frac{\Gamma, a{:}\kappa \vdash \gamma_2 : \varphi_1 \sim \varphi_2 \in \star/R}{\Gamma \vdash \forall a{:}\kappa.\gamma_2 : \forall a{:}\kappa.\varphi_1 \sim \forall a{:}\kappa.\varphi_2 \in \star/R}\ \textsc{CAll}$$

$$\frac{\Gamma \vdash \gamma : \forall a{:}\kappa.\varphi_1 \sim \forall a{:}\kappa.\varphi_2 \in \star/R \quad \Gamma \vdash \psi : \kappa}{\Gamma \vdash \gamma@\psi : (\varphi_1[a \mapsto \psi]) \sim (\varphi_2[a \mapsto \psi]) \in \star/R}\ \textsc{CInst}$$

$\boxed{\Gamma \vdash \overline{\gamma} : \overline{\varphi}_1 \sim \overline{\varphi}_2 \in \Delta}$

$$\frac{\vdash \Gamma}{\Gamma \vdash \cdot : \cdot \sim \cdot \in \cdot}\ \textsc{CNil}$$

$$\frac{\Gamma \vdash \gamma : \varphi_1 \sim \varphi_2 \in \kappa \quad \Gamma \vdash \overline{\gamma} : \overline{\varphi}_1 \sim \overline{\varphi}_2 \in \Delta}{\Gamma \vdash \gamma, \overline{\gamma} : \varphi_1, \overline{\varphi}_1 \sim \varphi_2, \overline{\varphi}_2 \in a{:}\kappa, \Delta}\ \textsc{CCons}$$

Figure 4. Coercions

Note that this judgment, like term typing, is syntax-directed. In particular, the role component R of the κ in this judgment is treated as *input* to the algorithm, and the η is an *output*—the context in which φ is used determines what the role should be. The only interesting case from this perspective is PAPP, in which φ_1 must be checked first to obtain R_2 so that the minimum of R_1 and R_2 can be passed as an input when checking φ_2.

3.3 Coercions and equality

In FC_2 a *coercion* is a proof term that witnesses the equality of two types. Coercions are used to change the type of a term, thus (Figure 2):

$$\frac{\Gamma \vdash e : \sigma_1 \quad \Gamma \vdash \gamma : \sigma_1 \sim \sigma_2 \in \star/\mathsf{T}}{\Gamma \vdash e \triangleright \gamma : \sigma_2}\ \textsc{ECoerce}$$

Here, γ is a *coercion* witnessing the equality $\sigma_1 \sim \sigma_2$ in role T; given that e has type σ_1, we can use γ to let us treat the term as having type σ_2. At compile time, these explicit coercions ensure that typechecking FC_2 programs is completely syntax directed. Such coercions have no run-time effect: they will be erased by the compiler before the program is run. Nevertheless, FC_2's operational

semantics includes coercions, thereby allowing us to establish type safety using standard techniques (Section 3.6).

The translation of a source program into FC_2 may extend the type environment Γ with new equality axioms. For example, the `Age` **`newtype`** definition generates the axiom:

$$\texttt{mkAge} : \texttt{Age} \sim \texttt{Int}/\mathsf{T}$$

Note that ECOERCE requires σ_1 and σ_2 to be equal when considered in role T, which is consistent with the idea that type equality determines when it is safe to coerce. On the other hand, source programs can also introduce code equalities. For example the type function `F` (Section 2.2) generates the two axioms:

$$\texttt{axF1} : \texttt{F Int} \sim \texttt{Bool}/\mathsf{C}$$
$$\texttt{axF2} : \texttt{F Age} \sim \texttt{Char}/\mathsf{C}$$

More generally we permit axiom *schemes*. For example, the source language declaration

`type instance` `F(Maybe a) = (a,a)`

would create the axiom scheme

$$\texttt{axF3} : (a{:}\star/\mathsf{C}).\,\texttt{F(Maybe a)} \sim \texttt{(a,a)}/\mathsf{C}$$

In general, as shown in Figure 1, the context Γ includes bindings of the form $c{:}\Delta.\,\varphi_1 \sim \varphi_2/R$ for coercion axioms. The metavariable Δ stands for a list of quantified type variable bindings of the form $a{:}\kappa$. The same binding form is used both for axioms introduced at top level, and (with empty Δ) for local assumptions introduced in ECABS (Figure 2).

Of course it is important to know that the top-level axioms are *consistent*—it would be unsound to assert that $\texttt{Bool} \sim \texttt{Char}/\mathsf{T}$, for example. Section 4 gives a sufficient set of conditions for ensuring that source programs generate consistent axioms.

Next, we need a way to compose coercions together to construct other coercions. Our goal is to have rules that allow the creation of composite coercions such as:

$$\langle \texttt{List} \rangle\ \texttt{mkAge} \ :\ \texttt{List Age} \sim \texttt{List Int}/\mathsf{T}$$
$$\langle \texttt{List} \rangle\ \texttt{axF2} \ :\ \texttt{List(F Int)} \sim \texttt{List Bool}/\mathsf{T}$$

On the other hand, the coercion formation rules should disallow the formation of a coercion of the form $\gamma_3 : \texttt{F Age} \sim \texttt{F Int}/\mathsf{T}$, which creates the unsoundness described in Section 2.2.

Figure 1 gives the syntax of coercion terms, γ, and Figure 4 gives their typing rules. Coercions are typechecked using the judgment: $\Gamma \vdash \gamma : \varphi_1 \sim \varphi_2 \in \eta/R$, which asserts that the type of a coercion γ is an equality proposition $\varphi_1 \sim \varphi_2 \in \eta/R$. This proposition in turn implies that φ_1 and φ_2 both have kind η and are equal in role R. Technically, is convenient to include η in the syntax of the judgement to enforce that both types have the same kind. However, this component is not always relevant, so we sometimes omit the $\in \eta$ part, as we have done in the examples above.

Rule CASSM instantiates an axiom scheme with types $\overline{\psi}$, using an auxiliary judgment $\Gamma \vdash \overline{\psi} : \Delta$ defined at the bottom of Figure 3 to ensure that each variable is instantiated with a type of the matching kind and role. The notation $\varphi[\Delta \mapsto \overline{\psi}]$ applies a multi-substitution of the types $\overline{\psi}$ for each of the corresponding variables in the domain of Δ.

Rule CREFL shows that any type φ can be lifted to a reflexive coercion $\langle\varphi\rangle$, while CSYM and CTRANS add symmetry and transitivity, ensuring that equality is an equivalence relation. The rules CAPP and CALL extend equality compatibly over applications and polymorphic types; their structure is analogous to the corresponding kinding rules in Figure 3. Rule CAPP is particularly important, because it implements the key coercion lifting idea we discussed in Section 2.1, using kinds to prevent the formation of the bogus coercion

$$\langle \texttt{F} \rangle\ \texttt{mkAge} : \texttt{F Age} \sim \texttt{F Int}/\mathsf{T}$$

To see why, recall that `F` has kind $\star/\mathsf{C} \to \star$, but the `mkAge` axiom holds only at role T—type equalities cannot be lifted through code functions. Another example of a coercion that is correctly rejected by the application rule (because of the kind of $(\sim_\eta)$) is

$$\langle (\sim_\star) \rangle\ \texttt{mkAge}\ \langle \texttt{Int} \rangle\ \langle \sigma \rangle$$

This coercion proves $(\texttt{Age} \sim \texttt{Int}) \Rightarrow \sigma \sim (\texttt{Int} \sim \texttt{Int}) \Rightarrow \sigma$, an equality that could be used to introduce a bogus assumption that $\texttt{Age} \sim \texttt{Int}/\mathsf{C}$ and satisfy it with reflexivity for `Int`.

As well as composing coercions to witness the equality of bigger types, it is also essential to do the reverse: to decompose equalities over complex types to give equalities of simpler types. Decomposition is required by FC_2's operational semantics (Section 3.6), and it also makes the language usefully more expressive. Rule CINST allows equalities between polymorphic types to be instantiated. The remaining, and most important decomposition rule is CNTHT, which decomposes the application of a datatype constant to arguments. For example, given a coercion γ : `List Int` $\sim$ `List a`$/\mathsf{T}$ we can use $\mathbf{nth}\ 0\ \gamma$ to conclude that `Int` $\sim$ `a`$/\mathsf{T}$. The soundness of this rule depends on the fact that datatypes are *injective*. In general, type functions are not, and hence CNTHT is restricted to datatypes T.

In rule CNTHT, the notation $T\,\overline{\varphi}$ abbreviates the multi-application $((T\,\varphi_1)\ldots\varphi_n)$ for $\varphi_1 \ldots \varphi_n$ in $\overline{\varphi}$. In the conclusion of the rule, the notation $nth\ k\ \overline{\psi}$, accesses the kth element of the sequence of types, and $nth\ k\ \Delta$, accesses the kind of the k^{th} variable binding. Both of these notations are undefined if k is not less than the length of the sequence. The context Δ in this rule is determined by matching the kind of the type constructor with the kinds of the types in the equality proposition.

DEFINITION 3. *We define* $\forall\,\Delta.\eta$ *by induction on* Δ *as follows:*

$$\begin{array}{lcl} \forall\,\cdot.\eta & = & \eta \\ \forall\,(a{:}\kappa, \Delta).\eta & = & \kappa \to (\forall\,\Delta.\eta) \end{array}$$

The coercion judgment satisfies a number of sanity checking properties.

LEMMA 4 (Coercion regularity). *If* $\Gamma \vdash \gamma : \varphi_1 \sim \varphi_2 \in \kappa$ *then* $\Gamma \vdash \varphi_1 : \kappa$ *and* $\Gamma \vdash \varphi_2 : \kappa$.

LEMMA 5 (Unique propositions). *If* $\Gamma \vdash \gamma : \varphi_1 \sim \varphi_2 \in \eta/R$ *and* $\Gamma \vdash \gamma : \varphi_1' \sim \varphi_2' \in \eta'/R$ *then* $\varphi_1 = \varphi_1'$ *and* $\varphi_2 = \varphi_2'$ *and* $\eta = \eta'$.

Equality for Cs is a refinement of that for Ts; that is, code equality implies type equality, but not vice versa.

LEMMA 6. *If* $\Gamma \vdash \gamma : \varphi_1 \sim \varphi_2 \in \eta/\mathsf{C}$ *then* $\Gamma \vdash \gamma : \varphi_1 \sim \varphi_2 \in \eta/\mathsf{T}$.

3.4 Coercion lifting

The application rule CAPP described in the previous section allows us to lift equalities through arbitrary type constructors; that is, for all datatypes T of kind $\star/\mathsf{T} \to \star$, we have a coercion T `Age` $\sim$ T `Int` $\in \star/\mathsf{T}$.

In fact, this notion of coercion lifting is not restricted to datatypes (like `List`), but is available for more general contexts. More precisely, given an arbitrary type σ with free variable a of kind $\star/\mathsf{T}$, we can also create a coercion $\sigma[a \mapsto \texttt{Age}] \sim \sigma[a \mapsto \texttt{Int}] \in \star/\mathsf{T}$.

We create such coercions with the *lifting operation*. This operation replaces type variables by coercions in types to produce a new coercion, relying on the fact that the syntax of types is a subset of the syntax of coercions:

DEFINITION 7 (Lifting Operation). *Define the lifting operation, written $\varphi[a \mapsto \gamma]$, by induction on φ.*

$$\begin{array}{lcll} a[a \mapsto \gamma] & = & \gamma & \\ b[a \mapsto \gamma] & = & \langle b \rangle & \textit{when } a \neq b \\ H[a \mapsto \gamma] & = & \langle H \rangle & \\ (\varphi\,\psi)[a \mapsto \gamma] & = & (\varphi[a \mapsto \gamma])\ (\psi[a \mapsto \gamma]) & \\ (\forall b{:}\kappa.\sigma)[a \mapsto \gamma] & = & \forall b{:}\kappa.(\sigma[a \mapsto \gamma]) & \end{array}$$

The lifting operation produces a valid result as long as the role of the lifted coercion matches the role of the type variable in the type.

