

Bryn Mawr College

## Scholarship, Research, and Creative Work at Bryn Mawr College

---

Computer Science Faculty Research and  
Scholarship

Computer Science

---

2015

### An Overabundance of Equality: Implementing Kind Equalities into Haskell

Richard A. Eisenberg

*Bryn Mawr College*, [rae@cs.brynmawr.edu](mailto:rae@cs.brynmawr.edu)

Follow this and additional works at: [https://repository.brynmawr.edu/compsci\\_pubs](https://repository.brynmawr.edu/compsci_pubs)



Part of the [Computer Sciences Commons](#)

[Let us know how access to this document benefits you.](#)

---

#### Citation

R. A. Eisenberg. An Overabundance of Equality: Implementing Kind Equalities into Haskell. University of Pennsylvania Technical Report MS-CIS-15-10, 2015.

This paper is posted at Scholarship, Research, and Creative Work at Bryn Mawr College.  
[https://repository.brynmawr.edu/compsci\\_pubs/14](https://repository.brynmawr.edu/compsci_pubs/14)

For more information, please contact [repository@brynmawr.edu](mailto:repository@brynmawr.edu).

# An overabundance of equality: Implementing kind equalities into Haskell

Richard A. Eisenberg

University of Pennsylvania  
eir@cis.upenn.edu

## Abstract

Haskell, as embodied by version 7.10.1 of the Glasgow Haskell Compiler (GHC), supports reasoning about equality among types, via generalized algebraic datatypes (GADTs) and type families. However, these features are not available among the kinds that classify the types. Motivated by a concrete example of how kind equalities can help programmers today, this paper presents the challenges and solutions encountered in integrating kind equalities into GHC, an industrial-strength compiler. The challenges addressed here all surround the many notions of type equality that exist in GHC today, and in particular around GHC’s role mechanism. These many different relations on types complicate the theory considerably

An update of GHC supporting reasoning about kind equalities is a key part of this work.

## 1. Introduction

Today’s Haskell<sup>1</sup> has an intriguing limitation.

The following declaration, straight from the standard library module *Data.Type.Equality*, defines the type of equality witnesses for two types of any kind  $k$ :

```
data (a :: k) ~: (b :: k) where
  Refl :: ∀ (a :: k). a ~: a
```

Pattern matching on this generalized algebraic datatype (GADT) [10, 19] allows GHC to discover the equality between two types:

```
castWith :: ∀ (a :: *) (b :: *) . (a ~: b) → a → b
castWith Refl x = x
```

In the definition of *castWith*, we pattern-match on *Refl*. This exposes the fact that  $a$  and  $b$  must, in fact, be the same. Then, GHC happily uses  $x$  of type  $a$  in a context expecting something of type  $b$ . All is good.

However, the following, very similar definition, is rejected:

```
data (a :: k1) ≈: (b :: k2) where
  HRefl :: ∀ (a :: k). a ≈: a
```

<sup>1</sup>Throughout this paper, I use “Haskell” to describe the language implemented by the Glasgow Haskell Compiler (GHC) version 7.10.1.

The only difference between  $(\sim:)$  and  $(\approx:)$  is in the kinds of the type arguments. Homogeneous equality  $(\sim:)$  takes two parameters,  $a$  and  $b$ , both of some kind  $k$ . Heterogeneous equality  $(\approx:)$ , on the other hand, takes its parameters of *different* kinds,  $k_1$  and  $k_2$ . Thus, pattern-matching on *HRefl* should yield both that the kinds  $k_1$  and  $k_2$  are equal and that the types  $a$  and  $b$  are equal. Such a definition is useful for enabling Haskell to operate in a distributed, cloud-based setting; see Section 2.1 for the details, as well as other motivation.

The restriction above exists because GHC reasons about only type equality, never kind equality. When a programmer uses *Refl* at type  $a \sim: b$  in an expression, GHC must create a proof that  $a$  indeed equals  $b$ . Conversely, when matching on *Refl*, GHC unpacks this equality proof and is able to use it when type-checking the body of the pattern match – this is how *castWith* is able to type-check, by making use of the proof that  $a$  equals  $b$ . However, GHC currently has no notion of kind equalities, so there is no equivalent proof that  $k_1$  equals  $k_2$  to pack and unpack. Relatedly, today’s Haskell does not support kind families – functions that take and return kinds – nor promoting GADTs to the kind level [20].

The solution to all of these problems is simple to state: merge the concepts of *type* and *kind*. If types and kinds are the same, then we surely have kind equalities. We can go one step further, by adding the  $* :: *$  axiom and avoiding an infinite hierarchy of sorts; see Section 9.1 for discussion about this design choice.

The solution introduced above is described in detail in previous work [18], which develops an enhanced internal language and proves it type safe. The current work goes beyond in that it deals in pragmatics. GHC/Haskell is a large, complex beast: it supports unlifted types (Section 4), roles (Sections 5-6), open and closed type families (Section 7), among many other features. (GHC also requires type inference, which is beyond the scope of this work, but see the work of Gundry [7].)

In this paper, I describe how the internal language from that previous work fits into GHC, resolving the thorny issues that arose in the process. A common thread among these pain points is that they all deal with different notions of type equality. As GHC has evolved, it has required several distinct notions of equality among types, and it is here that the challenge of implementing kind equality comes to a head.

I offer the following contributions:

- Sections 4 through 7 present the primary challenges in extending GHC’s type system with kind equalities, along with their solutions. These challenges appear to arise from the interaction between type system features, and are not merely due to GHC’s implementation particulars.
- In order to overcome those challenges, it has been necessary to augment GHC’s internal language, System FC. Section 3 introduces an updated version of the language, and the relevant

lemmas of the proof of type safety appear in the appendix. As the type safety of Haskell rests on the type safety of FC, maintaining an up-to-date description of FC is critical as Haskell evolves.

- I have made available an implementation of kind equalities in GHC.<sup>2</sup> The implementation is capable of compiling all of the examples in Weirich et al. [18], GHC itself, and the standard libraries, and it fares admirably on the GHC test suite. See also Section 8 for implementation notes. I expect that much of the system described in this paper will be available with the next stable release of GHC.

## 2. Motivation

### 2.1 Cloud Haskell

Cloud Haskell [5] is an ongoing project, aiming to support writing a Haskell program that can operate on several machines in parallel, communicating over a network. Naturally, we would like to do so in a type-safe manner. To do so, we need a way of communicating types over a wire – a runtime type representation. Here is our desired representation:

```
data TyCon (a :: k)
  -- abstract; Int is represented by a TyCon Int
data TypeRep (a :: k) where
  TyCon :: TyCon a → TypeRep a
  TyApp :: TypeRep a → TypeRep b → TypeRep (a b)
```

For every new type declared, the compiler would supply an appropriate value of the *TyCon* datatype. The type representation library would supply also the following function, which computes equality over *TyCons*, returning the heterogeneous equality from the introduction:

```
eqTyCon :: ∀ (a :: k1) (b :: k2).
  TyCon a → TyCon b → Maybe (a ≈: b)
```

It is critical that this function returns  $(\approx:)$ , not  $(\sim:)$ . This is because *TyCons* exist at many different kinds. For example, *Int* is at kind  $\star$ , and *Maybe* is at kind  $\star \rightarrow \star$ . Thus, when comparing two *TyCon* representations for equality, we want to learn whether the types and the kinds are equal. If we used  $(\sim:)$  here, then the *eqTyCon* could be used only when we know, from some other source, that the kinds are equal.

We can now easily write an equality test over these type representations:

```
eqT :: ∀ (a :: k1) (b :: k2).
  TypeRep a → TypeRep b → Maybe (a ≈: b)
eqT (TyCon t1) (TyCon t2) = eqTyCon t1 t2
eqT (TyApp a1 b1) (TyApp a2 b2)
  | Just Refl ← eqT a1 a2
  , Just Refl ← eqT b1 b2      = Just Refl
eqT _ _ = Nothing
```

Now that we have a type representation with computable equality, we can package that representation with a chunk of data, and so form a dynamically typed package:

```
data Dyn where
  Dyn :: ∀ (a ::  $\star$ ). TypeRep a → a → Dyn
```

The *a* type variable there is an *existential* type variable. We can think of this type as being part of the data payload of the *Dyn* constructor; it is chosen at construction time and unpacked

at pattern-match time. Because of the *TypeRep a* argument, we can learn more about *a* after unpacking. (Without the *TypeRep a* or some other type-level information about *a*, the unpacking code must treat *a* as an unknown type and must be parametric in the choice of type for *a*.)

Using *Dyn*, we can pack up arbitrary data along with its type, and push that data across a network. The receiving program can then make use of the data, without needing to subvert Haskell’s type system. The type representation library must be trusted to recreate the *TypeRep* on the far end of the wire, but the equality tests above and other functions below can live outside the trusted code base.

Suppose we were to send an object with a function type, say *Bool*  $\rightarrow$  *Int* over the network. For the time being, let’s ignore the complexities of actually serializing a function – there is a solution to that problem<sup>3</sup>, but here we are concerned only with the types. We would want to apply the received function to some argument. What we want is this:

```
dynApply :: Dyn → Dyn → Maybe Dyn
```

The function *dynApply* applies its first argument to the second, as long as the types line up. The definition of this function is fairly straightforward:

```
dynApply :: Dyn → Dyn → Maybe Dyn
dynApply (Dyn (TyApp
  (TyApp (TyCon tarrow) targ)
  tres)
  fun)
  (Dyn targ' arg)
  | Just Refl ← eqTyCon tarrow (tyCon :: TyCon (→))
  , Just Refl ← eqT targ targ'
  = Just (Dyn tres (fun arg))
dynApply _ _ = Nothing
```

We first match against the expected type structure – the first *Dyn* argument must be a function type. We then confirm that the *TyCon tarrow* is indeed the representation for  $(\rightarrow)$  (the construct *tyCon :: TyCon (→)* retrieves the compiler-generated representation for  $(\rightarrow)$ ) and that the actual argument type matches the expected argument type. If everything is good so far, we succeed, applying the function in *fun arg*.

Heterogeneous equality is necessary throughout this example. It first is necessary in the definition of *eqT*. In the *TyApp* case, we compare *a*<sub>1</sub> to *a*<sub>2</sub>. If we had only homogeneous equality, it would be necessary that the types represented by *a*<sub>1</sub> and *a*<sub>2</sub> be of the same kind. Yet, we can’t know this here! Even if the types represented by *TyApp a*<sub>1</sub> *b*<sub>1</sub> and *TyApp a*<sub>2</sub> *b*<sub>2</sub> have the same kind, it is possible that *a*<sub>1</sub> and *a*<sub>2</sub> would not. (For example, maybe the type represented by *a*<sub>1</sub> has kind  $\star \rightarrow \star$  and the type represented by *a*<sub>2</sub> has kind *Bool*  $\rightarrow \star$ .) With only homogeneous equality, we cannot even write an equality function over this form of type representation. The problem repeats itself in the definition of *dynApply*, when calling *eqTyCon tarrow TArrow*. The call to *eqT* in *dynApply*, on the other hand, *could* be homogeneous, as we would know at that point that the types represented by *targ* and *targ'* are both of kind  $\star$ .

In today’s Haskell, the lack of heterogeneous equality means that *dynApply* must rely critically on *unsafeCoerce*. With heterogeneous equality, we can see that *dynApply* can remain safely outside the trusted code base.

### 2.2 Toward dependent types

A further motivation for adding kind equalities is that this seems a necessary step on our way to having full dependent types. For a concrete example of what dependent types in Haskell might

<sup>2</sup> <https://github.com/goldfirere/ghc>, on the *nokinds* branch. The top-level README.md file has more information.

<sup>3</sup> <https://ghc.haskell.org/trac/ghc/wiki/StaticPointers>

$a, b$	Type variables	$c$	Coercion variables
$D$	<b>data</b> types	$N$	<b>newtypes</b>
$K$	Data constructors	$F$	Type families
$\mathcal{F}$	Type family axioms	$\mathcal{N}$	Newtype axioms

**Figure 1.** Metavariables for System FC

look like, see the work of Gundry [7], which explores the concept thoroughly – including type inference. That work is, in turn, closely based on Weirich et al. [18], from which the current paper has sprung forth. With kind equalities, I conjecture that an arbitrary dependently typed program can be converted to Haskell, in a type-preserving manner, using the singletons construction. Monnier and Haguenaer [9] write a proof that such a translation is possible, and it seems that the version of Haskell proposed in this paper is expressive enough to apply their work.

There is much motivation for dependent types in the folklore. In particular, an interested reader is encouraged to consider Idris [1], a language very similar to Haskell but with dependent types. Despite Idris’s relative youth – dating back only to 2008 – it appears to be gaining a strong following and has generated much buzz, in part owing to its use of dependent types. Despite Idris’s success in this area, it would also be nice to have dependent types in Haskell, as GHC is much more mature, and is considered to be industrial strength. Putting dependent types into Haskell would allow more programmers access to dependent types’ power.

Kind equalities are necessary because dependent types require having term-level constructs available in types. Currently, certain constructor expressions in Haskell are indeed expressible in both terms and types. For example, *Just True* is both a term and a type in Haskell, thanks to GHC’s promotion mechanism [20]. However, only a subset of constructors are promotable – constructors of GADTs, for example, are not. The inability to promote a GADT constructor is directly due to the lack of kind equalities. Just as a term-level GADT constructor wraps up a type equality, a type-level GADT constructor would have to wrap up a kind equality. Accordingly, we need kind equalities to be able to promote GADTs, and take this next step toward dependent types.

For further motivation around kind equalities, the reader is encouraged to see Section 2 of the work of Weirich et al. [18].

### 3. System FC

System FC [12] is GHC’s internal, typed language. It tracks the kind equalities that concern us in this paper. Previous work [2, 18] has a more detailed treatment of System FC than what appears here, but readers are not expected to know more than this introduction to understand the remainder of this paper.

System FC<sup>4</sup> extends System F, adding coercions, type families, and algebraic datatypes. See Figures 1-3 for a primer on the language; I have highlighted the parts that are new to this paper. The treatment of algebraic datatypes in System FC is standard. Coercions are a form unique to FC, written with the metavariable  $\gamma$ , that represent a proof that two types are equal. Coercions are typed by a judgment of the form

$$\Sigma; \Gamma \vdash \gamma : \tau_1 \sim_\rho \tau_2$$

where  $\Sigma$  is a signature containing definitions of type constants and  $\Gamma$  is a typing context containing assumptions. The  $\rho$  subscript to the equality operator  $\sim$  is a role, as explained in Section 5. Figuring

<sup>4</sup>This system has grown over the years and through a number of publications. Some of these extensions have given new names to the system, such as  $F_C^\dagger$  and  $FC_2$ . I refer to the evolving system under one name: FC.

$H$	$::=$ <b>TYPE</b>   $(\rightarrow)$   $'K$   $T$	Type constants
$T$	$::=$ $D$   $N$	Algebraic types
$\epsilon$	$::=$ <b>E</b>   <b>NE</b>	Erasure modalities
$\tau, \sigma, \kappa$	$::=$ $a$   $H$   $\tau \psi$   $\forall \delta. \tau$   $F[\bar{\tau}]$   $\tau \triangleright \gamma$	Types
$\xi$	$::=$ $a$   $H$   $\xi_1 \xi_2$   $\xi c$   $\xi \triangleright c$	Type patterns
$\delta$	$::=$ $a :^c \kappa$   $c : \phi$	Binders
$\psi$	$::=$ $\tau$   $\gamma$	Arguments
$\gamma, \eta$	$::=$ $\langle \tau \rangle$   <b>sym</b> $\gamma$   $\gamma_1 \S \gamma_2$   $\gamma_1 \gamma_2 (m)$   $\gamma_1 (\gamma_2, \gamma_3) \chi$   $\forall_n^c (a_1, a_2, c) \cdot \gamma$   $\forall_\chi (c_1, c_2) \cdot \gamma$   <b>kind</b> $\gamma$   <b>kapp</b> $\gamma$   <b>kapp</b> <sub>1</sub> $\gamma$   <b>kapp</b> <sub>2</sub> $\gamma$   $c$   $\mathcal{F}[i][\psi]$   $\mathcal{N}[\bar{\tau}]$   <b>sub</b> $\gamma$   $\gamma \triangleright \eta$   ...	Coercions
$\phi$	$::=$ $\tau_1 \sim_\rho \tau_2$	Propositions
$\chi$	$::=$ $\langle \eta_1, \eta_2 \rangle_\rho$	Higher-order cos.
$\rho$	$::=$ $N$   $R$	Roles
$\Phi$	$::=$ $[\Delta]. F[\bar{\xi}] \sim_N \sigma$	T.F. equations
$\Psi$	$::=$ $\bar{\Phi}$	T.F. axiom types
$\Sigma$	$::=$ $\emptyset$   $\Sigma, sbnd$	Signatures
$sbnd$	$::=$ $T : \forall \bar{a} : \bar{\rho} \kappa. \star$   $K : \tau$   $F : [\Delta]. \kappa$   $\mathcal{F} : \Psi$   $\mathcal{N} : [\bar{a} : \bar{\kappa}]. N$   $\bar{a} \sim_R^c \sigma$	Sig. bindings
$\Gamma, \Delta$	$::=$ $\emptyset$   $\Gamma, \delta$	Contexts
$t, p$	$::=$ ...	Erased types / args.

The type  $\tau_1 \rightarrow \tau_2$  is syntactic sugar for  $(\rightarrow) \tau_1 \tau_2$ .

**Figure 2.** Grammar for System FC. *TYPE* is discussed in Section 4.3; the erasure modality in Section 4.5; the new coercion forms in Section 6.3.2; erased types and type patterns in Section 7.2; and the new form  $\chi$  in Section 3.1.