LEMMA 8 (Lifting). *If $\Gamma, a{:}\eta/R \vdash \sigma : \kappa$ and $\Gamma \vdash \gamma : \varphi \sim \varphi' \in \eta/R$, then $\Gamma \vdash \sigma[a \mapsto \gamma] : \sigma[a \mapsto \varphi] \sim \sigma[a \mapsto \varphi'] \in \kappa$.*

In other words, if a were used in some indexed context in σ, that is, if its role were C, then we would not be able to lift the coercion $\texttt{Age} \sim \texttt{Int} \in \star/\mathsf{T}$ in σ. We generalise lifting to replace multiple type variables simultaneously in the obvious way, with notation $\sigma[\Delta \mapsto \overline{\gamma}]$.

3.5 Pattern matching and datatypes

FC_2 includes a formalization of recursive datatypes. These datatypes include all Haskell extensions to standard datatypes: empty datatypes, nested datatypes, existential types, first-class polymorphism and GADTs. Both datatypes T and data constructors K must be declared in a context Γ before they can be used. For example, using the syntax for Γ in Figure 1, the declarations for the data constructors of `List` are:

$$\begin{array}{lcl} \texttt{List} & : & \star/\mathsf{T} \to \star \\ \texttt{Nil} & : & (a{:}\star/\mathsf{T}).\,\texttt{List}\ a \\ \texttt{Cons} & : & (a{:}\star/\mathsf{T}).\ a \to \texttt{List}\ a \to \texttt{List}\ a \end{array}$$

What about GADTs? Here's an example in Haskell:

```
data Rep a where
  Rint  :: Rep Int
  Rlist :: Rep a → Rep (List a)
```

Although a Haskell programmer writes the data constructors of a GADT with non-parametric result types, in the internal type system it is more convenient for the result type of a data constructor to take the form $(T\ a_1 \ldots a_n)$, where the $\overline{a}$ are the type parameters, using equality constraints to express the indexing, thus:

$$\begin{array}{ll} \texttt{Rep} & :\star/\mathsf{C} \to \star \\ \texttt{Rint} & :(a{:}\star/\mathsf{C}).(a \sim \texttt{Int}) \Rightarrow \texttt{Rep}\ a \\ \texttt{Rlist} & :(a{:}\star/\mathsf{C}).\forall(b:\star/\mathsf{C}).(a \sim \texttt{List}\ b) \Rightarrow \texttt{Rep}\, b \to \texttt{Rep}\ a \end{array}$$

Notice here that `Rep`'s kind expresses that its argument is an *index* (role C) rather than a *parameter* (role T). In fact, the C role for variable a falls out naturally because a appears as argument to the $(\sim_\star)$ constructor (in the type of `Rint` and `Rlist`), which in turn requires it to have role C.

More generally, we use the notation of *telescopes* [de Bruijn 1991] to conveniently express the kind of a datatype and the types of its data constructors. Figure 1 defines a telescope Θ like this:

$$\Theta ::= \cdot \mid a{:}\kappa, \Theta \mid \varphi_1 \sim \varphi_2, \Theta \mid \sigma, \Theta$$

A telescope is like a mini-context just for arguments: a list of types, type variable bindings, and equality propositions (between codes only) that classify each argument of the data constructor. We also define the syntactic sugar $\forall\,\Theta.\sigma$ as follows:

DEFINITION 9 (Telescope syntactic sugar).

$$\begin{array}{lcl} \forall\,\cdot.\sigma & = & \sigma \\ \forall\,(a{:}\kappa, \Theta).\sigma & = & \forall a{:}\kappa.(\forall\,\Theta.\sigma) \\ \forall\,(\varphi_1 \sim \varphi_2, \Theta).\sigma & = & (\varphi_1 \sim \varphi_2) \Rightarrow (\forall\,\Theta.\sigma) \\ \forall\,(\sigma', \Theta).\sigma & = & \sigma' \to (\forall\,\Theta.\sigma) \end{array}$$

$$\frac{\Sigma \vdash \gamma : (\sigma_1 \to \upsilon_1) \sim (\sigma_2 \to \upsilon_2) \in \star/\mathsf{T} \quad \gamma_0 = \mathbf{sym}\,(\mathbf{nth}\ 0\ \gamma) \quad \gamma_1 = \mathbf{nth}\ 1\ \gamma}{((\lambda x{:}\sigma_1.e_1) \triangleright \gamma)\ e_2 \rightsquigarrow (\lambda x{:}\sigma_1.(e_1 \triangleright \gamma_1))\ (e_2 \triangleright \gamma_0)} \quad \text{SSPUSH}$$

$$\frac{\Sigma \vdash \gamma : \forall a{:}\kappa.\sigma_1 \sim \forall a{:}\kappa.\sigma_2 \in \star/\mathsf{T}}{((\Lambda a{:}\kappa.e) \triangleright \gamma)\ \varphi \rightsquigarrow (\Lambda a{:}\kappa.(e \triangleright \gamma@a))\ \varphi} \quad \text{SSTPUSH}$$

$$\frac{\begin{array}{c}\Sigma \vdash \gamma : (\varphi_1 \sim \varphi_2) \Rightarrow \sigma \sim (\varphi_1' \sim \varphi_2') \Rightarrow \sigma' \in \star/\mathsf{T} \\ \gamma_0 = \mathbf{nth}\ 0\ \gamma \quad \gamma_1 = \mathbf{sym}\,(\mathbf{nth}\ 1\ \gamma) \quad \gamma_2 = \mathbf{nth}\ 2\ \gamma\end{array}}{\begin{array}{l}((\Lambda c{:}\varphi_1 \sim \varphi_2.e) \triangleright \gamma)\ \gamma' \rightsquigarrow \\ \quad (\Lambda c{:}\varphi_1 \sim \varphi_2.(e \triangleright \gamma_2))\ (\gamma_0\ ;\ \gamma'\ ;\ \gamma_1)\end{array}} \quad \text{SSCPUSH}$$

$$\frac{\begin{array}{c}\Sigma \vdash \gamma : T\,\overline{\varphi} \sim T\,\overline{\varphi}' \in \star/\mathsf{T} \\ K{:}\Delta.\sigma \in \Sigma\end{array}}{\begin{array}{l}\mathbf{case}'_\sigma\ (K\,\overline{\varphi}\,\overline{\rho}) \triangleright \gamma\ \mathbf{of}\ brs \rightsquigarrow \\ \quad \mathbf{case}'_\sigma\ K\,\overline{\varphi}'\ (\overline{\rho} \triangleright \sigma[\Delta \mapsto nth\ \gamma])\ \mathbf{of}\ brs\end{array}} \quad \text{SSKPUSH}$$

Figure 5. Operational Semantics (Push rules)

Now the type of *any* data constructor has the form

$$K{:}\Delta.\forall\,\Theta.T\,\Delta$$

where $T\,\Delta$ is syntactic sugar for the application $((T\ a_1) \ldots a_n)$ for $a_1 \ldots a_n$ in the domain of Δ. For example, the telescope for `Cons` is $(a, \texttt{List}\ a, \cdot)$, and the one for `Rlist` is $(b{:}\star/\mathsf{C}, b \sim \texttt{List}\ a, (\texttt{Rep}\ b), \cdot)$.

Moreover, the Δ in the signature for a data constructor must exactly match the kind of its datatype, which we conveniently express by saying that $T{:}\forall\,\Delta.\star$, using the syntactic sugar $\forall\,\Delta.\eta$ in Definition 3.[3]

This notation is used to typecheck a case expression in rule ECASE (Figure 2). The type of the scrutinee of the case must be headed by a datatype constant T. Furthermore, for each data constructor that could create a T, there must be a corresponding branch. After substituting for the parameters, the branch for data constructor K_i must abstract the same arguments as K_i and and return the same result type as the entire case. To make sure that typechecking is syntax directed even when there are no branches (for empty datatypes), the case expression is annotated with its result type σ, and we must check that this type is well-formed in the current context.

3.6 Operational semantics: pushing coercions

The operational semantics of FC_2 is largely standard, so we highlight only the novel features here. As alluded to above, this operational semantics preserves the coercion proofs, which allows us to establish type safety using standard syntactic proofs of progress and preservation (described in the next section). In practice, all of the coercions are erased by the compiler and so impose no run-time costs.

The most important rules of the operational semantics are those that "push" coercions when they appear in active positions so that they do not interfere with reduction. Figure 5 shows the relevant pushing rules. (The complete rules of the operational semantics are listed in the appendix.)

The first three rules show how in an application of a coerced abstraction, the term steps to a new application, where the coercion has been decomposed into a coercion for the body of the abstrac-

[3] Note the difference between $\Delta.\sigma$, which is part of the syntax for declaring a data constructor (Figure 1) and $\forall\,\Delta.\eta$, which is syntactic sugar for the arrow kind of a datatype constructor.

$\boxed{\Gamma \vdash \overline{\rho} : \Theta}$

$$\frac{\vdash \Gamma}{\Gamma \vdash \cdot : \cdot} \quad \text{TNIL}$$

$$\frac{\Gamma \vdash e : \sigma \quad \Gamma \vdash \overline{\rho} : \Theta}{\Gamma \vdash e, \overline{\rho} : (\sigma, \Theta)} \quad \text{TCONSE}$$

$$\frac{\Gamma \vdash \varphi : \kappa \quad \Gamma \vdash \overline{\rho} : \Theta[a \mapsto \varphi]}{\Gamma \vdash \varphi, \overline{\rho} : (a{:}\kappa, \Theta)} \quad \text{TCONST}$$

$$\frac{\Gamma \vdash \gamma : \varphi_1 \sim \varphi_2 \in \kappa \quad \Gamma \vdash \overline{\rho} : \Theta}{\Gamma \vdash \gamma, \overline{\rho} : (\varphi_1 \sim \varphi_2, \Theta)} \quad \text{TCONSC}$$

Figure 6. Telescope rules

tion, and a coercion of the argument. For example, consider SSPUSH. Here, the γ is a coercion between function types $\sigma_1 \to \upsilon_1$ and $\sigma_2 \to \upsilon_2$. The rule uses $\mathbf{nth}$ and $\mathbf{sym}$ to decompose γ into two coercions, one from $\sigma_2 \sim \sigma_1$ (the order is reversed to account for contra-variance) and one from $\upsilon_1 \sim \upsilon_2$. These new coercions can be pushed to the body of the lambda and the function argument, exposing the reduction. Rules SSTPUSH and SSCPUSH work analogously.

Note, however that SSCPUSH justifies the kind of $(\sim_\eta)$, which requires that the first two arguments be codes. If we had assigned $(\sim_\eta)$ the parametric kind $\eta/\mathsf{T} \to \eta/\mathsf{T} \to \star/\mathsf{T} \to \star$, then the coercions γ_0 and γ_1 in the rule would both be type coercions. However, type coercions cannot be composed with γ' to form a code coercion, which is the role required for the right hand side of the rule to typecheck.

The last rule SSKPUSH pushes the coercion of a data constructor in the scrutinee position of a case expression into coercions of the arguments of the data constructor. In this rule we use the telescope notation at the term level: the arguments of a data constructor, notated ρ, can either be an expression, a type, or a coercion.

$$\rho ::= e \mid \varphi \mid \gamma$$

Returning to SSKPUSH, if the declared type of the data constructor K is $K{:}\Delta.\forall\,\Theta.\,T\,\Delta$, then we know that the arguments can be typed by the telescope. i.e. $\Gamma \vdash \overline{\rho} : \Theta[\Delta \mapsto \overline{\varphi}]$ (see Figure 6). However, the coercion changes the types of the parameters to be $\overline{\varphi}'$, so the new arguments must have type $\Theta[\Delta \mapsto \overline{\varphi}']$.

These new arguments are produced by coercing the list of arguments $\overline{\rho}$ with the coercion generated by *lifting* as described above. (The notation $\sigma[\Delta \mapsto \mathit{nth}\ \gamma]$ means that if $\Delta = a_1{:}\kappa_1, \ldots, a_n{:}\kappa_n$, then variable a_i is lifted to coercion $\mathbf{nth}\ i\ \gamma$.) Once this coercion has been defined by lifting, we use it to coerce the list of arguments of the data constructor with the following operation.

DEFINITION 10. *Define $\overline{\rho} \triangleright \gamma$ by induction on $\overline{\rho}$:*

$$\begin{array}{lcl} \cdot \triangleright \gamma & = & \cdot \\ (e, \overline{\rho}) \triangleright \gamma_1 \to \gamma_2 & = & (e \triangleright \gamma_1), \overline{\rho} \triangleright \gamma_2 \\ (\varphi, \overline{\rho}) \triangleright \forall a{:}\kappa.\gamma_2 & = & \varphi, \overline{\rho} \triangleright \gamma_2 \\ (\gamma, \overline{\rho}) \triangleright (\gamma_1 \sim \gamma_2) \Rightarrow \gamma_3 & = & (\mathbf{sym}\,\gamma_1\,;\,\gamma\,;\,\gamma_2), \overline{\rho} \triangleright \gamma_3 \end{array}$$

LEMMA 11. *If $\Gamma \vdash \overline{\rho} : \Theta$ and $\Gamma \vdash \gamma : \forall\,\Theta.\sigma \sim \forall\,\Theta'.\sigma' \in \star/\mathsf{T}$ then $\Gamma \vdash (\overline{\rho} \triangleright \gamma) : \Theta'$*

4. Type safety and consistency

The FC_2 language supports a straightforward proof of type safety based on the usual preservation and progress theorems. Importantly, the progress theorem holds only for *consistent* contexts—those that cannot equate `Int` and `Char`, for example. Below, we state the progress and preservation theorems and give a precise definition of consistency. In the next subsection, we formulate sufficient conditions for proving that a context is consistent.

4.1 Preservation and progress

The preservation proof for FC_2 is standard, relying on the usual regularity and substitution lemmas for the various judgement forms. For space reasons, we omit those definitions here and instead refer the reader to the extended version.

THEOREM 12 (Preservation). *If $\Gamma \vdash e_1 : \sigma$ and $e_1 \rightsquigarrow e_2$ then $\Gamma \vdash e_2 : \sigma$.*

The progress theorem holds only for *closed*, *consistent* contexts. A context is *closed* if it does not contain any term variable bindings. We use the metavariable Σ for closed contexts.

The definition of consistency and the canonical forms lemma are both stated using the notion of *value types*, which correspond to the types of un-coerced FC_2 values. Formally, we define values v and value types τ, with the following grammars:

$$\begin{array}{lcl} \tau & ::= & T \mid (\to) \mid (\sim_\eta) \mid \forall a{:}\kappa.\varphi \mid \tau\,\varphi \\ v & ::= & \lambda x{:}\sigma.e \mid \Lambda a{:}\kappa.e \mid \Lambda c{:}\varphi_1 \sim \varphi_2.e \mid K\,\overline{\varphi}\,\overline{\rho} \end{array}$$

The canonical forms lemma tells us that the shape of a value is determined by its type:

LEMMA 13 (Canonical Forms). *Say $\Sigma \vdash v : \sigma$. Then σ is a value type. Furthermore,*

1. *If $\sigma = \sigma_1 \to \sigma_2$ then v is $\lambda x{:}\sigma_1.e$ or $K\,\overline{\varphi}\,\overline{\rho}$.*
2. *If $\sigma = \forall a{:}\kappa.\sigma'$ then v is $\Lambda a{:}\kappa.e$ or $K\,\overline{\varphi}\,\overline{\rho}$.*
3. *If $\sigma = (\varphi_1 \sim \varphi_2) \Rightarrow \sigma'$ then v is $\Lambda c{:}\varphi_1 \sim \varphi_2.e$ or $K\,\overline{\varphi}\,\overline{\rho}$.*
4. *If $\sigma = T\,\overline{\varphi}_1$ then v is $K\,\overline{\varphi}\,\overline{\rho}$.*

In FC_2, not all irreducible forms are values. Evaluation can also produce a *coerced value* of the form $v \triangleright \gamma$, which erases to a value when coercions are dropped. To prove the progress theorem, we must reason about what sort of coercion γ could be so that we can appropriately apply the "push" rules in Figure 5. Here, because γ coerces the value v, we know (by ECOERCE and canonical forms) that $\gamma : \tau \sim \sigma$—the left type is a value type τ. *Consistency* of the axiom set assures us that if σ is also a value type, it must have the same head form.

DEFINITION 14 (Consistency). *A context Γ is consistent if whenever $\Gamma \vdash \gamma : \tau_1 \sim \tau_2 \in \eta/\mathsf{T}$ it is the case that*

1. *If τ_1 is $T\,\overline{\varphi}_1$ then τ_2 is $T\,\overline{\varphi}_2$.*
2. *If τ_1 is $(\to)\,\overline{\varphi}_1$ then τ_2 is $(\to)\,\overline{\varphi}_2$.*
3. *If τ_1 is $(\sim_\eta)\,\overline{\varphi}_1$ then τ_2 is $(\sim_\eta)\,\overline{\varphi}_2$.*
4. *If τ_1 is $\forall a{:}\kappa.\sigma_1$ then τ_2 is $\forall a{:}\kappa.\sigma_2$.*

Putting these observations together, we obtain:

THEOREM 15 (Progress). *If Σ is consistent and $\Sigma \vdash e_1 : \sigma$ and e_1 is not a value v or a coerced value $v \triangleright \gamma$, then there exists an e_2 such that $e_1 \rightsquigarrow e_2$.*

4.2 Conditions for consistency

Although the previous subsection gives a definition of when contexts are consistent, it does not provide any mechanism for determining whether a set of axioms leads to a consistent context.

This subsection defines *sufficient* conditions (written $\mathbf{Good}\,\Gamma$) for establishing context consistency—these conditions are not the only way to show consistency (they are not *necessary*) but they are permissive enough to cover the axioms generated by compilation of type family declarations and newtype definitions.

$\boxed{\Gamma \vdash \varphi \rightsquigarrow \varphi' \in \kappa}$

$$\frac{\Gamma \vdash a : \forall\, \Delta.\eta/R \quad \Gamma \vdash \overline{\varphi} \rightsquigarrow \overline{\varphi}' \in \Delta/R}{\Gamma \vdash a\,\overline{\varphi} \rightsquigarrow a\,\overline{\varphi}' \in \eta/R}\ \text{RVAR}$$

$$\frac{H{:}\forall\, \Delta.\eta \in \Gamma \quad \Gamma \vdash \overline{\varphi} \rightsquigarrow \overline{\varphi}' \in \Delta/R \quad \Gamma \not\vdash \mathbf{match}\, H\,\overline{\varphi}' \in \eta/R}{\Gamma \vdash H\,\overline{\varphi} \rightsquigarrow H\,\overline{\varphi}' \in \eta/R}\ \text{RCONST}$$

$$\frac{\Gamma, a{:}\kappa \vdash \sigma \rightsquigarrow \sigma' \in \star/R}{\Gamma \vdash \forall a{:}\kappa.\sigma \rightsquigarrow \forall a{:}\kappa.\sigma' \in \star/R}\ \text{RALL}$$

$$\frac{H{:}\forall\, \Delta_1.\forall\, \Delta_2.\eta \in \Gamma \quad \Gamma \vdash \overline{\varphi}_1 \rightsquigarrow \overline{\varphi}'_1 \in \Delta_1/R \quad \Gamma \vdash \overline{\varphi}_2 \rightsquigarrow \overline{\varphi}'_2 \in \Delta_2/R \quad \Gamma \vdash c\,\overline{\psi} : H\,\overline{\varphi}'_1 \sim \upsilon \in \forall\, \Delta_2.\eta/R}{\Gamma \vdash H\,\overline{\varphi}_1\,\overline{\varphi}_2 \rightsquigarrow \upsilon\,\overline{\varphi}'_2 \in \eta/R}\ \text{RRED}$$

$\boxed{\Gamma \vdash \overline{\varphi} \rightsquigarrow \overline{\varphi}' \in \Delta/R}$

$$\frac{}{\Gamma \vdash \cdot \rightsquigarrow \cdot \in \cdot/R}\ \text{RNIL}$$

$$\frac{\Gamma \vdash \varphi \rightsquigarrow \varphi' \in \eta/\mathit{min}(R_1, R_2) \quad \Gamma \vdash \overline{\varphi} \rightsquigarrow \overline{\varphi}' \in \Delta/R_1}{\Gamma \vdash \varphi, \overline{\varphi} \rightsquigarrow \varphi', \overline{\varphi}' \in a{:}\eta/R_2, \Delta/R_1}\ \text{RCONS}$$

Figure 7. Type rewriting

As in the previous version of FC, we show consistency by defining a rewriting system for types and proving that two types are joinable (share a common reduct) if and only if there is some coercion proof between those types. The rewrite system guarantees that value types preserve their head form throughout rewriting and therefore value types with different head forms can never be equated.

The rewriting relation is novel in two ways.

- It takes roles into account: rewriting occurs at some role R, which specifies what axioms are available. For example, at role T we can rewrite a newtype `Age` to its definition `Int`, but at role C, we cannot.
- It is *deterministic* and *total*. In a good context Γ, each φ has exactly one φ' that it rewrites to—the rewrite system is trivially confluent. As a consequence, to prove soundness and completeness with respect to the coercion proof system we do not need to show that the rewriting system is terminating.

These properties stand in contrast to previous work [Sulzmann et al. 2007] in which establishing type soundness is contingent on strong normalization of the axiom sets. With our new approach, this termination requirement is relaxed—a programmer can be confident that, even in the presence of possibly non-terminating type functions, if the compiler can show that the program is well-typed, it won't crash.

Figure 7 shows the rewriting relation, which is a variant of parallel reduction—it looks throughout the type, trying to do as many reductions as possible. Whether a reduction of a type constant happens is governed by rules RCONST and RRED. If, after the arguments to H have been reduced to $\overline{\varphi}'$, there is some instantiation of an axiom such that H applied to some prefix of the $\overline{\varphi}'$ matches the left-hand side of the coercion, then the type reduces to the right-hand-side type (RRED). The precondition $\Gamma \not\vdash \mathbf{match}\, H\,\overline{\varphi}' \in \eta/R$ in RCONST means that there is no such match, so these two rules are mutually exclusive, which is necessary for determinism.

Unlike standard definitions of parallel reduction, the rewriting relation has no general reflexivity rules. Instead, the relation is reflexive only for "normal form" types: those with no subcomponents that match an axiom. The definition of normal form types appears in the appendices.

LEMMA 16. *If* $\Gamma \vdash \varphi\, \mathbf{normal} \in \kappa$ *then* $\Gamma \vdash \varphi \rightsquigarrow \varphi \in \kappa$.

The sufficient conditions for consistent contexts are stated in terms of the normal forms of this rewrite relation.

DEFINITION 17 (Good contexts). *We have* $\mathbf{Good}\,\Gamma$ *when the following conditions hold:*

1. *All axioms rewrite type functions applied to normal arguments. In other words, all axioms are of the form:* $c : \Delta.\, F\,\overline{\varphi} \sim \psi/R$ *and if* $F{:}\forall\, \Delta'.\eta \in \Gamma$*, we have* $\Gamma \vdash \overline{\varphi}\, \mathbf{normal} \in \Delta'/R$.
2. *There is no overlap between axioms. For each* $F\,\overline{\varphi}$*, there is exactly one prefix* $\overline{\varphi}_1$ *of* $\overline{\varphi}$*, such that there exists a* c*,* $\overline{\psi}$*, and* υ *where* $\Gamma \vdash c\,\overline{\psi} : F\,\overline{\varphi}_1 \sim \upsilon \in \kappa$.