$\Sigma \vdash H \Leftarrow \bar{\rho}$	“Roles $\bar{\rho}$ are appropriate for $H$ .”
$\Sigma; \Gamma \vdash \mathbf{ctx}$	Context validity
$\Sigma; \Gamma \vdash \tau : \kappa$	Type kinding
$\Sigma; \Gamma \vdash_{\text{tel}} \bar{\psi} \Leftarrow \Delta$	Telescope validity
$\Sigma; \Gamma \vdash e : \tau$	Expression typing
$\Sigma \vdash \text{no\_conflict}(\Psi, \Phi, \bar{i}, i)$	“Equation $\Phi$ in axiom $\Psi$ at erased types $\bar{i}$ is not prevented from reducing by eqns. numbered $i$ or less.”

**Figure 3.** Typing judgment schemas for System FC

out the right roles in judgment rules is the primary occupation of Sections 5–6; I will often omit these subscripts until then. The metavariable  $\phi$  refers to equality propositions, such as  $\tau_1 \sim_\rho \tau_2$ .

Coercions can be formed in a multitude of ways. Figure 4 contains selected rules from the typing judgment and is included to help the reader understand how coercions combine. We will focus only on the highlighted parts in this paper.

Coercions are used in casts, such as the expression form  $e \triangleright \gamma$ , with the following typing rule:

$$\frac{\Sigma; \Gamma \vdash e : \tau_1 \quad \Sigma; \Gamma \vdash \gamma : \tau_1 \sim \tau_2}{\Sigma; \Gamma \vdash e \triangleright \gamma : \tau_2} \quad \text{TM\_CAST (VER. 1)}$$

We see here that we can take an expression  $e$  of type  $\tau_1$  and treat it as an expression of type  $\tau_2$  by inserting an explicit cast using the cast operator  $\triangleright$ .

Coercions arise from two sources: axioms in the environment and local assumptions. A type family instance compiles to an axiom  $\mathcal{F}$ . For example, the declaration

**type instance**  $F \text{ Int} = \text{Bool}$

yields an axiom  $a\mathcal{F} : F[\text{Int}] \sim_N \text{Bool}$ , which can be made into a coercion proving  $F[\text{Int}] \sim_N \text{Bool}$ . We see here that type families

$\frac{\Sigma; \Gamma \vdash \tau : \kappa}{\Sigma; \Gamma \vdash \langle \tau \rangle : \tau \sim_N \tau} \text{ CO\_REFL}$	$\frac{\Sigma; \Gamma \vdash \gamma : \tau_2 \sim_\rho \tau_1}{\Sigma; \Gamma \vdash \mathbf{sym} \gamma : \tau_1 \sim_\rho \tau_2} \text{ CO\_SYM}$	$\frac{\Sigma; \Gamma \vdash \gamma_1 : \tau_1 \sim_\rho \tau_2 \quad \Sigma; \Gamma \vdash \gamma_2 : \tau_2 \sim_\rho \tau_3}{\Sigma; \Gamma \vdash \gamma_1 \circ \gamma_2 : \tau_1 \sim_\rho \tau_3} \text{ CO\_TRANS}$
$\frac{\Sigma; \Gamma \vdash \gamma_1 : \tau_1 \sim_\rho \tau_2 \quad \Sigma; \Gamma \vdash \gamma_2 : \sigma_1 \sim_N \sigma_2 \quad \Sigma; \Gamma \vdash \sigma_1 : \kappa_1 \quad \Sigma; \Gamma \vdash \sigma_2 : \kappa_2 \quad \Sigma; \Gamma \vdash \eta : \kappa_1 \sim_\rho \kappa_2}{\Sigma; \Gamma \vdash \tau_1 \sigma_1 : \kappa_0 \quad \Sigma; \Gamma \vdash \tau_2 \sigma_2 : \kappa'_0} \text{ CO\_APPPTY}$	$\frac{\Sigma; \Gamma \vdash \eta : \kappa_1 \sim_\rho \kappa_2 \quad \Sigma; \Gamma, a_1 : \kappa_1, a_2 : \kappa_2, c : a_1 \sim_N a_2 \vdash \gamma : \tau_1 \sim_\rho \tau_2 \quad \Sigma; \Gamma \vdash \forall a_1 : \kappa_1. \tau_1 : \sigma_1 \quad \Sigma; \Gamma \vdash \forall a_2 : \kappa_2. \tau_2 : \sigma_2}{\Sigma; \Gamma \vdash \forall_{\eta} (a_1, a_2, c). \gamma : \forall a_1 : \kappa_1. \tau_1 \sim_\rho \forall a_2 : \kappa_2. \tau_2} \text{ CO\_FORALLTY}$	
$\frac{\Sigma; \Gamma \vdash \gamma_0 : \tau_1 \sim_\rho \tau_2 \quad \Sigma; \Gamma \vdash \gamma_1 : \phi_1 \quad \Sigma; \Gamma \vdash \tau_1 \gamma_1 : \kappa'_1 \quad \Sigma; \Gamma \vdash \gamma_2 : \phi_2 \quad \Sigma; \Gamma \vdash \tau_2 \gamma_2 : \kappa'_2 \quad \Sigma; \Gamma \vdash \chi : \phi_1 \sim_\rho \phi_2}{\Sigma; \Gamma \vdash \gamma_0 (\gamma_1, \gamma_2)_\chi : \tau_1 \gamma_1 \sim_\rho \tau_2 \gamma_2} \text{ CO\_APPCO}$	$\frac{\Sigma; \Gamma \vdash \chi : \phi_1 \sim_\rho \phi_2 \quad \Sigma; \Gamma, c_1 : \phi_1, c_2 : \phi_2 \vdash \gamma : \tau_1 \sim_\rho \tau_2 \quad \Sigma; \Gamma \vdash \forall c_1 : \phi_1. \tau_1 : \sigma_1 \quad \Sigma; \Gamma \vdash \forall c_2 : \phi_2. \tau_2 : \sigma_2}{\Sigma; \Gamma \vdash \forall_\chi (c_1, c_2). \gamma : \forall c_1 : \phi_1. \tau_1 \sim_\rho \forall c_2 : \phi_2. \tau_2} \text{ CO\_FORALLCO}$	
$\frac{\Sigma; \Gamma \vdash \gamma : \tau_1 \sim_\rho \tau_2 \quad \Sigma; \Gamma \vdash \tau_1 \triangleright \eta : \kappa'_1}{\Sigma; \Gamma \vdash \gamma \triangleright \eta : (\tau_1 \triangleright \eta) \sim_\rho \tau_2} \text{ CO\_COHERENCE}$	$\frac{\Sigma; \Gamma \vdash \gamma : \tau_1 \sigma_1 \sim_N \tau_2 \sigma_2 \quad \Sigma; \Gamma \vdash \sigma_1 : \kappa_1 \quad \Sigma; \Gamma \vdash \sigma_2 : \kappa_2}{\Sigma; \Gamma \vdash \mathbf{kapp} \gamma : \kappa_1 \sim_N \kappa_2} \text{ CO\_KAPPTY}$	
$\frac{\Sigma; \Gamma \vdash \gamma : \tau_1 \gamma_1 \sim_N \tau_2 \gamma_2 \quad \Sigma; \Gamma \vdash \gamma_1 : \sigma_1 \sim_\rho \sigma_2 \quad \Sigma; \Gamma \vdash \gamma_2 : \sigma_3 \sim_\rho \sigma_4}{\Sigma; \Gamma \vdash \mathbf{kapp}_1 \gamma : \sigma_1 \sim_N \sigma_3} \text{ CO\_KAPPCO1}$	$\frac{\Sigma; \Gamma \vdash \gamma : \tau_1 \gamma_1 \sim_N \tau_2 \gamma_2 \quad \Sigma; \Gamma \vdash \gamma_1 : \sigma_1 \sim_\rho \sigma_2 \quad \Sigma; \Gamma \vdash \gamma_2 : \sigma_3 \sim_\rho \sigma_4}{\Sigma; \Gamma \vdash \mathbf{kapp}_2 \gamma : \sigma_2 \sim_N \sigma_4} \text{ CO\_KAPPCO2}$	
$\frac{c : \phi \in \Gamma \quad \Sigma; \Gamma \vdash \mathbf{ctx}}{\Sigma; \Gamma \vdash c : \phi} \text{ CO\_VAR}$	$\frac{\Sigma; \Gamma \vdash \gamma : \tau_1 \sim_\rho \tau_2 \quad \Sigma; \Gamma \vdash \tau_1 : \kappa_1 \quad \Sigma; \Gamma \vdash \tau_2 : \kappa_2}{\Sigma; \Gamma \vdash \mathbf{kind} \gamma : \kappa_1 \sim_R \kappa_2} \text{ CO\_KIND}$	$\frac{\Sigma; \Gamma \vdash \gamma : \tau_1 \sim_N \tau_2}{\Sigma; \Gamma \vdash \mathbf{sub} \gamma : \tau_1 \sim_R \tau_2} \text{ CO\_SUB}$
$\frac{F : \Psi \in \Sigma \quad \Psi[i] = [\Delta]. F[\bar{\xi}] \sim_N \sigma \quad F : [\Delta_2]. \kappa' \in \Sigma \quad \Sigma; \Gamma \vdash_{\text{tel}} \bar{\psi} \Leftarrow \Delta \quad \text{erase}_{\Sigma; \Gamma}(\bar{\xi}[\bar{\psi}/\Delta]) \rightsquigarrow \bar{t} \quad \Sigma; \Gamma \vdash \kappa'[\bar{\xi}[\bar{\psi}/\Delta]/\Delta_2] : \star \quad \Sigma \vdash \text{no\_conflict}(\Psi, \Psi[i], \bar{t}, i)}{\Sigma; \Gamma \vdash F[i][\bar{\psi}] : F[\bar{\xi}][\bar{\psi}/\Delta] \sim_N \sigma[\bar{\psi}/\Delta]} \text{ CO\_TFAXIOM}$	$\frac{\mathcal{N} : [\bar{a}; \bar{\kappa}]. N \bar{a} \sim_R^{\kappa_0} \sigma \in \Sigma \quad \Sigma; \Gamma \vdash_{\text{tel}} \bar{\tau} \Leftarrow \bar{a}; \bar{\kappa} \quad \Sigma; \Gamma \vdash \kappa_0[\bar{\tau}/\bar{a}] : \star}{\Sigma; \Gamma \vdash \mathcal{N}[\bar{\tau}] : N \bar{\tau} \sim_R \sigma[\bar{\tau}/\bar{a}]} \text{ CO\_NTAXIOM}$	
$\Sigma; \Gamma \vdash \chi : \phi_1 \sim_\rho \phi_2 \quad \text{Higher-order coercion typing}$	$\Sigma; \Gamma \vdash \phi \text{ ok} \quad \text{Proposition validity}$	
$\frac{\Sigma; \Gamma \vdash \eta_1 : \sigma_1 \sim_\rho \sigma_3 \quad \Sigma; \Gamma \vdash \eta_2 : \sigma_2 \sim_\rho \sigma_4 \quad \phi_1 = \sigma_1 \sim_{\rho_2} \sigma_2 \quad \phi_2 = \sigma_3 \sim_{\rho_2} \sigma_4}{\Sigma; \Gamma \vdash \langle \eta_1, \eta_2 \rangle_{\rho_2} : \phi_1 \sim_\rho \phi_2} \text{ HCO\_PAIR}$	$\frac{\Sigma; \Gamma \vdash \tau_1 : \kappa_1 \quad \Sigma; \Gamma \vdash \tau_2 : \kappa_2}{\Sigma; \Gamma \vdash \tau_1 \sim_\rho \tau_2 \text{ ok}} \text{ PROP\_EQUALITY}$	

**Figure 4.** Selected rules of coercion formation:  $\Sigma; \Gamma \vdash \gamma : \phi$ , along with auxiliary judgments

in System FC are presented with a first-order syntax  $F[\dots]$ ; this is because type families must always appear saturated, both in Haskell and in FC.

Newtypes also compile to axioms  $\mathcal{N}$ . The declaration

**newtype** *Age* = *MkAge Int*

compiles to  $\mathbf{axAge} : \mathbf{Age} \sim_R \mathbf{Int}$ . The *MkAge* constructor does not appear in FC, as it is replaced by a cast using the axiom *axAge*. We see here that an important difference between type family axiom and newtype axioms is their roles: type family axioms have nominal roles, whereas newtype axioms have representational roles. See Section 5 for the details.

The use of GADTs lead to coercion assumptions. Consider the type *G*:

**data** *G a where*  
*MkGBool* :: *G Bool*

The *MkGBool* :: *G Bool* constructor is elaborated to have type  $\mathbf{MkGBool} :: \forall a. a \sim \mathbf{Bool} \Rightarrow \mathbf{G} a$ . This transformation is critical when analyzing **case** expressions, where we need the result types of all constructors to be uniform in the datatype parameters. (In other words, the result type of a constructor must be the datatype name followed by a correctly sized list of unrepeated type variables, such as *G a*.) The type  $\forall a. a \sim \mathbf{Bool} \Rightarrow \mathbf{G} a$  is understood to mean that *MkGBool* takes one parameter when elaborated in System FC – a coercion between type *a* and *Bool*. Then, when unpacking the constructor in a pattern match, this coercion is available within the body of the pattern match. For example, consider this function:

$match :: \forall a. G a \rightarrow a$   
 $match MkGBool = True$

The function *match* elaborates as follows:

$match :: \forall a. G a \rightarrow a$   
 $match = \Lambda(a :: \star) \rightarrow \lambda(x :: G a) \rightarrow \mathbf{case} \ x \ \mathbf{of}$   
 $MkGBool \ (c :: a \sim Bool) \rightarrow True \triangleright \mathbf{sym} \ c$

The cast is necessary because *match* must return a result of type *a*; the *sym* operator we see there reverses the order of the coercion *c*, proving that  $Bool \sim a$ , as desired.

### 3.1 Adding kind equalities

In Weirich et al. [18], my co-authors and I extended this ability of casts to include casting on types, using the following rule:

$$\frac{\Sigma; \Gamma \vdash \tau : \kappa_1 \quad \Sigma; \Gamma \vdash \gamma : \kappa_1 \sim \kappa_2}{\Sigma; \Gamma \vdash \tau \triangleright \gamma : \kappa_2} \quad \text{TY\_CAST (VER. I)}$$

This rule behaves identically to the term-level rule, but one level up. It is this ability to use an equality to change the kind of a type that forms the essential difference between the System FC with kind equalities and other versions of the language.

There are several knock-on effects of adding kind equalities, summarized here:

- Promoting a GADT constructor leads to a type constant, written  $\prime K$ , that takes a coercion argument. Accordingly, System FC allows type application to either types  $\tau \sigma$  or coercions  $\tau \gamma$ . This ability is more succinctly expressed in terms of  $\psi$ , which stands for either a type or a coercion. Thus, the application form looks like  $\tau \psi$ .
- In two places in the grammar (seen in rules CO\_APPCO and CO\_FORALLCO) it is necessary to prove an equality between two propositions. I call this a *higher-order coercion*, and write it  $\chi$ . A higher-order coercion, composed of two ordinary coercions, is a proof that the corresponding parts of two propositions are equal. See Figure 4 for the typing rule.

During compilation, GHC takes a source Haskell program and performs type inference on it, producing an annotated version of the source program. At this stage, any programmer errors should be caught and reported. In an error-free program, GHC then elaborates the annotated source program to a System FC program. The elaborated program is then optionally type checked. A type error in the System FC program would indicate a bug in the GHC implementation, as all user errors should have already been detected and reported. This redundancy is why type checking System FC is optional. However, having a typed internal language has proved to be a great asset to the GHC implementation, revealing a plenitude of bugs during development. System FC is also amenable to formal reasoning, allowing GHC/Haskell to rest on a solid type-theoretical framework.

### 3.2 Heterogeneous equality

System FC with kind equalities also directly supports *heterogeneous* equality, which relates type of (potentially) different kinds. To see how this arises, consider the *Proxy* type:

**data** *Proxy* ( $a :: k$ ) = *P*

The type *Proxy* has kind  $\forall k. k \rightarrow \star$ . Now, consider that we have some assumption  $c :: (k_0 \sim \star)$ ; that is, *c* is a proof that some kind  $k_0$  is equal to  $\star$ . Reflexive coercions can be built out of any type; the coercion  $\langle Proxy \rangle$  proves  $Proxy \sim Proxy$ . We can then build the coercion  $\langle Proxy \rangle c$ , proving  $Proxy \ k_0 \sim Proxy \ \star$ . But, we

can also see that  $Proxy \ k_0 :: k_0 \rightarrow \star$  and  $Proxy \ \star :: \star \rightarrow \star$ . Thus,  $\langle Proxy \rangle c$  is a heterogeneous coercion.

We thus allow coercions to relate types of different kinds. In the judgment for well-formed propositions  $\phi$  (Figure 4), we see that the two types related may have different kinds.

Alongside heterogeneous equality, we would also like to say that casts are irrelevant in types, a property termed *coherence*. We want to be able to prove that, for any  $\tau$  and  $\gamma$ :  $(\tau \triangleright \gamma) \sim \tau$ . For example, you should be able use a Haskell term of type  $Int \triangleright \langle \star \rangle$  where one of type *Int* is expected. This proof is embodied by a coherence coercion form, such as this rule from Weirich et al. [18]:

$$\frac{\Sigma; \Gamma \vdash \gamma : \tau_1 \sim \tau_2 \quad \Sigma; \Gamma \vdash \tau_1 \triangleright \gamma' : \kappa_1}{\Sigma; \Gamma \vdash \gamma \triangleright \gamma' : (\tau_1 \triangleright \gamma') \sim \tau_2} \quad \text{CO\_COHERENCENOROLE}$$

Although this rule is asymmetric, it can be used with the rule for symmetry (*sym*) to get coercions on either side of the  $(\sim)$ .