The condition that the arguments to type functions must be normal restricts the kind that a type function may have. For example, recall the axioms for `F` from Section 2.2:

$$\texttt{axF1} : \texttt{F Int} \sim \texttt{Bool}/\mathsf{C}$$
$$\texttt{axF2} : \texttt{F Age} \sim \texttt{Char}/\mathsf{C}$$

For this to be a $\mathbf{Good}$ axiom set, the kind of `F` must be $\star/\mathsf{C} \to \star$ because the newtype `Age` is only normal in role C. However, if a type function, such as `G` below, does not include any axioms that match newtypes, it may be assigned the kind $\star/\mathsf{T} \to \star$.

$$\texttt{axG1} : \texttt{G Int} \sim \texttt{Bool}/\mathsf{C}$$
$$\texttt{axG2} : \texttt{G Bool} \sim \texttt{Char}/\mathsf{C}$$

In the rest of this section, we sketch the proof that our conditions are sufficient for consistency. Below, assume that all contexts are good. We first observe that good contexts yield deterministic rewrite systems.

LEMMA 18 (Determinacy). *If* $\mathbf{Good}\,\Gamma$ *and* $\Gamma \vdash \varphi \rightsquigarrow \varphi_1 \in \kappa$ *and* $\Gamma \vdash \varphi \rightsquigarrow \varphi_2 \in \kappa$ *then* $\varphi_1 = \varphi_2$.

The two most important results of this section are that rewriting is sound and complete with respect to the coercion proof system. Soundness is a straightforward proof.

THEOREM 19 (Soundness). *If* $\Gamma \vdash \varphi_1 \rightsquigarrow \varphi_2 \in \kappa$ *then there is some* γ *such that* $\Gamma \vdash \gamma : \varphi_1 \sim \varphi_2 \in \kappa$.

We show completeness for a reflexive, symmetric, transitive closure of rewriting. We call this relation *joinability*.

DEFINITION 20 (Joinable). *Two types are* joinable *if they share a common reduct. Define* $\Gamma \vdash \varphi_1 \Leftrightarrow \varphi_2 \in \kappa$ *if* $\Gamma \vdash \varphi_1 \rightsquigarrow^* \varphi \in \kappa$ *and* $\Gamma \vdash \varphi_2 \rightsquigarrow^* \varphi \in \kappa$.

The two key lemmas of the completeness proof are that joinability is preserved under application and substitution.

LEMMA 21 (Application). *If* $\mathbf{Good}\,\Gamma$ *and* $\Gamma \vdash \varphi_1 \Leftrightarrow \varphi'_1 \in (\eta_1/R_1 \to \eta_2)/R_2$ *and* $\Gamma \vdash \varphi_2 \Leftrightarrow \varphi'_2 \in \eta_1/\mathit{min}(R_1, R_2)$ *then* $\Gamma \vdash \varphi_1\,\varphi_2 \Leftrightarrow \varphi'_1\,\varphi'_2 \in \eta_2/R_2$.

LEMMA 22 (Substitution). *If* $\mathbf{Good}\,\Gamma$ *and* $\Gamma, a{:}\kappa\,\Delta \vdash \sigma \rightsquigarrow^* \sigma' \in \kappa'$ *and* $\Gamma \vdash \varphi \rightsquigarrow^* \varphi' \in \kappa$*, then there is some* $\Gamma\,\Delta \vdash \sigma[a \mapsto \varphi] \Leftrightarrow \sigma'[a \mapsto \varphi'] \in \kappa'$.

THEOREM 23 (Completeness). *If* $\mathbf{Good}\,\Gamma$ *and* $\Gamma \vdash \gamma : \varphi_1 \sim \varphi_2 \in \kappa$ *then* $\Gamma \vdash \varphi_1 \Leftrightarrow \varphi_2 \in \kappa$.

COROLLARY 24 (Empty context is consistent). *The initial context Σ (with no axioms) is consistent as it trivially satisfies* $\mathbf{Good}\ \Sigma$.

5. Compilation from source Haskell

In the previous sections we have informally presented the translations of Haskell source features such as datatype, type family, and **newtype** declarations into FC_2. We summarize them here:

$$\begin{array}{ll}
\textbf{data}\ T\ \Delta\ \textbf{where}\ \overline{K_i : \sigma} & \mapsto \\
\quad T : \forall \Delta.\star, \overline{K_i : \Delta.\sigma} & \\
\textbf{type family}\ F : \overline{\eta/\mathsf{C}} \to \eta & \mapsto \\
\quad F : \overline{\eta/\mathsf{C}} \to \eta & \\
\textbf{type instance}\ \Delta.F\ \overline{\varphi} = \psi & \mapsto \\
\quad cF : \Delta.F\ \overline{\varphi} \sim \psi \in \eta/\mathsf{C} & \\
\textbf{newtype}\ \Delta.M\ \overline{a} = \mathtt{MkM}\ \varphi & \mapsto \\
\quad M : \Delta.\star, \mathtt{MkM} : \Delta.M\ \overline{a} \sim \varphi \in \star/\mathsf{T} &
\end{array}$$

The important parts of this definition are that (i) type families accept code arguments, (ii) type families give rise to code equalities, and (iii) newtype definitions give rise to type equality axioms. The bindings generated in this way can be easily checked for well-formedness. If, in addition, the resulting context is $\mathbf{Good}$ (see Section 4.2)—the only possible problem is the potential to generate overlapping **type instance** declarations—then the context is consistent, which in turn guarantees type safety.

The careful reader will have noticed that the source language features in this translation have been *already annotated* with their kinds. This is a reasonable assumption. Prior to type inference, which translates a source declaration to an FC_2 binding, we must have determined the kinds involved in the declarations. For the purposes of this paper, we assume that the kinds are given—in practice they would be the output of a kind inference process, potentially guided by the user to disambiguate role information and higher-order kinds.

Newtype deriving Generative type abstraction is achieved in Haskell using the **newtype deriving** mechanism, which allows type classes to be automatically lifted to new types. For instance, we may write

```
newtype Age = MkAge Int deriving Eq
```

The type class `Eq a` is a standard class in Haskell (signature, in ML terminology) that defines one method, `eq :: a → a → Bool`. For the type checker, a type class is nothing but a record type containing the method `eq`. The **deriving** line automatically generates an implementation of `Eq Age` from a pre-existing instance `Eq Int`. This can be done by simply applying a coercion `Eq Int` ∼ `Eq Age` to the old record. It is straightforward to construct this coercion: lift the `Age` ∼ `Int` axiom from the **newtype** definition over the `Eq` constructor and apply symmetry. Importantly, this lifting is safe because `Eq` has a *parametric kind* of the form $\star/\mathsf{T} \to \star$ (vs. $\star/\mathsf{C} \to \star$). However, if a type class has a *indexed kind*, **newtype deriving** is no longer sound. The documented GHC bug mentioned earlier arises precisely as the result of such an unsound lifting over a non-parametric type class.

6. Discussion

6.1 Relaxing decomposition

Recall the coercion decomposition rule, CNTHT, from Figure 4. This rule allows us to deconstruct an equality of the form $\Gamma \vdash \gamma : T\ \overline{\varphi} \sim T\ \overline{\psi} \in \eta/\mathsf{T}$. In effect, it asserts that data constructors are injective. The rule is important because it is used in the operational semantics to ensure subject reduction. However, the decomposition rule may be somewhat restrictive for some Haskell source programs. Consider the following:

```
newtype M a = MkM (Maybe [a])
data Eq a b where EQ :: Eq a a
f :: Eq (M a) (M b) → a → b
f EQ x = x
```

Pattern matching against the `EQ` constructor introduces a coercion between `M a` and `M b`, which cannot be decomposed using the CNTHT rule to obtain `a` ∼ `b`, so this program cannot be typed. Nevertheless, *we know* that `M` is injective, because `M a` is defined to be equal to `Maybe [a]`, which is clearly injective.

On the other hand, the following **newtype** is *not* injective.

```
type instance G a  = Char
newtype N a = MkN (G a)
```

Here, it is possible to derive $\Gamma \vdash \gamma :$ `N Int` ∼ `N Char` $\in \star/\mathsf{T}$, using the axiom for `G`, even though `Int` is not coercible to `Char`.

It turns out that **newtype** definitions are *always* injective with respect to code equality, but they might not be injective with respect to type equality (as illustrated by the two examples above). Thus it would be sound and potentially useful (but not necessary for type soundness) to introduce yet another decomposition rule for **newtype** definitions that takes advantage of injectivity with respect to codes (we use letter N below for newtypes):

$$\frac{\begin{array}{l}\Gamma \vdash \gamma : N\ \overline{\varphi} \sim N\ \overline{\psi} \in \eta/\mathsf{C} \\ N{:}\forall\, \Delta.\eta\ \in\ \Gamma \\ \eta'/R' = nth\ k\ \Delta\end{array}}{\Gamma \vdash \mathbf{nth}\ k\ \gamma : nth\ k\ \overline{\varphi} \sim nth\ k\ \overline{\psi} \in \eta'/R}\ \text{CNTHN}$$

The only subtle part of this rule is that R is not related to R', since the equality $\Gamma \vdash \gamma : N\ \overline{\varphi} \sim N\ \overline{\psi} \in \eta/\mathsf{C}$ is a C-equality (and $min(\mathsf{C}, R') = \mathsf{C}$).

Arguably, decomposition for injective type functions is also desirable, were we able to effectively specify and check that property.

6.2 Other technical differences of FC_2 from System FC

The intermediate language FC_2 described in this paper is a significant modification of System FC [Sulzmann et al. 2007] due to the introduction of codes. However, FC_2 also makes a number of *technical simplifications*:

- The original System FC presentation includes *coercion kinds*, $\sigma_1 \sim \sigma_2$. The original coercion language includes three additional constructs, one to coerce coercions, and two more to decompose coercion kinds. By treating $(\varphi_1 \sim \varphi_2) \Rightarrow \varphi_3$ as the application of a constructor $(\sim_\eta)$ we no longer need any of these constructs in the operational semantics, nor have we identified any uses of these constructs that are not encodable.
- The operational semantics rules of FC_2 in Figure 5 not only use simpler coercion constructs, but are also expressed without need for substitutions, contrary to their original FC versions.
- FC_2 replaces the FC coercions $\mathbf{left}$ and $\mathbf{right}$, which decomposed arbitrary type applications, by $\mathbf{nth}$, which decomposes only the application of a datatype constructor. The latter is a little less expressive. Generalizing the example from Section 6.1, should this program be well typed?

  ```
  data Eq a b where EQ :: Eq a a
  f :: Eq (p q) (r s) → q → s
  f EQ x = x
  ```

  To type it we must decompose a proof that $p\ q \sim r\ s$ to get a proof that $q \sim s$, which $\mathbf{right}$ could do, but $\mathbf{nth}$ cannot.
- One consequence of using $\mathbf{nth}$ instead of $\mathbf{left}$ and $\mathbf{right}$ is that type functions in FC_2 are not required to be saturated, as they were in System FC. Type family saturation was necessary

in FC, in order to prevent the decomposition of equalities as `F` $a \sim$ `Maybe` $[a]$ via **left** or **right**. Allowing unsaturated functions increases the expressivity of FC_2 but also opens new directions for future research on type inference in the presence of unsaturated type functions.

Some other differences are *presentational*:

- System FC used a common syntax for types and coercions, which is a convenient pun, but has turned out to be more confusing than helpful. In FC_2 we use a distinct syntax for types and coercions (Figure 1).
- In FC_2 we define top-level axiom schemes $c : \Delta.\, \varphi_1 \sim \varphi_2 / R$ directly, and fully instantiate them at every occurrence with the form $c\ \overline{\gamma}$ (Figure 1). System FC instead defined a top-level axiom scheme as an equality between polytypes, thus $c : \forall\Delta.\varphi_1 \sim \forall\Delta.\varphi_2$. Here again FC is confusing (but not wrong) so in FC_2 we opt for telling the story more directly, albeit with slightly more syntax. Moreover the kinding rules for $\forall$ (PALL and CALL) can insist that the body of the forall has kind $\star$ as is conventional.
- Using telescopes in the treatment of datatypes simplifies the operational semantics rules but is also (only slightly) more expressive: The types of data constructors do not have to have their quantified variables preceding their coercion and term arguments. Instead, telescopes allow arbitrary interleavings.