### 3.3 Metatheory

The metatheory of System FC is well explored in the literature [2, 4, 12, 18]. In the appendix, I update several of the lemmas to work with this new system. The two key lemmas needed to prove type safety are *lifting* (for preservation) and *consistency* (for progress).

The lifting lemma says that types are preserved when a cast stands in the way of a pattern match. It is significantly complicated by kind equalities, as explored in Weirich et al. [18]. In this work, it is updated with roles.

The consistency lemma says, essentially, that there is no coercion (in an empty context) proving  $Int \sim Bool$ . This is a key part of proving progress.

**Theorem** (Preservation). *Assume for all  $H \in \text{dom}(\Sigma)$ ,  $\Sigma \vdash H \Leftarrow \bar{p}$ . If  $\Sigma; \Gamma \vdash e : \tau$  and  $\Sigma \vdash e \rightarrow e'$ , then  $\Sigma; \Gamma \vdash e' : \tau$ .*

In System FC, a value is a lambda-abstraction or an expression headed by a constructor.

**Theorem** (Progress). *Assume for all  $H \in \text{dom}(\Sigma)$ ,  $\Sigma \vdash H \Leftarrow \bar{p}$ . If  $\Sigma; \Gamma \vdash e : \tau$ , then either  $\Sigma \vdash e \rightarrow e'$  for some  $e'$ ,  $e$  is a value, or  $e$  is a casted value.*

The full definition of this version of System FC, with the statement and proofs of the key lemmas, appears in the appendix.

## 4. Unlifted types and eliminating sub-kinding

### 4.1 Lifted types vs. unlifted types

Haskell, a non-strict language, differentiates between *lifted* types and *unlifted* types. A lifted type is one that contains *undefined* – the canonical  $\perp$  term in Haskell – and an unlifted type does not. As a consequence, evaluating expressions of unlifted types is always strict.

Inhabitants of lifted types may be *thunks* – unevaluated portions of a program. It is thus absolutely necessary for inhabitants of lifted types to be stored via pointers. The runtime system can distinguish between thunks and evaluated data before following the pointer. Inhabitants of unlifted types, however, can be represented without any indirection. Because we know an unlifted type is always strict, we can manipulate it directly. Haskell library-writers take advantage of this fact by using unlifted types in performance-critical code.

The difference in representation between lifted and unlifted types implies another distinguishing characteristic: it is not possible to abstract over unlifted types. For example, the value  $3\#$  is of type  $Int\#$ , yet writing  $id \ 3\#$  (where  $id :: \forall a. a \rightarrow a$  is the polymorphic identity) is erroneous. Upon reflection, we see that this code must

be wrong:<sup>5</sup> what machine code could be generated for *id*? All lifted types are represented by pointers, so it is straightforward to have an implementation for *id* that works on any lifted type. Yet, unlifted types can have any size and layout in memory; the machine code for one function cannot deal with this variety.

Haskell uses its type system to prevent constructions like *id 3#* by putting unlifted types into their own kind. The kind  $\star$  classifies lifted types (such as *Int*, *Bool*, and *Maybe Double*). The kind  $\#$  classifies unlifted types (such as *Int#*, *Word32#*, and *Array# Float#*). Accordingly, the full type of *id* should be written  $\forall (a :: \star). a \rightarrow a$ . When I say *id 3#*, I get a kind error:

```
Kind incompatibility when matching types :
  a      ::  $\star$ 
  Int#   ::  $\#$ 
```

## 4.2 Sub-kinding

Despite the separation between  $\star$  and  $\#$ , the following code type-checks:

```
quux :: Bool  $\rightarrow$  Int#
quux _ = undefined
```

This correct code begs the questions: What is the kind of  $(\rightarrow)$ ? And what is the type of *undefined*? Both  $(\rightarrow)$  and *undefined* are used above in conjunction with unlifted types, seemingly successfully.

The answer to these questions is that today's GHC has a sub-kinding feature.<sup>6</sup> When used fully applied, the  $(\rightarrow)$  type has the kind *OpenKind*  $\rightarrow$  *OpenKind*  $\rightarrow \star$ , where  $\#$  and  $\star$  are sub-kinds of *OpenKind*. Similarly, the type of *undefined* is properly  $\forall (a :: \text{OpenKind}). a$ . The type *Bool*  $\rightarrow$  *Int#* is thus well-kinded, according to the sub-kinding relationship; and using *undefined* at type *Int#* is also well-kinded. *OpenKind* also appears during type inference when checking a lambda-term. As we're checking  $\lambda x \rightarrow \dots$ , we don't yet know whether *x*'s type will be unlifted or lifted; GHC uses a unification variable of kind *OpenKind* to pull this off.

This use of sub-kinding has worked moderately well, but it does present a few oddities:

- A student of type systems can learn about the  $\star$  and  $\#$  kinds, and then be quite perplexed that *undefined* works at type *Int#*. This question comes up with some regularity on the Haskell mailing lists.<sup>7</sup>
- The function *error* ::  $\forall (a :: \text{OpenKind}). \text{String} \rightarrow a$  works similarly to *undefined*, but prints a user-specified error message when evaluated. It is sometimes convenient to define a function such as *flooError s = error ("Module Floo: " ++ s)*. Yet, user definitions cannot tap into the sub-kinding magic, and so *flooError* would be restricted to types of kind  $\star$ , making it less useful than *error*.
- From an implementation standpoint, the presence of sub-kinds complicates various parts of type inference, and has always seemed to be a less-than-ideal solution.

As we examine adding kind equalities, sub-kinding becomes even more of a thorn. For example, if we have an proof that  $k \sim \star$  (for some *k*), then what is *k*'s relationship to *OpenKind*? What is

<sup>5</sup> I am discounting the possibility of specializing *id* to concrete unlifted types here by duplicating its code, which GHC does not currently do.

<sup>6</sup> In personal communication, Simon Peyton Jones has said sub-kinding is not a feature, but a gross hack.

<sup>7</sup> For example: <https://www.haskell.org/pipermail/ghc-devs/2015-February/008222.html>

the proof for that relationship? Perhaps there is a story to be told here, but it would be complex.

## 4.3 Eliminating sub-kinds via levity polymorphism

Instead, merging types with kinds facilitates getting rid of sub-kinds altogether. The idea behind the new approach is to replace sub-kinding with polymorphism, over a type variable of the new kind *Levity*:

```
data Levity = Lifted | Unlifted
```

We then say that  $\star$  is just a synonym for *TYPE* 'Lifted and  $\#$  is a synonym for *TYPE* 'Unlifted, where *TYPE* is a new primitive constant in the type system. All the uses of sub-kinding now are easily expressed using polymorphism:

```
undefined ::  $\forall (v :: \text{Levity}) (a :: \text{TYPE } v). a$ 
error      ::  $\forall (v :: \text{Levity}) (a :: \text{TYPE } v). \text{String} \rightarrow a$ 
( $\rightarrow$ )   ::  $\forall (v_1 :: \text{Levity}) (v_2 :: \text{Levity}).$ 
               $\text{TYPE } v_1 \rightarrow \text{TYPE } v_2 \rightarrow \star$ 
```

As we can see, *TYPE* has type *Levity*  $\rightarrow$  *TYPE* 'Lifted, recalling that *TYPE* 'Lifted – that is,  $\star$  – is the classification of all kinds. This strange typing relationship (where a constant is mentioned in its own type) can be accommodated by a custom typing rule, much like that for  $(\rightarrow)$ . It presents no trouble in the formalization or proof.

## 4.4 Disallowing naughty levity polymorphism

I argue above that the following is nonsense:

```
id' ::  $\forall (v :: \text{Levity}) (a :: \text{TYPE } v). a \rightarrow a$ 
id' x = x
```

This *id'* is a function that takes a levity-polymorphic variable. It is thus not possible to generate concrete code for *id'*, as there is no way to know how *id'* expects to receive its argument. Will it be passed via a pointer or not? How big is the data? These questions are impossible to answer for a levity-polymorphic argument. Let's call this a *naughty* use of levity polymorphism. Of course, not all uses of levity polymorphism are naughty: *undefined*'s use of levity polymorphism is not naughty at all.

We can discern between these cases with a simple rule: *No binder may have a levity-polymorphic type*. This rule easily rules out *id'*, as the body of *id'* would have to abstract over  $x :: a$  where  $a :: \text{TYPE } v$ . Here, *a* is a levity-polymorphic type, and is thus disallowed as the type of a binder. Because *case* expressions also bind variables, this rule also effectively (and rightly) rules out levity-polymorphic arguments to data constructors.

## 4.5 Type polymorphism

Let's look again at the type of *undefined*:

```
undefined ::  $\forall (v :: \text{Levity}) (a :: \text{TYPE } v). a$ 
```

What, exactly, is the kind of that type? Is it even well-kinded? According to the traditional kinding rule for  $\forall$ -types, it isn't well-kinded at all:

$$\frac{\Sigma; \Gamma, a: \kappa \vdash \tau : \star}{\Sigma; \Gamma \vdash \forall a: \kappa. \tau : \star} \text{TY\_FORALLTY (VER. 1)}$$

The type variable *a* has kind *TYPE* *v*, where *v* might not be 'Lifted', and thus the traditional kinding rule fails. Clearly, we need to be able to abstract over both lifted and unlifted types. We thus use this rule:

$$\frac{\Sigma; \Gamma, a: \kappa \vdash \tau : \text{TYPE } \sigma}{\Sigma; \Gamma \vdash \forall a: \kappa. \tau : \text{TYPE } \sigma} \text{TY\_FORALLTY\_E}$$

(Ignore the E notations for now.) This rule allows the body of the  $\forall$  to have either a lifted type or an unlifted type and checks to make sure that levity type  $\sigma$  does not escape its scope. The conclusion might be somewhat surprising though, in that the kind of the abstraction is the same as the kind of the body. The motivation for this decision is that the difference between  $\star$  and  $\#$  is in the code generator and at runtime. We certainly don't want types – which get erased – to have an impact at runtime. A type abstraction over an unlifted type should surely remain unlifted.

Sadly, rule `TY_FORALLTY_E` excludes the type of *undefined*! The solution proposed here is to add a new rule to handle exactly this case:

$$\frac{\Sigma; \Gamma, a: \kappa \vdash \tau : \text{TYPE } \sigma}{\Sigma; \Gamma \vdash \forall a: \text{NE } \kappa. \tau : \star} \quad \text{TY\_FORALLTY\_NE}$$

This rule concludes that the final kind is  $\star$ , not  $\text{TYPE } \sigma$ . The difference between the two rules – what keeps them from overlapping – is the *erasure modality*, E (erased) or NE (not erased).<sup>8</sup> If we tweak the type of *undefined* to use non-erasing quantification and become  $\forall (v :: \text{NE } \text{Levity}) (a :: \text{TYPE } v). a$ , then it is well-kinded at kind  $\star$ . (When a colon is unlabeled, we assume it is erasing.) The intent is to use non-erasing quantification *only* for levity variables.<sup>9</sup>

Naturally, there is a runtime consequence of this design. Because levity abstraction always results in a type of kind  $\star$ , a levity-polymorphic value must be lifted, and thus represented by a pointer at runtime. In practice, this pointer will lead to a function that consumes (and simply discards) a runtime value of type *Levity*. There is thus a clear runtime effect of the design decision stated here. But this does not cause any trouble in practice: any non-naughty use of levity polymorphism is sure to diverge or throw an exception. This design simply means it will take a computer a few more cycles following the indirection before the program aborts – it can't cause a slowdown in a loop.

#### 4.6 Levity polymorphism in type inference

One of the signs that levity polymorphism is a good approach is how well it works with the existing type inference scheme. When GHC must reason about an as-yet-unknown type, it invents *unification variables*, written  $\alpha$  or  $\beta$ . When GHC learns, say, that  $\alpha$  should be *Int*, it just does an in-place mutable update of  $\alpha := \text{Int}$ .

Suppose GHC is inferring the type of  $x$  in the expression  $\lambda x \rightarrow \text{swizzle } x$ , where  $\text{swizzle} :: \text{Int} \rightarrow \text{Bool}$ . When type-checking the pattern  $x$ , GHC will invent a levity unification variable  $\alpha :: \text{Levity}$  and a type unification variable  $\beta :: \text{TYPE } \alpha$ , where  $x :: \beta$ . In the course of normal type inference, GHC will discover that  $\beta$  must be the type that *swizzle* expects, *Int*. Before setting  $\beta := \text{Int}$ , however, GHC does a kind check. (This kind check exists in today's Haskell, too.) It ensures that the type of  $\beta$ ,  $\text{TYPE } \alpha$ , matches the type of *Int*, which is  $\text{TYPE } \text{'Lifted}$ . In so doing, GHC discovers that it should set  $\alpha := \text{'Lifted}$ . Naturally, GHC does *another* kind check, but that straightforwardly confirms that the type of  $\alpha$  is the same as the type of  $\text{'Lifted}$ : they are both *Levity*. Thus, GHC sets  $\alpha := \text{'Lifted}$  and then  $\beta := \text{Int}$ . What is encouraging about all of this is that *nothing* in this part of the type inference algorithm had to change to support levity polymorphism.

#### 4.7 Discussion

Using levity polymorphism to eliminate sub-kinding is a clear win for GHC, in both theory and practice. While the  $\text{TYPE}$  constant is

<sup>8</sup> As this modality is written on the binding colon, a careful reader may expect erasure modality notations to appear in typing contexts as well. As the erasure modality plays no role in a typing context, these are omitted.

<sup>9</sup> In the extension of this language to include proper  $\Pi$ -types, the erasure modality will play a larger role, becoming closer to the phase modality of Gundry [7].

perhaps more complex than  $\star$  or  $\#$ , avoiding sub-kinding simplifies the type system by removing this extra relation among types. Implementing the feature also removed several checks to make sure the sub-kinding relation was being respected. This seems like a solid way to deal with a type system that admits multiple kinds of inhabited types, like  $\star$  and  $\#$ . Furthermore, eliminating sub-kinding is essentially forced by adding kind equalities, due to the necessity of interaction between the features.

However, levity polymorphism would not, on its own, be implementable in today's GHC without some pain. The problem is that levity variables appear in kinds. Today's GHC maintains an invariant that all variables that appear in kinds have type  $\square$ , the sort of kinds. Indeed, decisions based on a variable's kind happen quite often, as today's GHC treats kind variables somewhat differently than type variables. (For example, type variables are printed in error messages; kind variables are not.) This is not an easy limitation to work around. While I conjecture that the engineering challenges could be overcome with effort, integrating levity polymorphism fits more naturally in a system with a fully-merged grammar of types and kinds.

## 5. Roles on kind equalities

A critical step in the integration of kind equalities into GHC is figuring out a way to combine roles [2, 17] with kind equalities. It turns out that this combination leads to subtle interactions and forces some hard design choices.

### 5.1 An introduction to roles

Haskell supports the **newtype** construct, which allows the programmer to declare that one type shares a representation with another:

```
newtype Age = MkAge Int
```

This declaration says that the runtime representation of *Age* is identical to that of *Int*, although these types remain distinct to the type checker. This construct is a boon to programmers, because they can use **newtypes** to enforce abstraction in their code without paying a runtime penalty.

The usefulness of **newtypes** has led Haskellers to demand the ability to lift the free conversions through types. That is, we would want to be able to convert *Maybe [Age]* to *Maybe [Int]* with no runtime penalty. We will soon discover, however, that this is not safe with *all* types. For example, consider these declarations:

```
type family F a where
  F Int = Bool
  F Age = Double
data X a = MkX (F a)
```

We clearly cannot convert an  $X \text{ Int}$  to an  $X \text{ Age}$  – the former stores a *Bool* and the latter a *Double*! How can we tell the difference between safe coercions, based on types like  $[]$  and *Maybe*, and unsafe ones, based on types like  $X$ ?

To see the difference between *Maybe* and  $X$ , we must consider the two different notions of equality in play. We want safe coercions allowed between types that have the same representation at runtime. Yet, a type family can distinguish among such types, as we see above. *Age* and *Int* are equal in one sense, and distinct in another. We must carefully track these two equality relations to get this right.

To allow these free coercions safely, Weirich et al. [17] proposed distinguishing the two equality relations at work here. Breitner et al. [2] expanded upon that work and simplified it so that it was suitable for implementation.



## 5.2 Nominal and representational equality

The two equality relations at work are  $(\sim_N)$ , called nominal equality; and  $(\sim_R)$ , called representational equality. Nominal equality is what Haskell programmers think of as type equality. Nominal equality includes the reduction of type functions, such that  $F \text{ Int} \sim_N \text{ Bool}$ . Representational equality, on the other hand, is strictly coarser, relating also newtypes and their representations. Thus,  $\text{Age} \sim_R \text{ Int}$  while  $\text{Age} \not\sim_N \text{ Int}$ . Breitner et al. [2] introduced the new function<sup>10</sup>  $\text{coerce} :: a \sim_R b \Rightarrow a \rightarrow b$ , which allows programmers to freely convert one type to a representationally equal type.

In System FC, discerning between the two equality relations is done using an extra annotation on the  $\sim$  operator that forms equality propositions. Thus, the typing judgment for coercions is

$$\Sigma; \Gamma \vdash \gamma : \tau_1 \sim_\rho \tau_2$$

where  $\rho$  is a metavariable for roles;  $\rho$  may concretely become N or R.<sup>11</sup> Accordingly, every coercion proves either a nominal equality proposition or a representational one. The coercion former **sub** converts a nominal equality proof to a representational one. That is to say:

$$\frac{\Sigma; \Gamma \vdash \gamma : \tau_1 \sim_N \tau_2}{\Sigma; \Gamma \vdash \text{sub } \gamma : \tau_1 \sim_R \tau_2} \text{ CO\_SUB}$$

We must now return and refine the typing rule for casting expressions, first encountered in Section 3. In order to support casting from *Age* to *Int*, we see that the cast operator must work with representational equality. We thus get this typing rule:

$$\frac{\begin{array}{l} \Sigma; \Gamma \vdash e : \tau_1 \\ \Sigma; \Gamma \vdash \gamma : \tau_1 \sim_R \tau_2 \\ \Sigma; \Gamma \vdash \tau_2 : \text{TYPE } \sigma \end{array}}{\Sigma; \Gamma \vdash e \triangleright \gamma : \tau_2} \text{ TM\_CAST}$$

The differences from the previous version is the addition of the R subscript to the equality proposition proved by  $\gamma$ , and that we explicitly require the result type to be a valid target type of a cast.