7. Related work

Previous work on System FC [Sulzmann et al. 2007] discusses a significant amount of related work, in typed languages with explicit proof witnesses [Licata and Harper 2005; Shao et al. 2005], or in calculi that support coercions [Breazu-Tannen et al. 1991]. Below, we present related work in generativity and abstraction, type-indexed constructs and the separation between codes and types.

Generativity, abstraction, and module systems Generativity and abstraction has been studied extensively in the context of ML module systems [Milner et al. 1997]. Russo shows how generativity in module systems is connected to existential quantification [Russo 1999] and Dreyer [2005] has studied this connection in the presence of recursive modules. In recent work, Montagu and Rémy [2009] refine this connection by introducing "open" existential types.

Type abstraction can be understood in terms of name generation [Rossberg 2003; Vytiniotis et al. 2005], which can re-establish abstraction properties in languages with dynamic type analysis. Neis et al. [2009] prove a parametricity theorem in this setting. In addition, they use a translation from polymorphism to generative types to establish the parametric behavior of certain functions although they work in a non-parametric language.

Although many of these languages support type generativity and non-parametric features, they do not exhibit the soundness problems described in the paper, mainly due to the absence of type-level type dispatching. Nevertheless, the techniques developed in the aforementioned related work would be valuable in the formal study of the parametricity properties of FC_2.

Type-indexed types Although many systems for generic programming support dynamic computation based on types, very few systems allow the structure of *types* to be destructed to produce other types. However, such facility is often necessary to describe the *type* of generic programs. For example, Harper and Morrisett include a `Typerec` operator to their typed intermediate language λ_i^{ML} [Harper and Morrisett 1995], to describe type-directed optimizations. (They credit NuPRL's mechanism of "Universe Elimination" in NuPRL as the inspiration for this operation [Constable 1982; Constable and Zlatin 1984].)

To support generic programming in source languages, Hinze, Jeuring and Löh added Type-Indexed Datatypes [Hinze et al. 2002] to the Generic Haskell front end. In later work, Chakravarty et al. [2005b] introduced associated data families in GHC, which are type-indexed datatypes associated with type class instances. Extending this work, they later introduced associated type synonyms [Chakravarty et al. 2005a], which are proper type-level functions with instances associated with type class instances. Currently, the source language of GHC also supports standalone type-level type functions, often referred to as indexed type families [Kiselyov et al. 2010; Schrijvers et al. 2008], a feature that we have extensively used in our presentation.

Codes, types, and interpretations Our distinction between codes and types—and our terminology—is inspired by similar notions in intuitionistic type theory [Benke et al. 2003; Dybjer 2000; Martin-Löf 1975]. There, types (sets) are constructed as the recursive interpretation of codes, which inhabit inductively constructed *code universes*. A **`newtype`** definition can be viewed as giving rise to a new code, inhabiting an open universe of codes, and whose interpretation coincides with the interpretation of its definition.

Languages based on dependent type theory, such as Agda [Bove et al. 2009] or Coq [The Coq Team], naturally offer type-level computation to construct types, but they allow elimination of codes only, not types. Therefore, they do not exhibit the same soundness problem, as the expressiveness of these languages can readily enforce the distinction between types and codes. The disadvantage is the extra programming verbosity of explicit definitions and interpretations of codes. To better support generic programming, the dependently-typed language Epigram [Chapman et al. 2010] identifies types with their code universes.

The LX language [Crary et al. 1998] also uses universe constructions to solve problems with type-directed compilation. When the type translation in a compiler pass is not the identity then type dispatch must be compiled to code dispatch (so the generated code can dispatch on source types instead of target types). The interpretation of codes is then the type translation. To support universes, LX includes datakinds (for codes) and primitive recursive functions over datakinds (for their interpretation at types). In LX, source types `Age` and `Int` would be mapped to definable codes `AgeCode` and `IntCode`, and would be accompanied by an interpretation function such that `interp(AgeCode)` equals `Int` and `interp(IntCode)` equals `Int`. Therefore, the problem with generativity would not show up in that context. If one wanted to solve the problem in this paper along the LX lines, one would have to translate source Haskell types to void types that stand in as codes and handle the `interp()` function as any other type function. This function, as well as interpreting the codes as types, would have to be accompanied with suitable congruence axioms, like `interp(T t)` $\sim$ `T (interp(t))`. Explicitly introducing these axioms means that coercions would be significantly more verbose. Our system dispenses with an explicit `interp()` function by conveniently using the roles in the judgements to determine whether we wish to derive an equality between codes or between their interpretations.

8. Conclusions and future work

In this paper we have identified a problem for the safe interaction of flexible type generativity and type-level computation. We have proposed a solution that distinguishes between indexed and parametric type contexts, by extending the language of kinds, and formalized the solution in the FC_2 language. We have several avenues for future research in mind, which we outline below.

Source language technology We would like to work on ways to expose the FC_2 expressive features to programmers. Specific

directions are: enriching the kind declarations with the ability to declare parametric or indexed type-level constructs, introducing type family injectivity annotations, extending kind inference with roles, and extending type inference to support unsaturated functions using the more sophisticated kinds.

Enriching the universes of codes with terms We are currently working on enriching the universe of codes with constants or functions drawn from the *term* syntax, such as data constructors, in order to enable direct dependently-typed programming in Haskell.

Refining equality in code universes Lemma 6 asserts that the equivalence classes induced by T-equality are refined by the C-equality. However, our approach readily extends to arbitrary hierarchies of universes $\mathsf{C}_n \preceq \mathsf{C}_{n-1} \preceq \ldots \preceq \mathsf{C} \preceq \mathsf{T}$ with gradually more refined equivalence classes as we move down the $\preceq$ relation. It is an interesting direction for future research to investigate whether more levels in the universe hierarchy have any important theoretical or practical implications.

Acknowledgements

We would like to thank Brent Yorgey and the attendees of the Type System Wrestling sessions at MSR Cambridge for many useful discussions. We wrote this paper using the Ott tool (`http://www.cl.cam.ac.uk/~pes20/ott/`).

References

M. Benke, P. Dybjer, and P. Jansson. Universes for generic programs and proofs in dependent type theory. *Nordic J. of Computing*, 10(4):265–289, 2003. ISSN 1236-6064.

A. Bove, P. Dybjer, and U. Norell. A brief overview of agda — a functional language with dependent types. In *TPHOLs '09: Proceedings of the 22nd International Conference on Theorem Proving in Higher Order Logics*, pages 73–78, Berlin, Heidelberg, 2009. Springer-Verlag.

V. Breazu-Tannen, T. Coquand, C. A. Gunter, and A. Scedrov. Inheritance as implicit coercion. *Information and Computation*, 93:172–221, 1991.

M. M. T. Chakravarty, G. Keller, and S. P. Jones. Associated type synonyms. In *ICFP '05: Proceedings of the Tenth ACM SIGPLAN International Conference on Functional Programming*, pages 241–253, New York, NY, USA, 2005a. ACM.

M. M. T. Chakravarty, G. Keller, S. P. Jones, and S. Marlow. Associated types with class. *SIGPLAN Not.*, 40(1):1–13, 2005b. ISSN 0362-1340.

J. Chapman, P. Évariste Dagand, C. McBride, and P. Morris. The gentle art of levitation. In *Proceedings of the Fifteenth ACM SIGPLAN International Conference on Functional Programming (ICFP '10)*, Baltimore, MD, USA, September 2010. To appear.

J. Cheney and R. Hinze. First-class phantom types. CUCIS TR2003-1901, Cornell University, 2003.

R. L. Constable. Intensional analysis of functions and types. Technical Report CSR-118-82, Department of Computer Science, University of Edinburgh, June 1982.

R. L. Constable and D. R. Zlatin. The type theory of PL/CV3. *ACM Transactions on Programming Languages and Systems*, 6(1):94–117, Jan. 1984.

K. Crary, S. Weirich, and G. Morrisett. Intensional polymorphism in type erasure semantics. In *Proceedings of the Third ACM SIGPLAN International Conference on Functional Programming*, pages 301–313, Baltimore, MD, USA, Sept. 1998.

N. G. de Bruijn. Telescopic mappings in typed lambda calculus. *Inf. Comput.*, 91(2):189–204, 1991. ISSN 0890-5401.

D. Dreyer. Recursive type generativity. In *ICFP '05: Proceedings of the Tenth ACM SIGPLAN International Conference on Functional Programming*, pages 41–53, New York, NY, USA, 2005. ACM.

P. Dybjer. A general formulation of simultaneous inductive-recursive definitions in type theory. *Journal of Symbolic Logic*, 65(2):525–549, 2000.

C. V. Hall, K. Hammond, S. L. Peyton Jones, and P. L. Wadler. Type classes in Haskell. *ACM Transactions on Programming Languages and Systems*, 18(2):109–138, Mar. 1996.

R. Harper and G. Morrisett. Compiling polymorphism using intensional type analysis. In *POPL '95: Proceedings of the 22nd ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, pages 130–141, New York, NY, USA, 1995. ACM. ISBN 0-89791-692-1.

R. Hinze, J. Jeuring, and A. Löh. Type-indexed data types. In B. M. Eerke Boiten, editor, *Proceedings of the Sixth International Conference on Mathematics of Program Construction (MPC 2002)*, pages 148–174, Dagstuhl, Germany, July 2002.

O. Kiselyov, S. Peyton Jones, and C. Shan. *Fun with type functions*. Springer, 2010.

D. R. Licata and R. Harper. A formulation of dependent ML with explicit equality proofs. Technical Report CMU-CS-05-178, Carnegie Mellon University Department of Computer Science, 2005.

P. Martin-Löf. An intuitionistic theory of types: Predicative part. In *Proceedings of the Logic Colloquium, 1973*, volume 80 of *Studies in Logic and the Foundations of Mathematics*, pages 73–118. North-Holland, 1975.

R. Milner, M. Tofte, and D. Macqueen. *The Definition of Standard ML*. MIT Press, Cambridge, MA, USA, 1997. ISBN 0262631814.

B. Montagu and D. Rémy. Modeling abstract types in modules with open existential types. In *POPL '09: Proceedings of the 36th annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 354–365, New York, NY, USA, 2009. ACM.

G. Neis, D. Dreyer, and A. Rossberg. Non-parametric parametricity. In *ICFP '09: Proceedings of the 14th ACM SIGPLAN International Conference on Functional Programming*, pages 135–148, New York, NY, USA, 2009. ACM. ISBN 978-1-60558-332-7.

S. Peyton Jones et al. The Haskell 98 language and libraries: The revised report. *Journal of Functional Programming*, 13(1):0–255, Jan 2003. `http://www.haskell.org/definition/`.

S. L. Peyton Jones, D. Vytiniotis, S. Weirich, and G. Washburn. Simple unification-based type inference for GADTs. In *International Conference on Functional Programming (ICFP)*, Portland, OR, USA, Sept. 2006.

B. C. Pierce, editor. *Advanced Topics in Types and Programming Languages*. MIT Press, 2005.

A. Rossberg. Generativity and dynamic opacity for abstract types. In *PPDP '03: Proceedings of the 5th ACM SIGPLAN International Conference on Principles and Practice of Declaritive Programming*, pages 241–252, New York, NY, USA, 2003. ACM. ISBN 1-58113-705-2.

C. V. Russo. Non-dependent types for Standard ML modules. In *PPDP '99: Proceedings of the International Conference PPDP'99 on Principles and Practice of Declarative Programming*, pages 80–97, London, UK, 1999. Springer-Verlag. ISBN 3-540-66540-4.

T. Schrijvers, S. Peyton Jones, M. Chakravarty, and M. Sulzmann. Type checking with open type functions. In *ICFP '08: Proceeding of the 13th ACM SIGPLAN international conference on Functional programming*, pages 51–62, New York, NY, USA, 2008. ACM.

Z. Shao, V. Trifonov, B. Saha, and N. Papaspyrou. A type system for certified binaries. *ACM Trans. Program. Lang. Syst.*, 27(1):1–45, 2005.