With representational equality in hand, there is now a straightforward way to encode newtypes: every newtype declaration gives rise to an axiom for representational equality. For example, the declaration of *Age* in the introduction leads to the axiom  $\text{axAge}$  proving  $\text{Age} \sim_R \text{ Int}$ .

The addition of roles, unfortunately, complicates GHC’s type system considerably, both internally, and in ways visible to programmers. This is a regrettable consequence of allowing both a way to convert among representationally equal types while having type-system features that can discern among representationally equal types.

## 5.3 The role of kind coercions

Let’s now add roles to kind coercions. The first problem to tackle is how to update the TY\_CAST rule, introduced in Section 3. Should that equality proposition be nominal or representational? I have chosen that it should be representational, yielding the following rule:

$$\frac{\begin{array}{l} \Sigma; \Gamma \vdash \tau : \kappa_1 \\ \Sigma; \Gamma \vdash \gamma : \kappa_1 \sim_R \kappa_2 \end{array}}{\Sigma; \Gamma \vdash \tau \triangleright \gamma : \kappa_2} \text{ TY\_CAST}$$

This decision is not without consequences. Arguments in favor of each of the choices are below.

**Casting by nominal coercions is much simpler.** The only reason we have representational equality at all is to glean runtime benefits

<sup>10</sup> The operator  $(\sim_R)$  is actually spelled *Coercible* in GHC programs.

<sup>11</sup> Here, and throughout most of this paper, I ignore the possibility of *phantom* coercions, as introduced in Breitner et al. [2].

of having free conversions between newtypes and their representation types. Absent performance concerns, there would be little benefit of the representational equality relation. Yet, when reasoning about types, a performance argument falls flat – there is no need to make “free” conversions among types, as these conversions are never run at all. It would thus seem unnecessary to have representational equalities among kinds. Under this idea, a **newtype** declaration would be treated just as a **data** declaration would be when promoting data constructors to types. Even though the **newtype** constructor used at the term level is absent from a System FC program, that same constructor would be preserved when used at the type level.

Furthermore, casting types by nominal coercions avoids the thorny issues we explore below, caused by the choice of using representational equality in kind casts. The nominal equality choice would then lead to a significantly simpler system.

### **Casting by representational coercions is much more expressive.**

The chief argument in favor of casting by representational equalities is uniformity, echoing the decision to cast by representational equalities in terms. The work of integrating kind equalities into GHC is a key step along the way to dependent types, with a  $\Pi$ -quantifier, in Haskell. (See Section 2.2 for some more motivation.) As discussed in Gundry [7], having proper dependent types requires identifying a subset of the expression language that can also appear in types.

At a minimum, all datatypes and newtypes should be in this subset. Because newtype constructors elaborate to representational coercions, in order to freely promote expressions using newtypes, representational coercions must be allowed to cast the kinds of types.<sup>12</sup>

Using representational coercions in kind casts also opens the door to future expansions of the representational equality concept. One way to view representational equality is that it is a type equality that is never inferred – it must always be annotated. The programmer does this by writing a newtype constructor, or by calling *coerce*. One can imagine more ways to let types equal one another, requiring that the programmer specifies when to make the conversion. For example, GHC’s *Constraint* kind classifies (lifted) constraint types. As such, it is appropriately seen as indistinguishable from  $\star$  in today’s System FC. However, *Constraint* and  $\star$  are *different* kinds to a Haskell programmer. This situation – when two kinds are distinct in a Haskell program but should be seen as the same under the hood – is exactly the situation with newtypes. Perhaps a future application of the ability to use representational coercions in kind casts is to let *Constraint* and  $\star$  be representationally equal. This ability could be used to allow Haskell programs to convert regular values into dictionaries and back, a trick that currently requires *unsafeCoerce*.<sup>13</sup>

In the end, I decided to use representational coercions in kind casts, chiefly in order to support future dependent types work.

## 6. Extracting kind coercions from type coercions

Suppose we have  $\gamma : \tau_1 \sim_\rho \tau_2$ , where  $\tau_1 : \kappa_1$  and  $\tau_2 : \kappa_2$ . By definition, this means that  $\gamma$  shows that  $\tau_1$  and  $\tau_2$  are equal at role  $\rho$ . But, what does it say about  $\kappa_1$  and  $\kappa_2$ ? The system described in

<sup>12</sup> Promoted **newtypes** can be used in today’s Haskell by considering a **newtype** constructor akin to a **data** constructor. Such a treatment would fail, however, if GHC had to automatically promote certain expressions, which is necessary if it is to support  $\Pi$ -types. Today’s promotion is done entirely by hand in the source Haskell program – GHC never converts a term-level expression into a type.

<sup>13</sup> For example, see Edward Kmett’s reflection package, which makes use of this trick.

Weirich et al. [18] has the following rule:

$$\frac{\Sigma; \Gamma \vdash \gamma : \tau_1 \sim \tau_2 \quad \Sigma; \Gamma \vdash \tau_1 : \kappa_1 \quad \Sigma; \Gamma \vdash \tau_2 : \kappa_2}{\Sigma; \Gamma \vdash \mathbf{kind} \gamma : \kappa_1 \sim \kappa_2} \text{CO\_KINDNORoles}$$

We must now decide how to decorate this rule with roles. My decision, based on experience working with and implementing this system, is to have the conclusion have a representational role, regardless of the premise’s role:

$$\frac{\Sigma; \Gamma \vdash \gamma : \tau_1 \sim_{\rho} \tau_2 \quad \Sigma; \Gamma \vdash \tau_1 : \kappa_1 \quad \Sigma; \Gamma \vdash \tau_2 : \kappa_2}{\Sigma; \Gamma \vdash \mathbf{kind} \gamma : \kappa_1 \sim_{\mathbf{R}} \kappa_2} \text{CO\_KIND}$$

There appears to be, here, a free choice among several options. Though I have worked out the details only for the system with the rule immediately above, I conjecture that a similar system would support having the conclusion’s role match the premise’s role, and yet a different system would support removing this rule entirely. I consider these different options below.

### 6.1 Alternative: a nominal type equality implies a nominal kind equality

Here, we consider an alternate to CO\_KIND above:

$$\frac{\Sigma; \Gamma \vdash \gamma : \tau_1 \sim_{\rho} \tau_2 \quad \Sigma; \Gamma \vdash \tau_1 : \kappa_1 \quad \Sigma; \Gamma \vdash \tau_2 : \kappa_2}{\Sigma; \Gamma \vdash \mathbf{kind} \gamma : \kappa_1 \sim_{\rho} \kappa_2} \text{CO\_KINDALT}$$

At first blush, this seems like the right option. If we know that two types are nominally equal – that is, the two types are considered wholly interchangeable in source Haskell – we would expect their kinds to have the same property. However, this choice, along with the choice to use representational coercions in casts, leads to a fundamentally fragile type inference algorithm.

The central problem is that, with CO\_KINDALT, nominal equality is *not* coherent. Recall that coherence is the property that, for all  $\tau$  and  $\gamma$ ,  $\tau$  should be equal to  $\tau \triangleright \gamma$ . If a type equality relation is coherent, then the exact placement of casts in types is irrelevant. Yet, with CO\_KINDALT, the type  $\tau \triangleright \gamma$  might not be nominally equal to  $\tau$  – the kinds of  $\tau \triangleright \gamma$  and  $\tau$  might be only *representationally* equal, not nominally equal. If we could somehow derive a nominal equality between  $\tau$  and  $\tau \triangleright \gamma$  for any  $\tau$  and  $\gamma$ , we could promote a representational equality proof to a nominal one, thoroughly defeating the whole roles mechanism.

Can we live without coherence? No. Lack of coherence means that the placement of coercions in types is now relevant. Because the placement of coercions in types is determined during type inference – and often influenced by tiny changes in a user’s Haskell source – incoherence inevitably leads to a fragile type inference algorithm. Another way of viewing the problem is to consider a Haskell program as a compressed form of a System FC program; type inference and elaboration expands the compressed form. Without coherence, this expansion is non-deterministic: multiple, unequal FC types may be the expansion of one Haskell type. We thus must reject the CO\_KINDALT rule.

### 6.2 Alternative: a nominal type equality implies nothing about the types’ kinds

Though the details have not been worked out, my co-authors and I conjecture in Weirich et al. [18] that the  $\mathbf{kind} \gamma$  coercion form is optional – it can be left out without ill effect. I see no reason that this fact would be changed in the system with roles. So, we must consider this possibility.

In the GHC implementation, the ability to extract a kind coercion from a type coercion is useful. This comes into play most often when it is necessary to form a *homogeneous* coercion. A key

example is the implementation of type normalization. Given a type, possibly containing type family applications, we would like to produce a type without any reducible type family applications and the coercion that witnesses the reduction. Concretely, if we have **type instance**  $F \text{ Int} = \text{Bool}$ , given  $F \text{ Int}$ , we want to produce  $\text{Bool}$  and  $\gamma : F \text{ Int} \sim_{\mathbf{N}} \text{Bool}$ . The coercion produced must be homogeneous, as only homogeneous equality is substitutive – that is, we must be able to replace the normalized type in for the original. Thus, during normalization, if  $\tau_1 : \kappa_1$  normalizes to  $\tau_2 : \kappa_2$  with  $\gamma : \tau_1 \sim_{\mathbf{N}} \tau_2$ , we can use  $\tau_2 \triangleright \mathbf{sym}(\mathbf{kind} \gamma) : \kappa_1$  to substitute for  $\tau_1$ .

Despite the convenience of using  $\mathbf{kind}$  here, I believe it is strictly unnecessary. It seems quite possible to track changes of a type’s kind during normalization (and other, similar algorithms in GHC) and then to homogenize using a separately-formed kind coercion. However, I have also been unable to find a simplification made possible by the omission of  $\mathbf{kind}$ , so it seems better to have  $\mathbf{kind}$  than not.

### 6.3 Final decision: a nominal type equality implies a representational kind equality

I have thus adopted the following rule for kind extraction and coherence:

$$\frac{\Sigma; \Gamma \vdash \gamma : \tau_1 \sim_{\rho} \tau_2 \quad \Sigma; \Gamma \vdash \tau_1 : \kappa_1 \quad \Sigma; \Gamma \vdash \tau_2 : \kappa_2}{\Sigma; \Gamma \vdash \mathbf{kind} \gamma : \kappa_1 \sim_{\mathbf{R}} \kappa_2} \text{CO\_KIND}$$

This choice of rule leads to a straightforward addition of roles to the coherence rule:

$$\frac{\Sigma; \Gamma \vdash \gamma : \tau_1 \sim_{\rho} \tau_2 \quad \Sigma; \Gamma \vdash \tau_1 \triangleright \eta : \kappa'_1}{\Sigma; \Gamma \vdash \gamma \triangleright \eta : (\tau_1 \triangleright \eta) \sim_{\rho} \tau_2} \text{CO\_COHERENCE}$$

Regardless of the role of  $\gamma$ ,  $\mathbf{kind} \gamma$  is always a representational equality. This choice is not without its drawbacks, which I explore below. However, these drawbacks have, in practice, been more easily overcome than the drawbacks of other alternatives.

#### 6.3.1 Nominal equality is more inclusive than it “should” be.

Suppose  $\gamma : \text{Int} \sim_{\mathbf{R}} \text{Age}$ , built from  $\text{Age}$ ’s newtype axiom. Then, the coercion  $\langle 3 \rangle \triangleright \gamma$  proves  $(3 \triangleright \gamma) \sim_{\mathbf{N}} 3$ , a nominal equality. The fact that this proposition is provable is puzzling, because it involves a newtype axiom. Recall that nominal equality is source Haskell equality – it is intended that type inference can, without assistance, discover any nominal equality that can exist between two types. Yet, the whole point of newtypes is that type inference should not equate a newtype and its underlying representation, unless directed to do so by the programmer. Thus, our  $\langle 3 \rangle \triangleright \gamma$  coercion is suspect.

However, we can note a key fact here: the *kinds* of  $3 \triangleright \gamma$  and  $3$  are different; the coercion  $\langle 3 \rangle \triangleright \gamma$  is heterogeneous. Thus, for a Haskell programmer to notice the fact that  $3 \triangleright \gamma$  and  $3$  are nominally equal, there must be two nominally equal types, one of which expects a parameter of kind  $\text{Age}$  and the other of which expects a parameter of kind  $\text{Int}$ . This does not happen, and so we are saved. Understanding how this is so is best by way of a few examples.

Consider a basic *Proxy* type, with an explicit kind parameter:<sup>14</sup>

```
data Proxy (k :: *) (a :: k) = P
```

Both parameters  $k$  and  $a$  will be inferred to have representational roles. This means that we can prove  $\text{Proxy } k_1 \ a_1$  is representationally equal to  $\text{Proxy } k_2 \ a_2$  whenever  $k_1 \sim_{\mathbf{R}} k_2$  and  $a_1 \sim_{\mathbf{R}} a_2$ .

<sup>14</sup>This syntax – with explicit kinds – is actually legal in my implementation, as a natural consequence of combining types with kinds.

**Are Proxy Age (MkAge 3) and Proxy Int 3 representationally equal?** Yes, as they should be. We can straightforwardly prove that  $\text{Age} \sim_R \text{Int}$  and use coherence to show that  $3 \triangleright \gamma$  (which is the desugared form of  $\text{MkAge } 3$ ) is representationally equal to 3.

**Are Proxy Age (MkAge 3) and Proxy Int 3 nominally equal?** No, because  $\text{Age}$  and  $\text{Int}$  are not nominally equal. The coherence rule allows us to prove that  $3 \triangleright \gamma$  and 3 are nominally equal, but the overall types are still not nominally equal.

There is still a small lingering problem here. Even in today’s Haskell, users can write *role annotations* which alter the default roles GHC infers for types [2]. For example, a programmer might write the following annotation for *Proxy*:

```
type role Proxy representational nominal
```

This annotation means that, to prove that  $\text{Proxy } k_1 a_1$  and  $\text{Proxy } k_2 a_2$  are representationally equal,  $k_1$  can be representationally equal to  $k_2$ , but  $a_1$  and  $a_2$  are required to be nominally equal. With this annotation in place, we can *still* prove that  $\text{Proxy Age (MkAge 3)}$  is representationally equal to  $\text{Proxy Int 3}$ . This fact is slightly dissatisfying, because it means that GHC will “look through” the  $\text{MkAge}$  constructor. This fact may surprise some programmers, but the issue can come up only when a user has used a role annotation, and the problem does not threaten type safety. Furthermore,  $\text{Age}$  and  $\text{Int}$  are considered representationally equal only when the  $\text{MkAge}$  constructor is in scope, so the problem described here does not result in a loss of abstraction.

### 6.3.2 Type applications are hard to decompose.

Consider a type inference problem where we must prove the equality  $\beta_1 \beta_2 \sim_N \text{Proxy } \star \text{Int}$ , where  $\beta_1 :: \alpha \rightarrow \star$  and  $\beta_2 :: \alpha$ , and Greek letters denote unification variables. The decomposition seems straightforward; we should reduce to  $\beta_1 \sim_N \text{Proxy } \star$  and  $\beta_2 \sim_N \text{Int}$ . We cannot quite set  $\beta_1 := \text{Proxy } \star$  and  $\beta_2 := \text{Int}$ , because the kinds do not match up. Before we can proceed, we must prove  $(\alpha \rightarrow \star) \sim_R (\star \rightarrow \star)$  and  $\alpha \sim_R \star$ . However, we see here that the kind equalities are representational, not nominal; this is a direct consequence of our choice of roles on  $\text{kind } \gamma$ . After the constraint solver is done,  $\alpha$  will still be left ambiguous, as a representational equality does not fix the value of a unification variable. Indeed, this ambiguity is correct here, as it is conceivable that the choice of  $\alpha$  could have runtime significance through the selection of different class instances. (Consider, say, a **newtype**  $\text{Star} = \text{MkStar } \star$ , establishing a representational equality between  $\text{Star}$  and  $\star$ . Then,  $\text{Star}$  and  $\star$  could have different instances for a certain class.)

We might imagine tweaking type inference to produce nominal kind equalities here, but this would amount to “guessing” – making an unforced commitment during inference, something GHC studiously avoids in order to retain predictable type inference. Furthermore, when trying to decompose an *assumption* of type equality, (a Given constraint in the terminology of the work of Vytiniotis et al. [15]) we would be unable to produce a nominal kind equality in this scenario.

This issue is not merely a theoretical concern, either. This scenario came up when compiling the *Control.Arrow* module of GHC’s standard library. Without the fix described shortly, that module failed to compile due to an ambiguous kind variable.

My solution to this problem is to add a new way of extracting a kind coercion from a type coercion, described by this rule:

$$\frac{\begin{array}{l} \Sigma; \Gamma \vdash \gamma : \tau_1 \sigma_1 \sim_N \tau_2 \sigma_2 \\ \Sigma; \Gamma \vdash \sigma_1 : \kappa_1 \\ \Sigma; \Gamma \vdash \sigma_2 : \kappa_2 \end{array}}{\Sigma; \Gamma \vdash \mathbf{kapp} \gamma : \kappa_1 \sim_N \kappa_2} \text{CO\_KAPPTY}$$

Using **kapp**, we can extract a nominal coercion relating the kinds of the arguments of a type application. Of course, simply adding this one rule would violate type safety – we must also add an extra requirement to the coercion form that relates type applications:

$$\frac{\begin{array}{l} \Sigma; \Gamma \vdash \gamma_1 : \tau_1 \sim_\rho \tau_2 \\ \Sigma; \Gamma \vdash \gamma_2 : \sigma_1 \sim_N \sigma_2 \\ \Sigma; \Gamma \vdash \sigma_1 : \kappa_1 \quad \Sigma; \Gamma \vdash \sigma_2 : \kappa_2 \\ \Sigma; \Gamma \vdash \eta : \kappa_1 \sim_\rho \kappa_2 \\ \Sigma; \Gamma \vdash \tau_1 \sigma_1 : \kappa_0 \quad \Sigma; \Gamma \vdash \tau_2 \sigma_2 : \kappa'_0 \end{array}}{\Sigma; \Gamma \vdash \gamma_1 \gamma_2(\eta) : \tau_1 \sigma_1 \sim_\rho \tau_2 \sigma_2} \text{CO\_APPPTY}$$

We see that to prove a nominal equality between  $\tau_1 \sigma_1$  and  $\tau_2 \sigma_2$ , we must not only show that  $\tau_1$  and  $\sigma_1$  are nominally equal to  $\tau_2$  and  $\sigma_2$ , respectively, but also that  $\kappa_1$  equals  $\kappa_2$ . With this extra requirement on the application coercion form, rule  $\text{CO\_KAPPTY}$  becomes admissible, and therefore sound. See Appendix C for the full details.

Having addressed the two shortcomings of choosing a representational role for  $\text{kind } \gamma$ , I believe that this choice is the best and is the one implemented.

## 7. Maintaining sound type families

### 7.1 Overlap checking today

An open type family [3] in Haskell defines a function on types that can be extended. For example, we can write the following:

```
type family F (a :: *) :: *
type instance F Int = Char -- instance (1)
```

Then, perhaps in another module, we can add a new equation, thus:

```
type instance F Bool = Double -- instance (2)
```

With both **type instance** declarations in scope, GHC will reduce the type  $F \text{Int}$  to  $\text{Char}$  and  $F \text{Bool}$  to  $\text{Double}$ .

When adding equations to an open type family, it is necessary to make sure that the new equation does not overlap with the old one. For example, we cannot add the following instance to those above:

```
type instance F a = String -- instance (3)
```

This instance overlaps with both previous instances. If it were allowed, then type families would behave differently in different places, allowing a user to subvert the type system.

We thus need some way of eliminating the possibility of overlap. Because type family instances elaborate to axioms in System FC, our check must somehow ensure that the left-hand sides of the equations will never be nominally equal, even after arbitrary (well-typed) substitutions. In the case of the last type instance above, the substitution  $a \mapsto \text{Bool}$  would make the left-hand side overlap with the instance (2) above.

Our task is greatly simplified by the fact that type family equations cannot have type family applications on their left-hand side, much like how term-level patterns may not call functions. In today’s Haskell, the overlap check is a simple, syntactic unification algorithm. If the left-hand sides fail to unify, then they must not overlap.

A similar check is needed in the reduction of closed type families. Consider the following:

```
type family G a where
  G Int = Bool
  G a = Char
```

The equations in a closed type family are meant to be understood top-to-bottom. The definition for  $G$  means that  $G \text{Int}$  reduces to  $\text{Bool}$ , and  $G a$  reduces to  $\text{Char}$ , as long as  $a$  is *apart* from  $\text{Int}$ .

By apart here, I mean that the argument to  $G$  must never become  $Int$ . For example, we cannot reduce  $G (F a)$ , because we don't (yet) know whether  $F a$  is  $Int$  or not. The details of how apartness interacts with closed type family reduction are written out in full in previous work [4].

## 7.2 Type families with kind equalities

There are two aspects of the current system that cause trouble here: coercions can appear in types, and coercions can be abstracted over. The first problem is easily dispatched with. Simply erase coercions before checking for overlap and apartness. You can see this design choice in the coercion formation rules, Figure 4, which erases types before doing the closed-type-family apartness check, in rule `CO_TFAXIOM`.

The second problem – coercion abstraction – can be seen in an example:

```

type family G (a ::  $\star$ ) ::  $\star$ 
type instance G ( $\forall (c :: Int \sim Bool). Bool$ ) = Char
type instance G ( $\forall (c :: Bool \sim Int). Int$ ) = Double

```

Those two left-hand sides do not unify, yet they can be proved nominally equal. We must reject these instance declarations.

Happily, the solution here is already existent in GHC: forbid quantified types in patterns. The part that comes with kind equalities is that we must *also* forbid this construction in System FC – hence the restricted grammar for type patterns  $\xi$  that we see in Figure 2.<sup>15</sup>

In today's Haskell (and in my implementation), quantified types are somewhat limited in source Haskell – Haskell remains predicative. Although inference with impredicativity has been tried in GHC [14], most of that functionality has been removed, as it had too many corner cases and induced too much confusing behavior.

System FC, on the other hand, has always been fully impredicative. It has been possible, then, to allow axioms to work with quantified types. With kind equalities, though, we must forbid this construction. Eliminating quantified types on the left-hand side of type family axioms is enough to establish the key *consistency* lemma, the most intricate part of the proof of the progress theorem. The statement and proof appear in Appendix C.

## 8. Implementation notes

**A simpler equality to implement** Implementing a system such as the one described here is – for lack of a better word – fiddly. The problem is that the implementation works with yet a different equality relation than the ones discussed here: syntactic equality. GHC's function `eqType` checks if two types are equal only up to  $\alpha$ -equivalence.

What's challenging about syntactic equality is that it distinguishes between, say,  $Int$  and  $Int \triangleright \langle \star \rangle$ , and between  $\tau$ ,  $\tau \triangleright \gamma \triangleright \mathbf{sym} \gamma$ , and  $\tau \triangleright (\gamma \circ \mathbf{sym} \gamma)$ . A key property of System FC – proof irrelevance – “fails” with syntactic equality, because the actual structure of proofs matters there.

These difficulties can be overcome, of course, with very careful management of casts, and many uses of coherence coercions. Yet, during implementation, the rigidity of syntactic equality was a constant source of bugs and engineering challenge.

The struggle to deal with syntactic equality led to a key insight: use a more relaxed equality internally. We thus want to replace syntactic equality with a new definitional equality. A first candidate for this new definitional equality is *erased equality* – when checking two types for equality, remove all casts and coercions first and then

<sup>15</sup>Type patterns are also restricted in that all coercions must be bare coercion variables  $c$ . This is to allow the coercion to have any concrete form when instantiating.

check. However, simple erased equality does not work, as it might relate types of different kinds; we need the definitional equality to be substitutive, so a heterogeneous equality just won't do.

Instead, the right answer for definitional equality appears to be erased equality, plus an additional kind check. Of course, the kinds are to be checked with the same choice of definitional equality. We avoid infinite regress by the fact that all kinds have type  $\star$ . (That is, it can be proved that if  $\Sigma; \Gamma \vdash \tau : \kappa$ , then  $\Sigma; \Gamma \vdash \kappa : \star$ .) This decision works very well in practice, and this redesign allowed me to remove over 1,000 lines of code with no apparent change in functionality.

**Testsuite results** As of the time of writing, the implementation passes 3,762 of the 3,887 tests in the GHC testsuite, failing 125 tests. Notably, not a single test exhibits a program where my implementation accepts a program that should be rejected. The vast majority of the failures are due to changes in error messages; future work will include improving these. Another large source of errors is the lack of support for kind equalities in pattern synonyms or in the GHCi debugger; these features have yet to be integrated with my work.

**Pay-as-you-go complexity** The critical decision discussed in Section 5 is for casts in types to have representational roles, as a parallel to casts in terms. Despite the possibility of using representational equality among kinds to have a cleaner relationship between *Constraint* and  $\star$  (see Section 5.3), the primary motivation for this design decision is to prepare for proper dependent types down the road.

The next release of GHC will not, however, have proper dependent types. It therefore seems imprudent to have representational roles in kind casts until the addition of proper  $\Pi$ -types. Although the system as described in this paper is implemented, the representational roles in kind coercions will be removed as my implementation is merged into the main development stream of GHC. Nevertheless, my collaborators and I are unaware of a better solution of how to integrate roles with dependent types, and I will return representational roles in kind coercions in my branch as I work on adding proper  $\Pi$ -types.

## 9. Discussion

### 9.1 The $\star :: \star$ axiom and partial correctness

The language I present in this paper sports the  $\star :: \star$  axiom. This is in sharp contrast to more traditional dependently typed programming languages, such as Coq, Agda, and Idris, all of which have an infinite hierarchy of universes. In this infinite hierarchy, a standard type  $Int$  would have type  $Type$ , which in turn has type  $Type_1$ , which has  $Type_2$ , and so on. It has been established that the  $\star :: \star$  axiom causes a system to be inconsistent as a logic [6] and can allow authors to write non-terminating type-level programs.

However, these flaws do not concern us in Haskell. Adding dependent-type features to Haskell is *not* an attempt to make GHC a proof assistant. All types are already inhabited, by *undefined* at the term level, and by the open **type family** `Any (k ::  $\star$ ) :: k` at the type level. If having  $\star :: \star$  allows us another way to inhabit a type, it does not change the properties of the language. Due to its inconsistency as a logic, the best a Haskell programmer can hope for is *partial* correctness: if a Haskell program is ascribed to have a certain type, then it is known to have that type only if the program evaluates to a value in finite time. This guarantee has proved to be sufficient to Haskellers, who continue to use advanced type-level features despite the lack of total correctness.

There is intriguing related work, however, toward a Haskell termination checker [13] and pattern-match totality checker [8]. With these tools in place, it may be possible to provide even stronger

compile-time guarantees to programmers. An additional exciting application is this related work is that it would allow GHC to optimize away certain parts of a program that exist only to prove type equality. Currently, all term-level equality proofs must be executed at runtime; otherwise, we can't be sure that the equality is sound. If we could prove totality, though, running the proofs becomes unnecessary. More work needs to be done to make this a reality, but this is all an exciting direction to look to in the future.

## 9.2 Other related work

The previous paper describing the system implemented here [18] contains a thorough review of related work. The reader is encouraged to look there to see how System FC relates to the literature.

## 9.3 Future work

There is much work left to do. Here are some starting points:

- The implementation discussed here necessarily does type inference to produce a well-typed System FC program from a source Haskell text. Although GHC's type inference algorithm did not require extensive modifications to make this work, the process of analyzing types is somewhat more involved than it was previously. Future work on type inference includes an in-depth analysis and explanation of the new algorithm.
- GHC supports *deferred type errors* [16], which allow a user to successfully compile a type-incorrect program. If the program then executes type-incorrect code, the running program halts with an error. With the kind equalities implemented here, it is possible to extend this idea to deferred kind errors. The details have yet to be worked out, however.
- With kind equalities in GHC, we are much closer to being able to implement a proper dependent quantifier into Haskell, along the lines of Gundry [7]. Working out the details and implementing is important future work along this line of research.

## 9.4 Conclusion

The fundamental tension that causes the incorporation of kind equalities into GHC to be challenging is that there are many notions of equality (and equality-like relations, such as sub-kinding) in the compiler. In particular, there seems to be tension between performance and abstraction; it is the interaction between these two desiderata that gave birth to **newtypes** and, later, roles, in Haskell.

The solutions proposed in this work vary in elegance. In my opinion, levity polymorphism seems like a nice solution to a slightly thorny problem. On the other hand, the lack of a clean fit between roles and kind equalities is dissatisfying, as is the incompleteness of the power of type family matching. Yet, the solutions put forth here are adequately expressive, and provably implementable. With kind equalities in hand, users can start to adopt yet richer types and continue to push the limits of practical, strongly typed programming.

## Acknowledgments

Thanks to Stephanie Weirich, Simon Peyton Jones, and Dimitrios Vytiniotis for their collaboration – particularly about levity polymorphism. This paper is typeset with the help of `lhs2TeX`<sup>16</sup> and `ott` [11]. This work is supported by a Microsoft Research Graduate Student Fellowship and by the National Science Foundation under Grant No. 1116620.

<sup>16</sup><http://www.andres-loeh.de/lhs2tex/>

## References

- [1] Edwin Brady. Idris, a general-purpose dependently typed programming language: Design and implementation. *J. Funct. Prog.*, 23, 2013.
- [2] Joachim Breitner, Richard A. Eisenberg, Simon Peyton Jones, and Stephanie Weirich. Safe zero-cost coercions for Haskell. In *International Conference on Functional Programming*, ICFP '14. ACM, 2014.
- [3] Manuel M. T. Chakravarty, Gabriele Keller, and Simon Peyton Jones. Associated type synonyms. In *International Conference on Functional Programming*, ICFP '05. ACM, 2005.
- [4] Richard A. Eisenberg, Dimitrios Vytiniotis, Simon Peyton Jones, and Stephanie Weirich. Closed type families with overlapping equations. In *Principles of Programming Languages*, POPL '14. ACM, 2014.
- [5] Jeff Epstein, Andrew P. Black, and Simon Peyton Jones. Towards haskell in the cloud. In *Haskell Symposium*. ACM, 2011.
- [6] J.-Y. Girard. *Interprétation fonctionnelle et élimination des coupures de l'arithmétique d'ordre supérieur*. PhD thesis, Université Paris 7, 1972.
- [7] Adam Gundry. *Type Inference, Haskell and Dependent Types*. PhD thesis, University of Strathclyde, 2013.
- [8] Georgios Karachalias, Tom Schrijvers, Dimitrios Vytiniotis, and Simon Peyton Jones. GADTs meet their match. In *International Conference on Functional Programming*, ICFP '15. ACM, 2015.
- [9] Stefan Monnier and David Haguenuer. Singleton types here, singleton types there, singleton types everywhere. In *Programming languages meets program verification*, PLPV '10. ACM, 2010.
- [10] Simon Peyton Jones, Dimitrios Vytiniotis, Stephanie Weirich, and Geoffrey Washburn. Simple unification-based type inference for GADTs. In *International Conference on Functional Programming*, ICFP '06. ACM, 2006.
- [11] Peter Sewell, Francesco Zappa Nardelli, Scott Owens, Gilles Peskine, Thomas Ridge, Susmit Sarkar, and Rok Strniša. Ott: Effective tool support for the working semanticist. *J. Funct. Prog.*, 20, 2010.
- [12] Martin Sulzmann, Manuel M. T. Chakravarty, Simon Peyton Jones, and Kevin Donnelly. System F with type equality coercions. In *Types in languages design and implementation*, TLDI '07. ACM, 2007.
- [13] Niki Vazou, Eric L. Seidel, Ranjit Jhala, Dimitrios Vytiniotis, and Simon Peyton Jones. Refinement types for haskell. In *International Conference on Functional Programming*, ICFP '14. ACM, 2014.
- [14] Dimitrios Vytiniotis, Stephanie Weirich, and Simon Peyton Jones. Boxy types: Inference for higher-rank types and impredicativity. In *International Conference on Functional Programming*, ICFP '06. ACM, 2006.
- [15] Dimitrios Vytiniotis, Simon Peyton Jones, Tom Schrijvers, and Martin Sulzmann. OutsideIn(X): Modular type inference with local assumptions. *J. Funct. Prog.*, 21, 2011.
- [16] Dimitrios Vytiniotis, Simon Peyton Jones, and José Pedro Magalhães. Equality proofs and deferred type errors: A compiler pearl. In *International Conference on Functional Programming*, ICFP '12. ACM, 2012.
- [17] Stephanie Weirich, Dimitrios Vytiniotis, Simon Peyton Jones, and Steve Zdancewic. Generative type abstraction and type-level computation. In *POPL*. ACM, 2011.
- [18] Stephanie Weirich, Justin Hsu, and Richard A. Eisenberg. System FC with explicit kind equality. In *International Conference on Functional Programming*, ICFP '13. ACM, 2013.
- [19] Hongwei Xi, Chiyang Chen, and Gang Chen. Guarded recursive datatype constructors. In *Principles of Programming Languages*, POPL '03. ACM, 2003.
- [20] Brent A. Yorgey, Stephanie Weirich, Julien Cretin, Simon Peyton Jones, Dimitrios Vytiniotis, and José Pedro Magalhães. Giving Haskell a promotion. In *Types in Language Design and Implementation*, TLDI '12. ACM, 2012.

## A. System FC, in full

Throughout this entire proof of type safety, any omitted proof is by (perhaps mutual) straightforward induction on the relevant derivations.

As usual, all definitions and proofs are only up to  $\alpha$ -equivalence. If there is a name clash, assume a variable renaming to a fresh variable.