M. Sulzmann, M. M. T. Chakravarty, S. P. Jones, and K. Donnelly. System F with type equality coercions. In *TLDI '07: Proceedings of the 2007 ACM SIGPLAN International Workshop on Types in Languages Design and Implementation*, pages 53–66, New York, NY, USA, 2007. ACM.

The Coq Team. *Coq*. URL `http://coq.inria.fr`.

D. Vytiniotis, G. Washburn, and S. Weirich. An open and shut typecase. In *ACM SIGPLAN Workshop in Types in Language Design and Implementation*, Long Beach, CA, USA, Jan. 2005.

H. Xi, C. Chen, and G. Chen. Guarded recursive datatype constructors. In *POPL*, pages 224–235, 2003.

A. Additional specification

For space reasons, the following definitions and rules did not appear in the main text of the paper.

DEFINITION 25. *We define* $\forall\,\Delta.\sigma$ *by induction on* Δ *as follows:*

$$\begin{array}{lcl} \forall\,\cdot.\sigma & = & \sigma \\ \forall\,(a{:}\kappa,\Delta).\sigma & = & \forall a{:}\kappa.(\forall\,\Delta.\sigma) \end{array}$$

DEFINITION 26 (Multilifting Operation). *Define the multiple lifting operation, written* $\varphi[\Delta \mapsto \overline{\gamma}]$*, by induction on* φ*.*

$$\begin{array}{lcl} a[\Delta \mapsto \overline{\gamma}] & = & \gamma_i \quad \textit{when } a_i : \kappa_i \textit{ in } \Delta \\ b[\Delta \mapsto \overline{\gamma}] & = & \langle b \rangle \quad \textit{when } b \notin \Delta \\ H[\Delta \mapsto \overline{\gamma}] & = & \langle H \rangle \\ (\varphi\,\psi)[\Delta \mapsto \overline{\gamma}] & = & (\varphi[\Delta \mapsto \overline{\gamma}])\ (\psi[\Delta \mapsto \overline{\gamma}]) \\ (\forall b{:}\kappa.\sigma)[\Delta \mapsto \overline{\gamma}] & = & \forall b{:}\kappa.(\sigma[\Delta \mapsto \overline{\gamma}]) \end{array}$$

$\boxed{\Gamma \vdash bnd}$

$$\frac{}{\Gamma \vdash a{:}\kappa}\ \textsc{BTVar}$$

$$\frac{}{\Gamma \vdash (\rightarrow){:}\star/\mathsf{T} \rightarrow \star/\mathsf{T} \rightarrow \star}\ \textsc{BArr}$$

$$\frac{}{\Gamma \vdash (\sim_\eta){:}\eta/\mathsf{C} \rightarrow \eta/\mathsf{C} \rightarrow \star/\mathsf{T} \rightarrow \star}\ \textsc{BCoerce}$$

$$\frac{}{\Gamma \vdash T{:}\eta}\ \textsc{BConst}$$

$$\frac{}{\Gamma \vdash F{:}\eta}\ \textsc{BFun}$$

$$\frac{\Gamma\,\Delta \vdash \varphi_1 : \eta/R \quad \Gamma\,\Delta \vdash \varphi_2 : \eta/R}{\Gamma \vdash c{:}\Delta.\,\varphi_1 \sim \varphi_2/R}\ \textsc{BCVar}$$

$$\frac{\Gamma \vdash \sigma : \star/\mathsf{T}}{\Gamma \vdash x{:}\sigma}\ \textsc{BEVar}$$

$$\frac{\begin{array}{l} T{:}\forall\,\Delta.\star \in \Gamma \\ \Gamma\,\Delta \vdash \forall\,\Theta.T\,\Delta : \star/\mathsf{T} \end{array}}{\Gamma \vdash K{:}\Delta.(\forall\,\Theta.T\,\Delta)}\ \textsc{BDataCon}$$

$\boxed{\vdash \Gamma}$

$$\frac{}{\vdash \cdot}\ \textsc{GEmpty}$$

$$\frac{dom\ bnd \# dom\,\Gamma \quad \Gamma \vdash bnd \quad \vdash \Gamma}{\vdash \Gamma\ bnd}\ \textsc{GCons}$$

$\boxed{\Gamma \vdash \varphi\,\mathbf{normal} \in \kappa}$

$$\frac{\begin{array}{l} a{:}(\forall\,\Delta.\eta)/R \in \Gamma \\ \Gamma \vdash \overline{\varphi}\,\mathbf{normal} \in \Delta/R \end{array}}{\Gamma \vdash a\,\overline{\varphi}\,\mathbf{normal} \in \eta/R}\ \textsc{NVars}$$

$$\frac{\begin{array}{l} \Gamma \not\vdash \mathbf{match}\,H\,\overline{\varphi} \in \eta/R \\ H{:}\forall\,\Delta.\eta \in \Gamma \\ \Gamma \vdash \overline{\varphi}\,\mathbf{normal} \in \Delta/R \end{array}}{\Gamma \vdash H\,\overline{\varphi}\,\mathbf{normal} \in \eta/R}\ \textsc{NConst}$$

$$\frac{\Gamma, a{:}\kappa \vdash \sigma\,\mathbf{normal} \in \star/R}{\Gamma \vdash \forall a{:}\kappa.\sigma\,\mathbf{normal} \in \star/R}\ \textsc{NAll}$$

$\boxed{\Gamma \vdash \overline{\varphi}\,\mathbf{normal} \in \Delta/R}$

$$\frac{}{\Gamma \vdash \cdot\,\mathbf{normal} \in \cdot/R}\ \textsc{NFSNil}$$

$$\frac{\begin{array}{l} \Gamma \vdash \varphi\,\mathbf{normal} \in \eta/min(R_1,R_2) \\ \Gamma \vdash \overline{\varphi}\,\mathbf{normal} \in \Delta/R_1 \end{array}}{\Gamma \vdash \varphi,\overline{\varphi}\,\mathbf{normal} \in a{:}\eta/R_2, \Delta/R_1}\ \textsc{NFSCons}$$

$\boxed{e \rightsquigarrow e'}$

$$\frac{\begin{array}{c}\Sigma \vdash \gamma : (\sigma_1 \to \upsilon_1) \sim (\sigma_2 \to \upsilon_2) \in \star/\mathsf{T} \\ \gamma_0 = \mathbf{sym}\,(\mathbf{nth}\;0\;\gamma) \quad \gamma_1 = \mathbf{nth}\;1\;\gamma\end{array}}{((\lambda x{:}\sigma_1.e_1) \triangleright \gamma)\; e_2 \rightsquigarrow (\lambda x{:}\sigma_1.(e_1 \triangleright \gamma_1))\;(e_2 \triangleright \gamma_0)}\;\textsc{SSPush}$$

$$\frac{}{(\lambda x{:}\sigma.e_1)\; e_2 \rightsquigarrow e_1[x \mapsto e_2]}\;\textsc{SSBeta}$$

$$\frac{e_1 \rightsquigarrow e_1'}{e_1\; e_2 \rightsquigarrow e_1'\; e_2}\;\textsc{SSEApp}$$

$$\frac{\Sigma \vdash \gamma : \forall a{:}\kappa.\sigma_1 \sim \forall a{:}\kappa.\sigma_2 \in \star/\mathsf{T}}{((\Lambda a{:}\kappa.e) \triangleright \gamma)\;\varphi \rightsquigarrow (\Lambda a{:}\kappa.(e \triangleright \gamma@a))\;\varphi}\;\textsc{SSTPush}$$

$$\frac{}{(\Lambda a{:}\kappa.e)\;\varphi \rightsquigarrow e[a \mapsto \varphi]}\;\textsc{SSTBeta}$$

$$\frac{e_1 \rightsquigarrow e_1'}{e_1\;\varphi \rightsquigarrow e_1'\;\varphi}\;\textsc{SSTApp}$$

$$\frac{\begin{array}{c}\Sigma \vdash \gamma : (\varphi_1 \sim \varphi_2) \Rightarrow \sigma \sim (\varphi_1' \sim \varphi_2') \Rightarrow \sigma' \in \star/\mathsf{T} \\ \gamma_0 = \mathbf{nth}\;0\;\gamma \quad \gamma_1 = \mathbf{sym}\,(\mathbf{nth}\;1\;\gamma) \quad \gamma_2 = \mathbf{nth}\;2\;\gamma\end{array}}{((\Lambda c{:}\varphi_1 \sim \varphi_2.e) \triangleright \gamma)\;\gamma' \rightsquigarrow (\Lambda c{:}\varphi_1 \sim \varphi_2.(e \triangleright \gamma_2))\;(\gamma_0\,;\,\gamma'\,;\,\gamma_1)}\;\textsc{SSCPush}$$

$$\frac{}{(\Lambda c{:}\varphi_1 \sim \varphi_2.e)\;\gamma \rightsquigarrow e[c \mapsto \gamma]}\;\textsc{SSCBeta}$$

$$\frac{e_1 \rightsquigarrow e_1'}{e_1\;\gamma \rightsquigarrow e_1'\;\gamma}\;\textsc{SSCApp}$$

$$\frac{}{(v \triangleright \gamma_1) \triangleright \gamma_2 \rightsquigarrow v \triangleright (\gamma_1\,;\,\gamma_2)}\;\textsc{SSTrans}$$

$$\frac{e \rightsquigarrow e'}{e \triangleright \gamma \rightsquigarrow e' \triangleright \gamma}\;\textsc{SSCoerce}$$

$$\frac{\Sigma \vdash \gamma : T\;\overline{\varphi} \sim T\;\overline{\varphi}' \in \star/\mathsf{T} \quad K{:}\Delta.\sigma' \in \Sigma}{\mathbf{case}_\sigma\;(K\;\overline{\varphi}\;\overline{\rho}) \triangleright \gamma\;\mathbf{of}\;brs \rightsquigarrow \mathbf{case}_\sigma\;K\;\overline{\varphi}'\;(\overline{\rho} \triangleright \sigma'[\Delta \mapsto nth\;\gamma])\;\mathbf{of}\;brs}\;\textsc{SSKPush}$$

$$\frac{1 \le j \le n}{\mathbf{case}_\sigma\;(K_j\;\overline{\varphi}\;\overline{\rho})\;\mathbf{of}\;\overline{K_i \Rightarrow e_i}^{\,i \in 1..n} \rightsquigarrow e_j\;\overline{\rho}}\;\textsc{SSCaseMatch}$$

$$\frac{e \rightsquigarrow e'}{\mathbf{case}_\sigma\;e\;\mathbf{of}\;brs \rightsquigarrow \mathbf{case}_\sigma\;e'\;\mathbf{of}\;brs}\;\textsc{SSCase}$$

B. Additional lemmas and proofs

B.1 Preservation and progress

We state additional basic properties of our judgements below. Proofs of these properties are by straightforward induction.

LEMMA 27 (Type regularity). *If* $\Gamma \vdash e : \sigma$ *then* $\Gamma \vdash \sigma : \star/\mathsf{T}$ *and* $\vdash \Gamma$.

LEMMA 28 (Type Substitution). *Say* $\Gamma_1 \vdash \varphi' : \kappa'$.

1. *If* $\Gamma_1, a{:}\kappa'\,\Gamma_2 \vdash \varphi : \kappa$ *then* $\Gamma_1\,(\Gamma_2[a \mapsto \varphi']) \vdash \varphi[a \mapsto \varphi'] : \kappa$
2. *If* $\Gamma_1, a{:}\kappa'\,\Gamma_2 \vdash \overline{\varphi} : \Delta$ *then* $\Gamma_1\,(\Gamma_2[a \mapsto \varphi']) \vdash \overline{\varphi}[a \mapsto \varphi'] : \Delta$
3. *If* $\Gamma_1, a{:}\kappa'\,\Gamma_2 \vdash \gamma : \varphi_1 \sim \varphi_2 \in \kappa$ *then* $\Gamma_1\,(\Gamma_2[a \mapsto \varphi']) \vdash \gamma[a \mapsto \varphi'] : \varphi_1[a \mapsto \varphi'] \sim \varphi_2[a \mapsto \varphi'] \in \kappa$.
4. *If* $\Gamma_1, a{:}\kappa'\,\Gamma_2 \vdash \overline{\gamma} : \overline{\varphi}_1 \sim \overline{\varphi}_2 \in \Delta$ *then* $\Gamma_1\,(\Gamma_2[a \mapsto \varphi']) \vdash \overline{\gamma}[a \mapsto \varphi'] : \overline{\varphi}_1[a \mapsto \varphi'] \sim \overline{\varphi}_2[a \mapsto \varphi'] \in \Delta$.
5. *If* $\Gamma, a{:}\kappa'\,\Gamma_2 \vdash e : \sigma$ *then* $\Gamma_1\,(\Gamma_2[a \mapsto \varphi']) \vdash e[a \mapsto \varphi'] : \sigma[a \mapsto \varphi']$

LEMMA 29 (Coercion substitution). *Say* $\Gamma_1 \vdash \gamma : \varphi_1 \sim \varphi_2 \in \eta/R$.