### A.1 The grammar of System FC

$H$	::= $TYPE \mid (\rightarrow) \mid 'K \mid T$	Type constants
$T$	::= $D \mid N$	Algebraic types
$e, u$	::= $x \mid \lambda \delta. e \mid e_1 e_2 \mid e \tau \mid e \gamma \mid e \triangleright \gamma$	Expressions
$\pi$	::= $K \mid \text{case } e \text{ return } \tau \text{ of } \bar{\pi} \rightarrow \bar{u}$	contra $\gamma \tau$
$\epsilon$	::= $E \mid NE$	Erasure modalities
$\tau, \sigma, \kappa$	::= $a \mid H \mid \tau \psi \mid \forall \delta. \tau \mid F[\bar{\tau}] \mid \tau \triangleright \gamma$	Types
$\xi$	::= $a \mid H \mid \xi_1 \xi_2 \mid \xi c \mid \xi \triangleright c$	Type patterns
$\delta$	::= $a : \epsilon \kappa \mid c : \phi \mid x : \tau$	Binders
$\psi$	::= $\tau \mid \gamma$	Arguments
$\gamma, \eta$	::= $\langle \tau \rangle \mid \text{sym } \gamma \mid \gamma_1 \circ \gamma_2 \mid \gamma_1 \rightarrow \gamma_2$	Coercions
	$\mid H(\bar{w}) \mid \gamma_1 \gamma_2(\eta) \mid \gamma_1(\gamma_2, \gamma_3)_X \mid \forall \eta^c(a_1, a_2, c). \gamma$	
	$\mid \forall_X(c_1, c_2). \gamma \mid F[\bar{\tau}] \mid \text{nth}^i \gamma \mid \text{left } \gamma \mid \text{right } \gamma$	
	$\mid \gamma @ \omega \mid \text{kind } \gamma \mid \text{kapp } \gamma \mid \text{kapp}_1 \gamma \mid \text{kapp}_2 \gamma$	
	$\mid c \mid \mathcal{F}[i][\bar{\psi}] \mid \mathcal{N}[\bar{\tau}] \mid \text{sub } \gamma \mid \gamma \triangleright \eta$	
$\omega$	::= $\gamma \mid (\gamma_1, \gamma_2)_\rho$	Coercion args.
$\phi$	::= $\tau_1 \sim_\rho \tau_2$	Propositions
$\chi$	::= $\langle \eta_1, \eta_2 \rangle_\rho$	Higher-order cos.
$z$	::= $a \mid c$	Type/coercion var.
$\zeta$	::= $\kappa \mid \phi$	Type/coercion kind
$\rho$	::= $N \mid R$	Roles
$\Phi$	::= $[\Delta]. F[\bar{\xi}] \sim_N \sigma$	T.F. equations
$\Psi$	::= $\Phi$	T.F. axiom types
$\Sigma$	::= $\emptyset \mid \Sigma, \text{sbnd}$	Signatures
$\text{sbnd}$	::= $T : \forall \Delta. \star \mid K : \tau \mid F : [\Delta]. \kappa$	Sig. bindings
	$\mid \mathcal{F} : \Psi \mid \mathcal{N} : [\bar{a} : \bar{\kappa}]. N \bar{a} \sim_R^{\bar{\kappa}} \sigma$	
$\Gamma, \Delta$	::= $\emptyset \mid \Gamma, \delta$	Contexts
$\Delta$	::= $\emptyset \mid \Delta, \text{rbnd}$	Telescopes w/roles
$\text{rbnd}$	::= $a : \epsilon \rho \kappa \mid c : \phi$	Role bindings
$\theta$	::= $\emptyset \mid \theta, \text{map}$	Substitutions
$\text{map}$	::= $\tau / a \mid \gamma / c$	Mappings
$t$	::= $a \mid H \mid t p \mid \forall d. t \mid F[\bar{t}]$	Erased types
$f$	::= $t_1 \sim_\rho t_2$	Erased props.
$p$	::= $t_{(k)} \mid \bullet_{(f)}$	Erased args.
$d$	::= $a : \epsilon k \mid \bullet : f$	Erased binders
$q$	::= $\emptyset \mid q, \text{emap}$	Erased subst.
$\text{emap}$	::= $t / a \mid \bullet / c$	Erased mappings
$L$	::= $\emptyset \mid L, \text{lmap}$	Lifting contexts
$\text{lmap}$	::= $a \mapsto \gamma \mid c \mapsto (\eta_1, \eta_2)$	Liftings

### A.2 Typing and validity judgments

$\Sigma \vdash H$  has roles  $\bar{\rho}$     Role assignment to constants

$$\frac{T : \forall \bar{a}_i : \bar{\rho}_i \cdot \bar{\kappa}_i^i \cdot \star \in \Sigma}{\Sigma \vdash T \text{ has roles } \bar{\rho}_i^i} \text{ ROLES\_TYCON}$$

$$\frac{K : \forall \bar{a}_i : \bar{\rho}_i \cdot \bar{\kappa}_i^i \cdot \forall \bar{z}_j : \bar{\rho}_j \cdot \bar{\zeta}_j^j \cdot \bar{\sigma}_k^k \rightarrow D \bar{a}_i \bar{\kappa}_i^i \in \Sigma}{\Sigma \vdash 'K \text{ has roles } \bar{N}^i, \bar{N}^j, \bar{R}^k} \text{ ROLES\_DCON}$$

$$\overline{\Sigma \vdash (\rightarrow) \text{ has roles } R, R} \text{ ROLES\_ARROW}$$

$$\overline{\Sigma \vdash TYPE \text{ has roles } N} \text{ ROLES\_TYPE}$$

$\Sigma \vdash H : \kappa$     Constant kinds

$$\overline{\Sigma \vdash TYPE : \text{Levity} \rightarrow \star} \text{ CONST\_TYPE}$$

$$\overline{\Sigma \vdash (\rightarrow) : \star \rightarrow \star \rightarrow \star} \text{ CONST\_ARROW}$$

$$\frac{K : \tau \in \Sigma}{\Sigma \vdash 'K : \tau} \text{ CONST\_DATACON}$$

$$\frac{T : \forall \bar{a}_i : \bar{\rho}_i \cdot \bar{\kappa}_i^i \cdot \star \in \Sigma}{\Sigma \vdash T : \forall \bar{a}_i : \bar{\rho}_i \cdot \bar{\kappa}_i^i \cdot \star} \text{ CONST\_TYCON}$$

$\text{erase}_{\Sigma; \Gamma}(\tau) \rightsquigarrow t$     Erasure of types

$$\overline{\text{erase}_{\Sigma; \Gamma}(a) \rightsquigarrow a} \text{ ERASE\_VAR}$$

$$\overline{\text{erase}_{\Sigma; \Gamma}(H) \rightsquigarrow H} \text{ ERASE\_TYCON}$$

$$\frac{\text{erase}_{\Sigma; \Gamma}(\tau_1) \rightsquigarrow t_1 \quad \text{erase}_{\Sigma; \Gamma}(\tau_2) \rightsquigarrow t_2 \quad \Sigma; \Gamma \vdash \tau_2 : \kappa \quad \text{erase}_{\Sigma; \Gamma}(\kappa) \rightsquigarrow k}{\text{erase}_{\Sigma; \Gamma}(\tau_1 \tau_2) \rightsquigarrow t_1 t_2(k)} \text{ ERASE\_APPTY}$$

$$\frac{\text{erase}_{\Sigma; \Gamma}(\tau) \rightsquigarrow t \quad \Sigma; \Gamma \vdash \gamma : \phi \quad \text{erase}_{\Sigma; \Gamma}(\phi) \rightsquigarrow f}{\text{erase}_{\Sigma; \Gamma}(\tau \gamma) \rightsquigarrow t \bullet_{(f)}} \text{ ERASE\_APPCO}$$

$$\frac{\text{erase}_{\Sigma; \Gamma}(\kappa) \rightsquigarrow k \quad \text{erase}_{\Sigma; \Gamma, a : \kappa}(\tau) \rightsquigarrow t}{\text{erase}_{\Sigma; \Gamma}(\forall a : \epsilon \kappa. \tau) \rightsquigarrow \forall a : \epsilon k. t} \text{ ERASE\_FORALLTY}$$

$$\frac{\text{erase}_{\Sigma; \Gamma}(\phi) \rightsquigarrow f \quad \text{erase}_{\Sigma; \Gamma, c : \phi}(\tau) \rightsquigarrow t}{\text{erase}_{\Sigma; \Gamma}(\forall c : \phi. \tau) \rightsquigarrow \forall \bullet : f. t} \text{ ERASE\_FORALLCO}$$

$$\frac{\text{erase}_{\Sigma; \Gamma}(\bar{\tau}) \rightsquigarrow \bar{t}}{\text{erase}_{\Sigma; \Gamma}(F[\bar{\tau}]) \rightsquigarrow F[\bar{t}]} \text{ ERASE\_TYFAM}$$

$$\frac{\text{erase}_{\Sigma; \Gamma}(\tau) \rightsquigarrow t}{\text{erase}_{\Sigma; \Gamma}(\tau \triangleright \gamma) \rightsquigarrow t} \text{ ERASE\_CAST}$$

$\text{erase}_{\Sigma; \Gamma}(\bar{\psi}) \rightsquigarrow \bar{p}$     Erasure of argument lists

$$\overline{\text{erase}_{\Sigma; \Gamma}(\emptyset) \rightsquigarrow \emptyset} \text{ ERASE\_NIL}$$

$$\frac{\text{erase}_{\Sigma; \Gamma}(\tau) \rightsquigarrow t \quad \Sigma; \Gamma \vdash \tau : \kappa \quad \text{erase}_{\Sigma; \Gamma}(\kappa) \rightsquigarrow k \quad \text{erase}_{\Sigma; \Gamma}(\bar{\psi}) \rightsquigarrow \bar{p}}{\text{erase}_{\Sigma; \Gamma}(\tau, \bar{\psi}) \rightsquigarrow t_{(k)}, \bar{p}} \text{ ERASE\_TYPE}$$

$$\frac{\Sigma; \Gamma \vdash \gamma : \phi \quad \text{erase}_{\Sigma; \Gamma}(\phi) \rightsquigarrow f \quad \text{erase}_{\Sigma; \Gamma}(\bar{\psi}) \rightsquigarrow \bar{p}}{\text{erase}_{\Sigma; \Gamma}(\gamma, \bar{\psi}) \rightsquigarrow \bullet_{(f)}, \bar{p}} \text{ ERASE\_COERCION}$$

$\text{erase}_{\Sigma; \Gamma}(\phi) \rightsquigarrow f$	Erasure of propositions	$\frac{\text{erase}_{\Sigma; \Gamma}(\kappa_1) \rightsquigarrow k_1 \quad \text{erase}_{\Sigma; \Gamma}(\kappa_2) \rightsquigarrow k_2 \quad \text{erase}_{\Sigma; \Gamma}(\tau_1) \rightsquigarrow t_1 \quad \text{erase}_{\Sigma; \Gamma}(\tau_2) \rightsquigarrow t_2}{\text{erase}_{\Sigma; \Gamma}(\tau_1 \sim_{\rho} \tau_2) \rightsquigarrow t_1 \sim_{\rho} t_2} \text{ERASE\_PROP}$
$\Sigma \vdash \text{compat}(\Phi_1, \Phi_2)$	Type family equation compatibility	$\frac{\Sigma; \Gamma \vdash \tau : \forall a: \epsilon \kappa_1. \kappa_2 \quad \Sigma; \Gamma \vdash \sigma : \kappa_1 \quad \Sigma; \Gamma \vdash \kappa_1 : \star}{\Sigma; \Gamma \vdash \tau \sigma : \kappa_2[\sigma/a]} \text{TY\_APPTY}$
$\Sigma \vdash \text{compat}(\Phi_1, \Phi_2)$	Type family equation compatibility	$\frac{\Sigma; \Gamma \vdash \tau : \forall c: \phi. \kappa \quad \Sigma; \Gamma \vdash \gamma : \phi}{\Sigma; \Gamma \vdash \tau \gamma : \kappa[\gamma/c]} \text{TY\_APPCO}$
$\Sigma \vdash \text{compat}(\Phi_1, \Phi_2)$	Type family equation compatibility	$\frac{\Sigma; \Gamma, a: \kappa \vdash \tau : \text{TYPE } \sigma \quad \Sigma; \Gamma \vdash \sigma : \text{Levity}}{\Sigma; \Gamma \vdash \forall a: \text{E}\kappa. \tau : \text{TYPE } \sigma} \text{TY\_FORALLTY\_E}$
$\Sigma \vdash \text{compat}(\Phi_1, \Phi_2)$	Type family equation compatibility	$\frac{\Sigma; \Gamma, a: \kappa \vdash \tau : \text{TYPE } \sigma}{\Sigma; \Gamma \vdash \forall a: \text{NE}\kappa. \tau : \star} \text{TY\_FORALLTY\_NE}$
$\Sigma \vdash \text{compat}(\Phi_1, \Phi_2)$	Type family equation compatibility	$\frac{\Sigma; \Gamma, c: \phi \vdash \tau : \star \quad \Sigma; \Gamma \vdash \forall c: \phi. \tau : \star}{\Sigma; \Gamma \vdash \forall c: \phi. \tau : \star} \text{TY\_FORALLCO}$
$\Sigma \vdash \text{compat}(\Phi_1, \Phi_2)$	Type family equation compatibility	$\frac{F : [\Delta]. \kappa \in \Sigma \quad \Sigma; \Gamma \vdash_{\text{tel}} \bar{\tau} \Leftarrow \Delta}{\Sigma; \Gamma \vdash F[\bar{\tau}] : \kappa[\bar{\tau}/\Delta]} \text{TY\_TYFAM}$
$\Sigma \vdash \text{compat}(\Phi_1, \Phi_2)$	Type family equation compatibility	$\frac{\Sigma; \Gamma \vdash \tau : \sigma_1 \quad \Sigma; \Gamma \vdash \gamma : \sigma_1 \sim_{\text{R}} \sigma_2 \quad \Sigma; \Gamma \vdash \sigma_2 : \star}{\Sigma; \Gamma \vdash \tau \triangleright \gamma : \sigma_2} \text{TY\_CAST}$
$\Sigma \vdash \text{no\_conflict}(\Psi, \Phi, \bar{t}, i)$	T.F. equation conflict check	$\frac{\Sigma; \Gamma \vdash \gamma : \phi}{\Sigma; \Gamma \vdash \gamma : \phi} \text{Coercion typing}$
$\Sigma \vdash \text{no\_conflict}(\Psi, \Phi, \bar{t}, 0)$	NC_ZERO	$\frac{\Sigma; \Gamma \vdash \tau : \kappa}{\Sigma; \Gamma \vdash \langle \tau \rangle : \tau \sim_{\text{N}} \tau} \text{CO\_REFL}$
$\Sigma \vdash \text{no\_conflict}(\Psi, \Phi, \bar{t}, j)$	NC_APART	$\frac{\Sigma; \Gamma \vdash \gamma : \tau_2 \sim_{\rho} \tau_1}{\Sigma; \Gamma \vdash \text{sym } \gamma : \tau_1 \sim_{\rho} \tau_2} \text{CO\_SYM}$
$\Sigma \vdash \text{no\_conflict}(\Psi, \Phi, \bar{t}_0, j+1)$	NC_APART	$\frac{\Sigma; \Gamma \vdash \gamma_1 : \tau_1 \sim_{\rho} \tau_2 \quad \Sigma; \Gamma \vdash \gamma_2 : \tau_2 \sim_{\rho} \tau_3}{\Sigma; \Gamma \vdash \gamma_1 \circ \gamma_2 : \tau_1 \sim_{\rho} \tau_3} \text{CO\_TRANS}$
$\Sigma \vdash \text{no\_conflict}(\Psi, \Phi, \bar{t}_0, j+1)$	NC_COMPATIBLE	$\frac{\Sigma; \Gamma \vdash \gamma_1 : \tau_1 \sim_{\rho} \sigma_1 \quad \Sigma; \Gamma \vdash \gamma_2 : \tau_2 \sim_{\rho} \sigma_2}{\Sigma; \Gamma \vdash \gamma_1 \rightarrow \gamma_2 : (\tau_1 \rightarrow \tau_2) \sim_{\rho} (\sigma_1 \rightarrow \sigma_2)} \text{CO\_ARROW}$
$\Sigma; \Gamma \vdash \tau : \kappa$	Kinding	$\frac{\Sigma \vdash H \text{ has roles } \bar{\rho}_i^i \quad \Sigma; \Gamma \vdash \omega_i : (\psi_i, \psi'_i)_{\rho_i} \quad \Sigma; \Gamma \vdash H \bar{\psi}_i^i : \kappa_1 \quad \Sigma; \Gamma \vdash H \bar{\psi}'_i^i : \kappa_2}{\Sigma; \Gamma \vdash H(\bar{\omega}_i^i) : H \bar{\psi}_i^i \sim_{\text{R}} H \bar{\psi}'_i^i} \text{CO\_TYCONAPP}$
$\Sigma; \Gamma \vdash \text{ctx}$	TY_VAR	$\frac{a: \tau \in \Gamma \quad \Sigma; \Gamma \vdash \text{ctx}}{\Sigma; \Gamma \vdash a : \tau} \text{TY\_VAR}$
$\Sigma; \Gamma \vdash H : \kappa$	TY_CONST	$\frac{\Sigma; \Gamma \vdash \text{ctx} \quad \Sigma \vdash H : \kappa}{\Sigma; \Gamma \vdash H : \kappa} \text{TY\_CONST}$
$\Sigma; \Gamma \vdash \tau_1 : \text{TYPE } \sigma_1$	TY_ARROW	$\frac{\Sigma; \Gamma \vdash \tau_1 : \text{TYPE } \sigma_1 \quad \Sigma; \Gamma \vdash \tau_2 : \text{TYPE } \sigma_2}{\Sigma; \Gamma \vdash \tau_1 \rightarrow \tau_2 : \star} \text{TY\_ARROW}$
$\Sigma; \Gamma \vdash \tau : \kappa_1 \rightarrow \kappa_2$	TY_APP	$\frac{\Sigma; \Gamma \vdash \tau : \kappa_1 \rightarrow \kappa_2 \quad \Sigma; \Gamma \vdash \sigma : \kappa_1 \quad \Sigma; \Gamma \vdash \kappa_1 : \star \quad \neg \exists \tau' \text{ s.t. } \tau = (\rightarrow) \tau'}{\Sigma; \Gamma \vdash \tau \sigma : \kappa_2} \text{TY\_APP}$
$\Sigma; \Gamma \vdash \tau_1 : \text{TYPE } \sigma_1$	TY_ARROW	$\frac{\Sigma; \Gamma \vdash \gamma_1 : \tau_1 \sim_{\rho} \tau_2 \quad \Sigma; \Gamma \vdash \gamma_2 : \sigma_1 \sim_{\text{N}} \sigma_2 \quad \Sigma; \Gamma \vdash \sigma_1 : \kappa_1 \quad \Sigma; \Gamma \vdash \sigma_2 : \kappa_2 \quad \Sigma; \Gamma \vdash \eta : \kappa_1 \sim_{\rho} \kappa_2 \quad \Sigma; \Gamma \vdash \tau_1 \sigma_1 : \kappa_0 \quad \Sigma; \Gamma \vdash \tau_2 \sigma_2 : \kappa'_0}{\Sigma; \Gamma \vdash \gamma_1 \gamma_2(\eta) : \tau_1 \sigma_1 \sim_{\rho} \tau_2 \sigma_2} \text{CO\_APPTY}$

$\frac{\begin{array}{l} \Sigma; \Gamma \vdash \gamma_0 : \tau_1 \sim_\rho \tau_2 \\ \Sigma; \Gamma \vdash \gamma_1 : \phi_1 \quad \Sigma; \Gamma \vdash \tau_1 \gamma_1 : \kappa'_1 \\ \Sigma; \Gamma \vdash \gamma_2 : \phi_2 \quad \Sigma; \Gamma \vdash \tau_2 \gamma_2 : \kappa'_2 \\ \Sigma; \Gamma \vdash \chi : \phi_1 \sim_\rho \phi_2 \end{array}}{\Sigma; \Gamma \vdash \gamma_0 (\gamma_1, \gamma_2)_\chi : \tau_1 \gamma_1 \sim_\rho \tau_2 \gamma_2}$	CO_APPCO	$\frac{\begin{array}{l} \Sigma; \Gamma \vdash \gamma : \tau_1 \sigma_1 \sim_N \tau_2 \sigma_2 \\ \Sigma; \Gamma \vdash \sigma_1 : \kappa_1 \\ \Sigma; \Gamma \vdash \sigma_2 : \kappa_2 \end{array}}{\Sigma; \Gamma \vdash \mathbf{kapp} \gamma : \kappa_1 \sim_N \kappa_2}$	CO_KAPPTY
$\frac{\begin{array}{l} \Sigma; \Gamma \vdash \eta : \kappa_1 \sim_\rho \kappa_2 \\ \Sigma; \Gamma, a_1 : \kappa_1, a_2 : \kappa_2, c : a_1 \sim_N a_2 \vdash \gamma : \tau_1 \sim_\rho \tau_2 \\ \Sigma; \Gamma \vdash \forall a_1 : \kappa_1. \tau_1 : \sigma_1 \quad \Sigma; \Gamma \vdash \forall a_2 : \kappa_2. \tau_2 : \sigma_2 \end{array}}{\Sigma; \Gamma \vdash \forall \eta (a_1, a_2, c). \gamma : \forall a_1 : \kappa_1. \tau_1 \sim_\rho \forall a_2 : \kappa_2. \tau_2}$	CO_FORALLTY	$\frac{\begin{array}{l} \Sigma; \Gamma \vdash \gamma : \tau_1 \gamma_1 \sim_N \tau_2 \gamma_2 \\ \Sigma; \Gamma \vdash \gamma_1 : \sigma_1 \sim_\rho \sigma_2 \\ \Sigma; \Gamma \vdash \gamma_2 : \sigma_3 \sim_\rho \sigma_4 \end{array}}{\Sigma; \Gamma \vdash \mathbf{kapp}_1 \gamma : \sigma_1 \sim_N \sigma_3}$	CO_KAPPCO1
$\frac{\begin{array}{l} \Sigma; \Gamma \vdash \chi : \phi_1 \sim_\rho \phi_2 \\ \Sigma; \Gamma, c_1 : \phi_1, c_2 : \phi_2 \vdash \gamma : \tau_1 \sim_\rho \tau_2 \\ \Sigma; \Gamma \vdash \forall c_1 : \phi_1. \tau_1 : \sigma_1 \quad \Sigma; \Gamma \vdash \forall c_2 : \phi_2. \tau_2 : \sigma_2 \end{array}}{\Sigma; \Gamma \vdash \forall \chi (c_1, c_2). \gamma : \forall c_1 : \phi_1. \tau_1 \sim_\rho \forall c_2 : \phi_2. \tau_2}$	CO_FORALLCO	$\frac{\begin{array}{l} \Sigma; \Gamma \vdash \gamma : \tau_1 \gamma_1 \sim_N \tau_2 \gamma_2 \\ \Sigma; \Gamma \vdash \gamma_1 : \sigma_1 \sim_\rho \sigma_2 \\ \Sigma; \Gamma \vdash \gamma_2 : \sigma_3 \sim_\rho \sigma_4 \end{array}}{\Sigma; \Gamma \vdash \mathbf{kapp}_2 \gamma : \sigma_2 \sim_N \sigma_4}$	CO_KAPPCO2
$\frac{\begin{array}{l} \Sigma; \Gamma \vdash \gamma_i : \tau_i \sim_N \sigma_i^i \\ \Sigma; \Gamma \vdash F[\bar{\tau}] : \kappa_{01} \\ \Sigma; \Gamma \vdash F[\bar{\sigma}] : \kappa_{02} \end{array}}{\Sigma; \Gamma \vdash F[\bar{\gamma}] : F[\bar{\tau}] \sim_N F[\bar{\sigma}]}$	CO_TYFAM	$\frac{\begin{array}{l} c : \phi \in \Gamma \\ \Sigma; \Gamma \vdash \mathbf{ctx} \\ \Sigma; \Gamma \vdash c : \phi \end{array}}{\text{CO\_VAR}}$	
$\frac{\begin{array}{l} \Sigma; \Gamma \vdash \gamma : H \bar{\psi}_j^j \sim_R H \bar{\psi}_j^j \\ \psi_i = \tau \quad \Sigma; \Gamma \vdash \tau : \kappa_1 \\ \psi'_i = \sigma \quad \Sigma; \Gamma \vdash \sigma : \kappa_2 \\ \Sigma \vdash H \text{ has roles } \bar{\rho}_j^j \\ H \text{ is not a newtype} \end{array}}{\Sigma; \Gamma \vdash \mathbf{nth}^i \gamma : \tau \sim_{\rho_i} \sigma}$	CO_NTH	$\frac{\begin{array}{l} \mathcal{F} : \Psi \in \Sigma \quad \Psi[i] = [\Delta]. F[\bar{\xi}] \sim_N \sigma \\ F : [\Delta_2]. \kappa' \in \Sigma \quad \Sigma; \Gamma \vdash_{\text{tel}} \bar{\psi} \Leftarrow \Delta \\ \text{erase}_{\Sigma; \Gamma}(\bar{\xi}[\bar{\psi}/\Delta]) \rightsquigarrow \bar{t} \quad \Sigma; \Gamma \vdash \kappa'[\bar{\xi}[\bar{\psi}/\Delta]/\Delta_2] : \star \\ \Sigma \vdash \text{no\_conflict}(\Psi, \Psi[i], \bar{t}, i) \end{array}}{\Sigma; \Gamma \vdash \mathcal{F}[i][\bar{\psi}] : F[\bar{\xi}][\bar{\psi}/\Delta] \sim_N \sigma[\bar{\psi}/\Delta]}$	CO_TFAXIOM
$\frac{\begin{array}{l} \Sigma; \Gamma \vdash \gamma : \forall a_1 : \kappa_1. \tau_1 \sim_\rho \forall a_2 : \kappa_2. \tau_2 \\ \Sigma; \Gamma \vdash \mathbf{nth}^0 \gamma : \kappa_1 \sim_\rho \kappa_2 \end{array}}{\text{CO\_NTHTY}}$	CO_NTHTY	$\frac{\begin{array}{l} \mathcal{N} : [\bar{a}; \bar{\kappa}]. N \bar{a} \sim_{\mathbb{R}}^{\kappa_0} \sigma \in \Sigma \\ \Sigma; \Gamma \vdash_{\text{tel}} \bar{\tau} \Leftarrow \bar{a}; \bar{\kappa} \\ \Sigma; \Gamma \vdash \kappa_0[\bar{\tau}/\bar{a}] : \star \end{array}}{\Sigma; \Gamma \vdash \mathcal{N}[\bar{\tau}] : N \bar{\tau} \sim_R \sigma[\bar{\tau}/\bar{a}]}$	CO_NTAXIOM
$\frac{\Sigma; \Gamma \vdash \gamma : \tau_1 \sim_N \tau_2}{\Sigma; \Gamma \vdash \mathbf{sub} \gamma : \tau_1 \sim_R \tau_2}$	CO_SUB	$\frac{\begin{array}{l} \Sigma; \Gamma \vdash \gamma : \tau_1 \sim_\rho \tau_2 \\ \Sigma; \Gamma \vdash \tau_1 \triangleright \eta : \kappa'_1 \end{array}}{\Sigma; \Gamma \vdash \gamma \triangleright \eta : (\tau_1 \triangleright \eta) \sim_\rho \tau_2}$	CO_COHERENCE
$\frac{\Sigma; \Gamma \vdash \gamma : (\forall c_1 : \tau_1 \sim_{\rho_2} \tau'_1. \sigma_1) \sim_\rho (\forall c_2 : \tau_2 \sim_{\rho_2} \tau'_2. \sigma_2)}{\Sigma; \Gamma \vdash \mathbf{nth}^0 \gamma : \tau_1 \sim_\rho \tau_2}$	CO_NTH0CO	$\Sigma; \Gamma \vdash \omega : (\psi_1, \psi_2)_\rho$	Coercion argument typing
$\frac{\Sigma; \Gamma \vdash \gamma : (\forall c_1 : \tau_1 \sim_{\rho_2} \tau'_1. \sigma_1) \sim_\rho (\forall c_2 : \tau_2 \sim_{\rho_2} \tau'_2. \sigma_2)}{\Sigma; \Gamma \vdash \mathbf{nth}^1 \gamma : \tau'_1 \sim_\rho \tau'_2}$	CO_NTH1CO	$\frac{\Sigma; \Gamma \vdash \gamma : \tau_1 \sim_\rho \tau_2}{\Sigma; \Gamma \vdash \gamma : (\tau_1, \tau_2)_\rho}$	COARG_TY
$\frac{\begin{array}{l} \Sigma; \Gamma \vdash \gamma : \tau_1 \psi_1 \sim_N \tau_2 \psi_2 \\ \Sigma; \Gamma \vdash \tau_1 : \kappa_1 \quad \Sigma; \Gamma \vdash \tau_2 : \kappa_2 \end{array}}{\Sigma; \Gamma \vdash \mathbf{left} \gamma : \tau_1 \sim_N \tau_2}$	CO_LEFT	$\frac{\begin{array}{l} \Sigma; \Gamma \vdash \gamma_1 : \phi_1 \\ \Sigma; \Gamma \vdash \gamma_2 : \phi_2 \end{array}}{\Sigma; \Gamma \vdash (\gamma_1, \gamma_2)_\rho : (\gamma_1, \gamma_2)_\rho}$	COARG_CO
$\frac{\begin{array}{l} \Sigma; \Gamma \vdash \gamma : \tau_1 \sigma_1 \sim_N \tau_2 \sigma_2 \\ \Sigma; \Gamma \vdash \sigma_1 : \kappa_1 \quad \Sigma; \Gamma \vdash \sigma_2 : \kappa_2 \end{array}}{\Sigma; \Gamma \vdash \mathbf{right} \gamma : \sigma_1 \sim_N \sigma_2}$	CO_RIGHT	$\Sigma; \Gamma \vdash \chi : \phi_1 \sim_\rho \phi_2$	Higher-order coercion typing
$\frac{\begin{array}{l} \Sigma; \Gamma \vdash \gamma : \forall a_1 : \kappa_1. \tau_1 \sim_\rho \forall a_2 : \kappa_2. \tau_2 \\ \Sigma; \Gamma \vdash \eta : \sigma_1 \sim_N \sigma_2 \\ \Sigma; \Gamma \vdash \sigma_1 : \kappa_1 \quad \Sigma; \Gamma \vdash \sigma_2 : \kappa_2 \end{array}}{\Sigma; \Gamma \vdash \gamma @ \eta : \tau_1[\sigma_1/a_1] \sim_\rho \tau_2[\sigma_2/a_2]}$	CO_INSTTY	$\frac{\begin{array}{l} \Sigma; \Gamma \vdash \eta_1 : \sigma_1 \sim_\rho \sigma_3 \\ \Sigma; \Gamma \vdash \eta_2 : \sigma_2 \sim_\rho \sigma_4 \\ \phi_1 = \sigma_1 \sim_{\rho_2} \sigma_2 \quad \phi_2 = \sigma_3 \sim_{\rho_2} \sigma_4 \end{array}}{\Sigma; \Gamma \vdash \langle \eta_1, \eta_2 \rangle_{\rho_2} : \phi_1 \sim_\rho \phi_2}$	HCO_PAIR
$\frac{\begin{array}{l} \Sigma; \Gamma \vdash \gamma : \forall c_1 : \phi_1. \tau_1 \sim_\rho \forall c_2 : \phi_2. \tau_2 \\ \Sigma; \Gamma \vdash \eta_1 : \phi_1 \\ \Sigma; \Gamma \vdash \eta_2 : \phi_2 \end{array}}{\Sigma; \Gamma \vdash \gamma @ (\eta_1, \eta_2)_N : \tau_1[\eta_1/c_1] \sim_\rho \tau_2[\eta_2/c_2]}$	CO_INSTCO	$\Sigma; \Gamma \vdash_{\text{tel}} \bar{\psi} \Leftarrow \Delta$	Telescope typing
$\frac{\begin{array}{l} \Sigma; \Gamma \vdash \gamma : \tau_1 \sim_\rho \tau_2 \\ \Sigma; \Gamma \vdash \tau_1 : \kappa_1 \quad \Sigma; \Gamma \vdash \tau_2 : \kappa_2 \end{array}}{\Sigma; \Gamma \vdash \mathbf{kind} \gamma : \kappa_1 \sim_R \kappa_2}$	CO_KIND	$\frac{\Sigma; \Gamma \vdash \mathbf{ctx}}{\Sigma; \Gamma \vdash_{\text{tel}} \emptyset \Leftarrow \emptyset}$	TEL_NIL
		$\frac{\begin{array}{l} \Sigma; \Gamma \vdash_{\text{tel}} \bar{\psi} \Leftarrow \Delta \\ \Sigma; \Gamma \vdash \tau : \kappa[\bar{\psi}/\Delta] \end{array}}{\Sigma; \Gamma \vdash_{\text{tel}} \bar{\psi}, \tau \Leftarrow \Delta, a : \kappa}$	TEL_TY



$$\frac{\Sigma; \Gamma \vdash_{\text{tel}} \bar{\psi} \Leftarrow \Delta \quad \Sigma; \Gamma \vdash \gamma : \phi[\bar{\psi}/\Delta]}{\Sigma; \Gamma \vdash_{\text{tel}} \bar{\psi}, \gamma \Leftarrow \Delta, c : \phi} \text{TEL\_CO}$$

$\Sigma; \Gamma \vdash \phi \text{ ok}$  Proposition validity

$$\frac{\Sigma; \Gamma \vdash \tau_1 : \kappa_1 \quad \Sigma; \Gamma \vdash \tau_2 : \kappa_2}{\Sigma; \Gamma \vdash \tau_1 \sim_{\rho} \tau_2 \text{ ok}} \text{PROP\_EQUALITY}$$

$\Sigma; \Gamma \vdash \text{ctx}$  Context validity

$$\frac{\vdash \Sigma \text{ ok}}{\Sigma; \emptyset \vdash \text{ctx}} \text{CTX\_EMPTY}$$

$$\frac{\Sigma; \Gamma \vdash \kappa : \star \quad a \# \Gamma}{\Sigma; \Gamma, a : \kappa \vdash \text{ctx}} \text{CTX\_TYVAR}$$

$$\frac{\Sigma; \Gamma \vdash \phi \text{ ok} \quad c \# \Gamma}{\Sigma; \Gamma, c : \phi \vdash \text{ctx}} \text{CTX\_COVAR}$$

$$\frac{\Sigma; \Gamma \vdash \tau : \text{TYPE}' \text{Lifted} \quad x \# \Gamma}{\Sigma; \Gamma, x : \tau \vdash \text{ctx}} \text{CTX\_LIFTEDVAR}$$

$$\frac{\Sigma; \Gamma \vdash \tau : \text{TYPE}' \text{Unlifted} \quad x \# \Gamma}{\Sigma; \Gamma, x : \tau \vdash \text{ctx}} \text{CTX\_UNLIFTEDVAR}$$

$\vdash \Sigma \text{ ok}$  Signature validity

$\vdash \text{Levity} : \star, \text{Lifted} : \text{Levity}, \text{Unlifted} : \text{Levity} \text{ ok}$  SIG\_BOOT

$$\frac{\Sigma; \emptyset \vdash \forall \overline{a_i : \mathbb{E} \kappa_i} . \star : \star \quad T \# \Sigma}{\vdash \Sigma, T : \forall \overline{a_i : \mathbb{E} \rho_i \kappa_i} . \star \text{ ok}} \text{SIG\_TYCON}$$

$$\frac{\tau = \forall \overline{a_i : \mathbb{E} \kappa_i} . \forall \Delta. D \overline{a_i \kappa_i} \quad \Sigma; \emptyset \vdash \tau : \star \quad K \# \Sigma}{\vdash \Sigma, K : \tau \text{ ok}} \text{SIG\_DATACON}$$

$$\frac{\Sigma; \overline{a_i : \kappa_i} \vdash \tau : \star \quad F \# \Sigma}{\vdash \Sigma, F : [\overline{a_i : \kappa_i}]. \tau \text{ ok}} \text{SIG\_TYFAM}$$