1. *If* $\Gamma_1, c{:}\varphi_1 \sim \varphi_2/R\,\Gamma_2 \vdash \gamma' : \psi_1 \sim \psi_2 \in \kappa'$ *then* $\Gamma_1\,\Gamma_2 \vdash \gamma'[c \mapsto \gamma] : \psi_1 \sim \psi_2 \in \kappa'$
2. *If* $\Gamma_1, c{:}\varphi_1 \sim \varphi_2/R\,\Gamma_2 \vdash \overline{\gamma} : \overline{\psi}_1 \sim \overline{\psi}_2 \in \Delta$ *then* $\Gamma_1\,\Gamma_2 \vdash \overline{\gamma}[c \mapsto \gamma] : \overline{\psi}_1 \sim \overline{\psi}_2 \in \Delta$
3. *If* $\Gamma_1, c{:}\varphi_1 \sim \varphi_2/R\,\Gamma_2 \vdash e : \sigma$ *then* $\Gamma_1\,\Gamma_2 \vdash e[c \mapsto \gamma] : \sigma$

LEMMA 30 (Term substitution). *Say* $\Gamma_1 \vdash e' : \sigma'$. *If* $\Gamma_1, x{:}\sigma'\,\Gamma_2 \vdash e : \sigma$, *then* $\Gamma_1\,\Gamma_2 \vdash e[x \mapsto e'] : \sigma$.

LEMMA 31 (Multilifting). *If* $\Gamma\,\Delta \vdash \sigma : \kappa$ *and* $\Gamma \vdash \gamma_i : \varphi_i \sim \varphi_i' \in \kappa_i$ *for each* $a_i{:}\kappa_i$ *in* Δ, *then* $\Gamma \vdash \sigma[\Delta \mapsto \overline{\gamma}] : \sigma[\Delta \mapsto \overline{\varphi}] \sim \sigma[\Delta \mapsto \overline{\varphi}'] \in \kappa$

Next we sketch the proofs of the progress and preservation theorems.
PROOF OF THEOREM 12 (Preservation): If $\Gamma \vdash e_1 : \sigma$ and $e_1 \rightsquigarrow e_2$ then $\Gamma \vdash e_2 : \sigma$.

Proof by induction on $e_1 \rightsquigarrow e_2$.

- Case SSBETA, SSTBETA, SSCBETA: Application of the appropriate substitution lemma.
- Case SSCASEMATCH: By inversion $\Gamma \vdash K_j\,\overline{\varphi}\,\overline{\rho} : T\,\overline{\varphi}$ and $K_j{:}\Delta.\psi_j \in \Gamma$ and $\psi_j[\Delta \mapsto \overline{\varphi}] = \forall\,\Theta_j.\,T\,\overline{\varphi}$ and $\Gamma \vdash e_j : \forall\,\Theta_j.\sigma$. Further inversion gives $\Gamma \vdash \overline{\rho} : \Theta_j$ By repeated use of the application rule, $\Gamma \vdash e_j\,\overline{\rho} : \sigma$.
- Case SSPUSH: By inversion $\sigma = \upsilon_2$ and $\Gamma \vdash \gamma : (\sigma_1 \to \upsilon_1) \sim (\sigma_2 \to \upsilon_2) \in \star/\mathsf{T}$ and $\Gamma \vdash (\lambda x{:}\sigma_1.e_1) : \sigma_1 \to \upsilon_1$ and $\Gamma \vdash e_2 : \sigma_2$. We have $\Gamma \vdash \gamma_0 : \sigma_2 \sim \sigma_1 \in \star/\mathsf{T}$ and $\Gamma \vdash \gamma_1 : \upsilon_1 \sim \upsilon_2 \in \star/\mathsf{T}$. Therefore, $\Gamma \vdash (\lambda x{:}\sigma_1.(e_1 \triangleright \gamma_1)) : \sigma_1 \to \upsilon_2$ and $\Gamma \vdash e_2 \triangleright \gamma_0 : \sigma_1$ and the result follows by the application typing rule.
- Case SSTPUSH: Straightforward use of inversion and typing/coercion rules.
- Case SSCPUSH: By inversion, $\Gamma \vdash \gamma : (\varphi_1 \sim \varphi_2) \Rightarrow \sigma \sim (\varphi_1' \sim \varphi_2') \Rightarrow \sigma' \in \star/\mathsf{T}$ and $\Gamma \vdash \gamma' : \varphi_1' \sim \varphi_2' \in \eta/\mathsf{C}$ and $\Gamma, c{:}\varphi_1 \sim \varphi_2/\mathsf{C} \vdash e : \sigma$. We have $\Gamma \vdash \gamma_0 : \varphi_1 \sim \varphi_1' \in \eta/\mathsf{C}$ and $\Gamma \vdash \gamma_1 : \varphi_2' \sim \varphi_2 \in \eta/\mathsf{C}$ and $\Gamma \vdash \gamma_2 : \sigma \sim \sigma' \in \star/\mathsf{T}$. Therefore $\Gamma \vdash e \triangleright \gamma_2 : \sigma'$ and $\Gamma \vdash \gamma_0\,;\,\gamma'\,;\,\gamma_1 : \varphi_1 \sim \varphi_2 \in \eta/\mathsf{C}$. Finally, the RHS has type σ' by coercion abstraction and application typing rules.
- Case SSKPUSH: By inversion, $\Gamma \vdash \gamma : T\,\overline{\varphi} \sim T\,\overline{\varphi}' \in \star/\mathsf{T}$ and $K{:}\Delta.\sigma' \in \Sigma$ and $\Gamma \vdash K\,\overline{\varphi}\,\overline{\rho} \triangleright \gamma : T\,\overline{\varphi}'$. Further inversion yields $\Gamma \vdash K\,\overline{\varphi}\,\overline{\rho} : T\,\overline{\varphi}$ and $\Gamma \vdash \overline{\rho} : \Theta[\Delta \mapsto \overline{\varphi}]$ where $\sigma' = \forall\Theta.\,T\,\Delta$. Let $\gamma = (\forall\Theta.\,T\,\Delta)[\Delta \mapsto nth\ \gamma]$ By lifting lemma, $\Gamma \vdash \gamma : \forall\,\Theta[\Delta \mapsto \overline{\varphi}].\,T\,\overline{\varphi} \sim \forall\,\Theta[\Delta \mapsto \overline{\varphi}'].\,T\,\overline{\varphi}' \in \star/\mathsf{T}$. Therefore we have by Lemma 11 that $\Gamma \vdash \overline{\rho} \triangleright \gamma : \Theta[\Delta \mapsto \overline{\varphi}']$ and thus $\Gamma \vdash K\,\overline{\varphi}'\,(\overline{\rho} \triangleright \gamma) : T\,\overline{\varphi}'$.
- Case TRANS: Application of CTRANS.
- All other cases by induction.

PROOF OF THEOREM 15 (Progress): If Σ is consistent and $\Sigma \vdash e_1 : \sigma$ and e_1 is not a value v or a coerced value $v \triangleright \gamma$, then there exists an e_2 such that $e_1 \rightsquigarrow e_2$.

Proof by induction on e_1. Assume e_1 is not a value or a coerced value.

- Case $e_1 = e\ e'$. By induction, either e is a value v or a coerced value $v \triangleright \gamma$ or takes a step. In the first case, by canonical forms, v is either an abstraction (which beta reduces) or a constructor application (which means that e_1 is a value). In the second case, we have a coercion γ between a value type τ (the type of v) and $\sigma_1 \to \sigma_2$. By consistency, then τ must be $\sigma_1' \to \sigma_2'$ and the push rule applies. In the last case e_1 steps by the application congruence rule.
- Case $e_1 = e\,\varphi$ and $e_1 = e\,\gamma$ are analogous to the previous case.
- Case $e_1 = e \triangleright \gamma$. By induction, either e is value v or a coerced value $v \triangleright \gamma'$ or takes a step. In the first case, then e_1 is a coerced value. In the second case, $(v \triangleright \gamma') \triangleright \gamma$ steps to $v \triangleright (\gamma'\,;\,\gamma)$. In the last case, the congruence rule for coercion apply.
- Case $e_1 = \mathbf{case}_\sigma\ e\ \mathbf{of}\ brs$. By induction, either e is a value v or a coerced value $v \triangleright \gamma$ or takes a step. In the first case, by canonical forms, v is a a constructor application, so the case expression reduces. In the second case, we have a coercion γ between a value type τ (the type of v) and $T\,\overline{\varphi}$. By consistency, then τ must be $T\,\overline{\varphi}'$ and the push rule applies. In the last case e_1 steps by the case congruence rule.

B.2 Rewriting

LEMMA 32 (Rewriting regularity). *If* $\Gamma \vdash \varphi_1 \rightsquigarrow \varphi_2 \in \kappa$ *then* $\vdash \Gamma$ *and* $\Gamma \vdash \varphi_1 : \kappa$ *and* $\Gamma \vdash \varphi_2 : \kappa$.

Once we get a type constants at the head, it remains.

LEMMA 33 (Constant Rewriting). *If* $\mathbf{Good}\,\Gamma$ *and* $\Gamma \vdash T\,\overline{\varphi} \rightsquigarrow \varphi' \in \eta/R$ *then* $\varphi' = T\,\overline{\varphi}'$ *and* $\Gamma \vdash \overline{\varphi} \rightsquigarrow \overline{\varphi}' \in \Delta/R$.

(Proof is by inspection of the rules of type rewriting.) There is a similar result for types of the form $\forall a{:}\kappa.\sigma$.
We can add types to the end of a list of arguments that reduce.

LEMMA 34 (Snoc). *If* $\Gamma \vdash \overline{\varphi} \rightsquigarrow \overline{\varphi}' \in \Delta/R_1$ *and* $\Gamma \vdash \psi \rightsquigarrow \psi' \in \eta/min(R_1, R_2)$, *then* $\Gamma \vdash \overline{\varphi}, \psi \rightsquigarrow \overline{\varphi}', \psi' \in (\Delta, a{:}\eta/R_2)/R_1$

LEMMA 35 (Single Rewriting Application). *If* $\mathbf{Good}\,\Gamma$ *and* $\Gamma \vdash \varphi_1 \rightsquigarrow \varphi_1' \in (\eta_1/R_1 \to \eta_2)/R_2$ *and* $\Gamma \vdash \varphi_2 \rightsquigarrow \varphi_2' \in \eta_1/min(R_1, R_2)$ *then* $\Gamma \vdash \varphi_1\,\varphi_2 \Leftrightarrow \varphi_1'\,\varphi_2' \in \eta_2/R_2$.

Proof By case analysis of φ_1. The only interesting case is for when φ_1 is of the form $F\,\overline{\varphi}$ which reduces by rule RRED. In this case we have that $\Gamma \vdash F\,\overline{\varphi} \rightsquigarrow F\,\overline{\varphi}' \in (\kappa_1 \to \eta)/R$ given that $\Gamma \vdash \overline{\varphi} \rightsquigarrow \overline{\varphi}' \in \Delta/R$ and $F\,\overline{\varphi}'$ does not match any top-level axiom. In this case we have two cases:

- $F\,\overline{\varphi}'\,\varphi_2'$ matches uniquely some top-level axiom giving υ. In this case, $\varphi_1\,\varphi_2$ is $F\,\overline{\varphi}\,\varphi_2$ and we have that $\Gamma \vdash F\,\overline{\varphi}\,\varphi_2 \rightsquigarrow \upsilon \in \eta/R$. On the other hand, since $F\,\overline{\varphi}'\,\varphi_2'$ matches a top-level axiom, $\overline{\varphi}'$ and φ_2' must be normal forms and hence $\Gamma \vdash \overline{\varphi}' \rightsquigarrow \overline{\varphi}' \in \Delta/R$ and $\Gamma \vdash \varphi_2' \rightsquigarrow \varphi_2' \in \kappa_2$. It follows that $\Gamma \vdash F\,\overline{\varphi}'\,\varphi_2' \rightsquigarrow \upsilon \in \eta/R$ and hence $\Gamma \vdash \varphi_1\,\varphi_2 \Leftrightarrow^1 \varphi_1'\,\varphi_2' \in \eta/R$ as required.
- $F\,\overline{\varphi}'\,\varphi_2'$ does not match any top-level axiom. In this case we are finished by applying the snoc lemma and then rule RCONST.

PROOF OF LEMMA 21: If $\mathbf{Good}\,\Gamma$ and $\Gamma \vdash \varphi_1 \Leftrightarrow \varphi_1' \in (\eta_1/R_1 \to \eta_2)/R_2$ and $\Gamma \vdash \varphi_2 \Leftrightarrow \varphi_2' \in \eta_1/min(R_1, R_2)$ then $\Gamma \vdash \varphi_1\,\varphi_2 \Leftrightarrow \varphi_1'\,\varphi_2' \in \eta_2/R_2$.

Proof Assume the intermediate join points of φ_1 and φ_1' and φ_2 and φ_2', call them σ_1 and σ_2 respectively. Let k be the maximum number of steps for any of these rewritings. Because rewriting is deterministic and total, we can extend the rewritings of all of the others to be k steps to get $\Gamma \vdash \varphi_1 \rightsquigarrow^* \sigma_1' \in (\eta_1/R_1 \to \eta)/R_2$ and $\Gamma \vdash \varphi_1' \rightsquigarrow^* \sigma_1' \in (\eta_1/R_1 \to \eta)/R_2$ and $\Gamma \vdash \varphi_2 \rightsquigarrow^* \sigma_2' \in \eta_2/min(R_1, R_2)$ and $\Gamma \vdash \varphi_2' \rightsquigarrow^* \sigma_2' \in \eta_2/min(R_1, R_2)$.

By the Single Rewriting Application Lemma (and an inner induction on k), it must be that $\Gamma \vdash \varphi_1\,\varphi_2 \Leftrightarrow \sigma_1'\,\sigma_2' \in \eta_2/R_2$. Similarly, it must be that $\Gamma \vdash \varphi_1'\,\varphi_2' \Leftrightarrow \sigma_1'\,\sigma_2' \in \eta_2/R_2$. By transitivity we get finally $\Gamma \vdash \varphi_1\,\varphi_2 \Leftrightarrow \varphi_1'\,\varphi_2' \in \eta_2/R_2$ as required.

COROLLARY 36 (Multi-Application). *If* $\mathbf{Good}\,\Gamma$ *and* $\Gamma \vdash \varphi_1 \Leftrightarrow \varphi_1' \in (\forall\,\Delta.\eta)/R$ *and* $\Gamma \vdash \overline{\varphi}_2 \Leftrightarrow \overline{\varphi}_2' \in \Delta/R$ *then* $\Gamma \vdash \varphi_1\,\overline{\varphi}_2 \Leftrightarrow \varphi_1'\,\overline{\varphi}_2' \in \eta/R$.

LEMMA 37 (StepSubst1). *If* $\mathbf{Good}\,\Gamma$ *and* $\Gamma, a{:}\kappa\,\Delta \vdash \sigma : \eta/R$ *and* $\Gamma \vdash \varphi \rightsquigarrow \varphi' \in \kappa$, *then* $\Gamma \vdash \sigma[a \mapsto \varphi] \Leftrightarrow \sigma[a \mapsto \varphi'] \in \eta/R$.

Proof by induction on σ.
Case $\sigma = F\,\overline{\varphi}$: By induction, we have $\Gamma\,\Delta \vdash \overline{\varphi}[a \mapsto \varphi] \Leftrightarrow \overline{\varphi}[a \mapsto \varphi'] \in \Delta_1/R$. Result holds by lemma (Application).
Case $\sigma = b\,\overline{\varphi}$: By induction, we have $\Gamma\,\Delta \vdash \overline{\varphi}[a \mapsto \varphi] \Leftrightarrow \overline{\varphi}[a \mapsto \varphi'] \in \Delta_1/R$. If b is not a, we are done by lemma (Application). Otherwise, suppose $a = b$: so we want to show that $\Gamma\,\Delta \vdash \varphi\,(\overline{\varphi}[a \mapsto \varphi]) \Leftrightarrow \varphi\,(\overline{\varphi}[a \mapsto \varphi']) \in \kappa$. This also holds by lemma (Application).
Case $\sigma = T\,\overline{\varphi}$: By induction and Application.
Case $\sigma = \forall b{:}\kappa.\sigma'$: Result holds by induction.

LEMMA 38 (StepSubstMany). *If* $\mathbf{Good}\,\Gamma$ *and* $\Gamma, a{:}\kappa\,\Delta \vdash \sigma : \kappa'$ *and* $\Gamma \vdash \varphi \rightsquigarrow^* \varphi' \in \kappa$, *then* $\Gamma \vdash \sigma[a \mapsto \varphi] \Leftrightarrow \sigma[a \mapsto \varphi'] \in \kappa'$.

Proof Proof is by induction on the number of steps in $\Gamma \vdash \varphi \rightsquigarrow^* \varphi' \in \kappa$. If $n = 0$ then the result is trivial. Say $n = m + 1$ and $\Gamma \vdash \varphi \rightsquigarrow \varphi'' \in \kappa$ and $\Gamma \vdash \varphi'' \rightsquigarrow^* \varphi' \in \kappa$ in m steps. By induction, we have $\Gamma \vdash \sigma[a \mapsto \varphi''] \Leftrightarrow \sigma[a \mapsto \varphi'] \in \kappa'$. We just need to show that $\Gamma \vdash \sigma[a \mapsto \varphi] \Leftrightarrow \sigma[a \mapsto \varphi''] \in \kappa'$. However, this result holds by lemma StepSubst1.

LEMMA 39 (StepSubst2). *If* $\mathbf{Good}\,\Gamma$ *and* $\Gamma, a{:}\kappa\,\Delta \vdash \sigma \rightsquigarrow \sigma' \in \kappa'$ *and* $\Gamma \vdash \varphi : \kappa$, *then* $\Gamma\,\Delta \vdash \sigma[a \mapsto \varphi] \Leftrightarrow \sigma[a \mapsto \varphi'] \in \kappa'$.

Proof is by induction on σ, appealing to Application.

PROOF OF LEMMA 22 If $\mathbf{Good}\,\Gamma$ and $\Gamma, a{:}\kappa\,\Delta \vdash \sigma \rightsquigarrow^* \sigma' \in \kappa'$ and $\Gamma \vdash \varphi \rightsquigarrow^* \varphi' \in \kappa$, then there is some $\Gamma\,\Delta \vdash \sigma[a \mapsto \varphi] \Leftrightarrow \sigma'[a \mapsto \varphi'] \in \kappa'$. :

Proof is by induction on the number of steps in $\Gamma, a{:}\kappa\,\Delta \vdash \sigma \rightsquigarrow^* \sigma' \in \kappa'$. If $n = 0$, then the result follows from StepSubstMany. If $n = m + 1$, suppose $\Gamma, a{:}\kappa\,\Delta \vdash \sigma \rightsquigarrow \sigma'' \in \kappa'$ and $\Gamma, a{:}\kappa\,\Delta \vdash \sigma'' \rightsquigarrow^* \sigma' \in \kappa'$ in m steps. By induction, we have $\Gamma\,\Delta \vdash \sigma''[a \mapsto \varphi] \Leftrightarrow \sigma'[a \mapsto \varphi'] \in \kappa'$. We just need to show that $\Gamma \vdash \sigma[a \mapsto \varphi] \Leftrightarrow \sigma''[a \mapsto \varphi] \in \kappa'$. However, this result holds by lemma StepSubst2.

PROOF OF LEMMA 23 If $\mathbf{Good}\,\Gamma$ and $\Gamma \vdash \gamma : \varphi_1 \sim \varphi_2 \in \kappa$ then $\Gamma \vdash \varphi_1 \Leftrightarrow \varphi_2 \in \kappa$. :

Proof is by induction on γ.

- $\gamma = \langle\varphi\rangle$. Trivial as $\varphi_1 = \varphi_2$.
- $\gamma = \gamma_1\,\gamma_2$. Holds by induction and application lemma above.
- $\gamma = \forall a{:}\kappa.\gamma'$. Holds by induction and RALL.
- $\gamma = c\,\overline{\psi}$ where $\kappa = \eta/R$. We have $\varphi_1 = \sigma_1[\Delta \mapsto \overline{\psi}]$ and $\varphi_2 = \upsilon[\Delta \mapsto \overline{\psi}]$. We also must have $\Gamma\,\Delta \vdash \sigma_1 \rightsquigarrow \upsilon \in \eta/R$ (by noting that type variables are normal and instantiating c with variables in Δ.) The desired result holds by the substitution lemmas and transitivity.
- $\gamma = \mathbf{sym}\,\gamma'$ Trivial.
- $\gamma = \gamma_1\,;\,\gamma_2$ Holds by determinacy of rewriting.
- $\gamma = \mathbf{nth}\,k\,\gamma'$ By inversion we have $\Gamma \vdash \gamma' : T\,\overline{\varphi}_1 \sim T\,\overline{\varphi}_2 \in \eta/\mathsf{T}$. We want to show that there is some φ such that, $\Gamma \vdash \mathit{nth}\ k\ \overline{\varphi}_1 \rightsquigarrow^* \varphi \in \mathit{nth}\ k\ \Delta$ and $\Gamma \vdash \mathit{nth}\ k\ \overline{\varphi}_2 \rightsquigarrow^* \varphi \in \mathit{nth}\ k\ \Delta$.
  By induction we have φ, such that $\Gamma \vdash T\,\overline{\varphi}_1 \rightsquigarrow^* \varphi \in \eta/\mathsf{T}$ and $\Gamma \vdash T\,\overline{\varphi}_2 \rightsquigarrow^* \varphi \in \eta/\mathsf{T}$. By Constant Rewriting, we have $\varphi = T\,\overline{\varphi}'$, and $\Gamma \vdash \overline{\varphi}_1 \rightsquigarrow^* \overline{\varphi}' \in \Delta/\mathsf{T}$ and $\Gamma \vdash \overline{\varphi}_2 \rightsquigarrow^* \overline{\varphi}' \in \Delta/\mathsf{T}$. By inversion of these two results, we get the appriate φ.
- $\gamma = \gamma_1@\psi$ By inversion we have $\Gamma \vdash \gamma_1 : \forall a : \kappa.\sigma_1 \sim \forall a : \kappa.\sigma_2 \in \star/\mathsf{T}$ and $\Gamma \vdash \psi : \kappa$. We want to show that there is some φ, such that $\Gamma \vdash \sigma_1[a \mapsto \psi] \rightsquigarrow^* \varphi \in \star/\mathsf{T}$ and $\Gamma \vdash \sigma_2[a \mapsto \psi] \rightsquigarrow^* \varphi \in \star/\mathsf{T}$. By induction, we know that there is some σ and φ', such that $\Gamma \vdash \forall a : \kappa.\sigma_1 \rightsquigarrow^* \forall a : \kappa.\sigma \in \star/\mathsf{T}$ and $\Gamma \vdash \forall a : \kappa.\sigma_2 \rightsquigarrow^* \forall a : \kappa.\sigma \in \star/\mathsf{T}$. The substitution lemma and transitivity gives us the desired result.