$\forall i :$

$$\Phi_i = [\Delta_i]. F[\bar{\xi}_i] \sim_{\mathbb{N}} \sigma_i$$

$$\Sigma; \Delta_i \vdash F[\bar{\xi}_i] : \kappa_i$$

$$\Sigma; \Delta_i \vdash \sigma_i : \kappa_i$$

$\mathcal{F} \# \Sigma$

$n > 1$

no axiom for  $F$  exists in  $\Sigma$

$$\vdash \Sigma, \mathcal{F} : \overline{\Phi_i}^{i < n} \text{ ok} \quad \text{SIG\_TFBRAXIOM}$$

$$\Sigma; \Delta \vdash F[\bar{\xi}] : \kappa$$

$$\Sigma; \Delta \vdash \sigma : \kappa$$

$$\mathcal{F} \# \Sigma$$

$\forall i$  such that  $\mathcal{F}'_i : [\Delta_i]. F[\bar{\xi}_i] \sim_{\mathbb{N}} \sigma_i \in \Sigma :$

$$\Sigma \vdash \text{compat}([\Delta]. F[\bar{\xi}] \sim_{\mathbb{N}} \sigma, [\Delta_i]. F[\bar{\xi}_i] \sim_{\mathbb{N}} \sigma_i)$$

SIG\_TFAX1

$$\vdash \Sigma, \mathcal{F} : [\Delta]. F[\bar{\xi}] \sim_{\mathbb{N}} \sigma \text{ ok}$$

$$\Sigma; \bar{a} : \bar{\kappa} \vdash N \bar{a} : \kappa$$

$$\Sigma; \bar{a} : \bar{\kappa} \vdash \sigma : \kappa$$

$$\mathcal{N} \# \Sigma$$

no axiom for  $N$  exists in  $\Sigma$

$$\vdash \Sigma, \mathcal{N} : [\bar{a} : \bar{\kappa}]. N \bar{a} \sim_{\mathbb{R}}^{\kappa} \sigma \text{ ok} \quad \text{SIG\_NTAXIOM}$$

$\Sigma; \Gamma \vdash e : \tau$  Typing

$$\frac{x : \tau \in \Gamma \quad \Sigma; \Gamma \vdash \text{ctx}}{\Sigma; \Gamma \vdash x : \tau} \text{TM\_VAR}$$

$$\frac{\Sigma; \Gamma, x : \tau_1 \vdash e : \tau_2}{\Sigma; \Gamma \vdash \lambda x : \tau_1. e : \tau_1 \rightarrow \tau_2} \text{TM\_ABS}$$

$$\frac{\Sigma; \Gamma \vdash e : \tau_1 \rightarrow \tau_2 \quad \Sigma; \Gamma \vdash u : \tau_1}{\Sigma; \Gamma \vdash e u : \tau_2} \text{TM\_APP}$$

$$\frac{\Sigma; \Gamma, a : \kappa \vdash e : \tau}{\Sigma; \Gamma \vdash \lambda a : \epsilon \kappa. e : \forall a : \epsilon \kappa. \tau} \text{TM\_TABS}$$

$$\frac{\Sigma; \Gamma \vdash e : \forall a : \epsilon \kappa. \sigma \quad \Sigma; \Gamma \vdash \tau : \kappa}{\Sigma; \Gamma \vdash e \tau : \sigma[\tau/a]} \text{TM\_TAPP}$$

$$\frac{\Sigma; \Gamma, c : \phi \vdash e : \tau}{\Sigma; \Gamma \vdash \lambda c : \phi. e : \forall c : \phi. \tau} \text{TM\_CABS}$$

$$\frac{\Sigma; \Gamma \vdash e : \forall c : \phi. \sigma \quad \Sigma; \Gamma \vdash \gamma : \phi}{\Sigma; \Gamma \vdash e \gamma : \sigma[\gamma/c]} \text{TM\_CAPP}$$

$$\frac{\Sigma; \Gamma \vdash e : \tau_1 \quad \Sigma; \Gamma \vdash \gamma : \tau_1 \sim_{\mathbb{R}} \tau_2 \quad \Sigma; \Gamma \vdash \tau_2 : \text{TYPE } \sigma}{\Sigma; \Gamma \vdash e \triangleright \gamma : \tau_2} \text{TM\_CAST}$$

$$\frac{K : \tau \in \Sigma \quad \Sigma; \Gamma \vdash \text{ctx}}{\Sigma; \Gamma \vdash K : \tau} \text{TM\_DATACON}$$

$$\Sigma; \Gamma \vdash e : D \bar{\tau}_j^j$$

$$\Sigma; \Gamma \vdash \tau : \star$$

$\overline{K_i}^i$  are exhaustive for  $D$

$\forall i :$

$$K_i : \forall \overline{a_j : \mathbb{E} \kappa_j} . \forall \overline{z_{ik} : \mathbb{E} \zeta_{ik} . \overline{\sigma_{im}}^m} \rightarrow D \overline{a_j}^j \in \Sigma$$

$$\Sigma; \Gamma, \overline{z_{ik} : \mathbb{E} \zeta_{ik} [\bar{\tau}/\bar{a}]}^k, \overline{x_{im} : \sigma_{im} [\bar{\tau}/\bar{a}]}^m \vdash u_i : \tau$$

$$\Sigma; \Gamma \vdash \text{case } e \text{ return } \tau \text{ of } \overline{K_i \bar{z}_i \bar{x}_i \rightarrow u_i}^i : \tau$$

TM\_CASE

$$\Sigma; \Gamma \vdash \gamma : H_1 \bar{\tau} \sim_{\mathbb{N}} H_2 \bar{\sigma}$$

$$H_1 \neq H_2$$

$$\Sigma; \Gamma \vdash \tau : \text{TYPE } \sigma$$

$$\Sigma; \Gamma \vdash \text{contra } \gamma \tau : \tau \quad \text{TM\_CONTRA}$$

$\boxed{\Sigma; \Delta \vdash_\rho \tau \text{ ok}}$  “Assuming  $\Delta$ ,  $\tau$  can be used at role  $\rho$ .”

$$\frac{a; \rho' \kappa \in \Delta \quad \rho' \leq \rho}{\Sigma; \Delta \vdash_\rho a \text{ ok}} \text{ R\_VAR}$$

$$\frac{b \# \Delta}{\Sigma; \Delta \vdash_\rho b \text{ ok}} \text{ R\_OTHERVAR}$$

$$\frac{\Sigma \vdash H \text{ has roles } \bar{\rho} \quad \Sigma; \Delta \vdash_{\rho_i} \tau_i \text{ ok}^i}{\Sigma; \Delta \vdash_R H \bar{\tau} \text{ ok}} \text{ R\_TYCONAPP}$$

$$\frac{}{\Sigma; \Delta \vdash_N H \text{ ok}} \text{ R\_TYCON}$$

$$\frac{\Sigma; \Delta \vdash_\rho \tau \text{ ok} \quad \Sigma; \Delta \vdash_N \sigma \text{ ok}}{\Sigma; \Delta \vdash_\rho \tau \sigma \text{ ok}} \text{ R\_APPTY}$$

$$\frac{\Sigma; \Delta \vdash_\rho \tau \text{ ok}}{\Sigma; \Delta \vdash_\rho \tau \gamma \text{ ok}} \text{ R\_APPCO}$$

$$\frac{\Sigma; \Delta \vdash_\rho \kappa \text{ ok} \quad \Sigma; \Delta, a; \bar{N} \kappa \vdash_\rho \tau \text{ ok}}{\Sigma; \Delta \vdash_\rho \forall a: \epsilon \kappa. \tau \text{ ok}} \text{ R\_FORALLTY}$$

$$\frac{\Sigma; \Delta \vdash_\rho \phi \text{ ok} \quad \Sigma; \Delta, c: \phi \vdash_\rho \tau \text{ ok}}{\Sigma; \Delta \vdash_\rho \forall c: \phi. \tau \text{ ok}} \text{ R\_FORALLCO}$$

$$\frac{\Sigma; \Delta \vdash_N \tau_i \text{ ok}^i}{\Sigma; \Delta \vdash_\rho F[\bar{\tau}] \text{ ok}} \text{ R\_TYFAM}$$

$$\frac{\Sigma; \Delta \vdash_\rho \tau \text{ ok}}{\Sigma; \Delta \vdash_\rho \tau \triangleright \gamma \text{ ok}} \text{ R\_CAST}$$

$\boxed{\Sigma; \Delta \vdash_\rho \phi \text{ ok}}$  “Assuming  $\Delta$ ,  $\phi$  can be used at role  $\rho$ .”

$$\frac{\Sigma; \Delta \vdash_{\min(\rho, \rho_2)} \sigma_1 \text{ ok} \quad \Sigma; \Delta \vdash_{\min(\rho, \rho_2)} \sigma_2 \text{ ok}}{\Sigma; \Delta \vdash_\rho \sigma_1 \sim_{\rho_2} \sigma_2 \text{ ok}} \text{ RPROP\_EQUALITY}$$

$\boxed{\rho_1 \leq \rho_2}$  “ $\rho_1$  is a sub-role of  $\rho_2$ .”

$$\frac{}{N \leq R} \text{ SUB\_NOMREP}$$

$$\frac{}{\rho \leq \rho} \text{ SUB\_REFL}$$

$\boxed{\Sigma \vdash H \Leftarrow \bar{\rho}}$  “ $\bar{\rho}$  are appropriate roles for  $H$ .”

$$\frac{\forall \bar{a}, \bar{b}, \bar{\sigma} \text{ s.t. } K : \forall \bar{a}: \bar{E} \bar{\kappa}. \forall \bar{b}: \bar{E} \bar{\kappa}'. \bar{\sigma} \rightarrow D \bar{a} \in \Sigma : \quad \Sigma; \bar{a}: \bar{\rho} \bar{\kappa} \vdash_R \sigma_i \text{ ok}^i}{\Sigma \vdash D \Leftarrow \bar{\rho}} \text{ ROLES\_DATA}$$

$$\frac{\mathcal{N} : [\bar{a}: \bar{\kappa}]. N \bar{a} \sim_R^\kappa \sigma \in \Sigma \quad \Sigma; \bar{a}: \bar{\rho} \bar{\kappa} \vdash_R \sigma \text{ ok}}{\Sigma \vdash N \Leftarrow \bar{\rho}} \text{ ROLES\_NEWTYP E}$$

**Lemma 1** (Sub-roling). *If  $\Sigma; \Delta \vdash_\rho \tau \text{ ok}$  and  $\rho \leq \rho'$ , then  $\Sigma; \Delta \vdash_{\rho'} \tau \text{ ok}$ .*

## B. Lifting

**Definition 2** (Lifting contexts). Define a lifting context  $L$  to be a list of mappings from type variables to coercions ( $a \mapsto \gamma$ ) and coercion variables to pairs of coercions  $c \mapsto (\eta_1, \eta_2)$ .

Lifting contexts are checked for validity by the following judgment:

$\boxed{\Sigma; \Gamma \vdash L \Leftarrow \Delta}$  Lifting context validity

$$\frac{}{\Sigma; \Gamma \vdash \emptyset \Leftarrow \emptyset} \text{ LC\_NIL}$$

$$\frac{\Sigma; \Gamma \vdash L \Leftarrow \Delta \quad \Sigma; \Gamma \vdash \gamma : \sigma_1 \sim_\rho \sigma_2 \quad \Sigma; \Gamma \vdash \sigma_1 : L_{\Sigma; \Gamma}^L(\kappa) \quad \Sigma; \Gamma \vdash \sigma_2 : L_{\Sigma; \Gamma}^R(\kappa)}{\Sigma; \Gamma \vdash L, a \mapsto \gamma \Leftarrow \Delta, a: \bar{\rho} \kappa} \text{ LC\_TYPE}$$

$$\frac{\Sigma; \Gamma \vdash L \Leftarrow \Delta \quad \Sigma; \Gamma \vdash \gamma_1 : L_{\Sigma; \Gamma}^L(\phi) \quad \Sigma; \Gamma \vdash \gamma_2 : L_{\Sigma; \Gamma}^R(\phi)}{\Sigma; \Gamma \vdash L, c \mapsto (\gamma_1, \gamma_2) \Leftarrow \Delta, c: \phi} \text{ LC\_COERCION}$$

**Definition 3** (Lifting substitutions). If  $L$  is a lifting context, then let  $\theta = L_{\Sigma; \Gamma}^L$  be a substitution, built by the following two rules:

1. For every  $a \mapsto \gamma \in L$ ,  $a \mapsto \sigma_1 \in \theta$ , where  $\Sigma; \Gamma \vdash \gamma : \sigma_1 \sim_\rho \sigma_2$ .
2. For every  $c \mapsto (\gamma_1, \gamma_2) \in L$ ,  $c \mapsto \gamma_1 \in \theta$ .

Define  $L_{\Sigma; \Gamma}^R$  similarly, but with  $\sigma_2$  and  $\gamma_2$  instead of  $\sigma_1$  and  $\gamma_1$ .

**Definition 4** (Lifting). Define the lifting operation, written  $L_{\Sigma; \Gamma}(\tau)_\rho = \gamma$  over types,  $L_{\Sigma; \Gamma}(\gamma)_\rho = \omega$  over coercions, and  $L_{\Sigma; \Gamma}(\phi)_\rho = \chi$  over propositions, as follows, with equations tried in order from

top to bottom.

$$\begin{aligned}
L_{\Sigma;\Gamma}(a)_\rho &= \gamma \\
&\text{where } a \mapsto \gamma \in L \wedge \Sigma; \Gamma \vdash \gamma : \sigma_1 \sim_\rho \sigma_2 \\
L_{\Sigma;\Gamma}(a)_R &= \mathbf{sub} \gamma \\
&\text{where } a \mapsto \gamma \in L \\
L_{\Sigma;\Gamma}(a)_N &= \langle a \rangle \\
&\text{where } a \notin \text{dom}(L) \\
L_{\Sigma;\Gamma}(a)_R &= \mathbf{sub} \langle a \rangle \\
&\text{where } a \notin \text{dom}(L) \\
L_{\Sigma;\Gamma}(\tau_1 \rightarrow \tau_2)_\rho &= L_{\Sigma;\Gamma}(\tau_1)_\rho \rightarrow L_{\Sigma;\Gamma}(\tau_2)_\rho \\
L_{\Sigma;\Gamma}(H \bar{\psi})_R &= H(\overline{L_{\Sigma;\Gamma}(\psi_i)_{\rho_i}}^i) \\
&\text{where } \Sigma \vdash H \text{ has roles } \bar{\rho} \\
L_{\Sigma;\Gamma}(H)_N &= \langle H \rangle \\
L_{\Sigma;\Gamma}(\tau_1 \tau_2)_\rho &= L_{\Sigma;\Gamma}(\tau_1)_\rho L_{\Sigma;\Gamma}(\tau_2)_{N(L_{\Sigma;\Gamma}(\kappa_2)_\rho)} \\
&\text{where } \Sigma; \Gamma \vdash \tau_2 : \kappa_2 \\
L_{\Sigma;\Gamma}(\tau \gamma)_\rho &= L_{\Sigma;\Gamma}(\tau)_\rho (L_{\Sigma;\Gamma}^L(\gamma), L_{\Sigma;\Gamma}^R(\gamma))_{L_{\Sigma;\Gamma}(\phi)_\rho} \\
&\text{where } \Sigma; \Gamma \vdash \gamma : \phi \\
L_{\Sigma;\Gamma}(\forall a:^\epsilon \kappa. \tau)_\rho &= \forall_{L_{\Sigma;\Gamma}(\kappa)_\rho}^\epsilon (a_1, a_2, c). L'_{\Sigma;\Gamma'}(\tau)_\rho \\
&\text{where } L' = L, a \mapsto c \\
&\quad \Gamma' = \Gamma, a_1: L_{\Sigma;\Gamma}^L(\kappa), a_2: L_{\Sigma;\Gamma}^R(\kappa), c: a_1 \sim_N a_2 \\
&\quad a_1, a_2, \text{ and } c \text{ are fresh} \\
L_{\Sigma;\Gamma}(\forall c: \phi. \tau)_\rho &= \forall_{L_{\Sigma;\Gamma}(\phi)_\rho} (c_1, c_2). L'_{\Sigma;\Gamma'}(\tau)_\rho \\
&\text{where } L' = L, c \mapsto (c_1, c_2) \\
&\quad \Gamma' = \Gamma, c_1: L_{\Sigma;\Gamma}^L(\phi), c_2: L_{\Sigma;\Gamma}^R(\phi) \\
&\quad c_1 \text{ and } c_2 \text{ are fresh} \\
L_{\Sigma;\Gamma}(F[\bar{\tau}])_N &= F[L_{\Sigma;\Gamma}(\bar{\tau})_N] \\
L_{\Sigma;\Gamma}(F[\bar{\tau}])_R &= \mathbf{sub} F[L_{\Sigma;\Gamma}(\bar{\tau})_N] \\
L_{\Sigma;\Gamma}(\tau \triangleright \gamma)_\rho &= (\mathbf{sym} ((\mathbf{sym} L_{\Sigma;\Gamma}(\tau)_\rho) \triangleright L_{\Sigma;\Gamma}^R(\gamma))) \triangleright L_{\Sigma;\Gamma}^L(\gamma) \\
L_{\Sigma;\Gamma}(\gamma)_\rho &= (L_{\Sigma;\Gamma}^L(\gamma), L_{\Sigma;\Gamma}^R(\gamma))_\rho \\
L_{\Sigma;\Gamma}(\tau_1 \sim_{\rho_2} \tau_2)_\rho &= \langle L_{\Sigma;\Gamma}(\tau_1)_{\min(\rho, \rho_2)}, L_{\Sigma;\Gamma}(\tau_2)_{\min(\rho, \rho_2)} \rangle_{\rho_2}
\end{aligned}$$

**Lemma 5 (Lifting).** Assume  $\Sigma; \Gamma \vdash L \Leftarrow \Delta$ , and let  $\Gamma' = \Gamma, |\Delta|$ .

1. If  $\Sigma; \Gamma' \vdash \tau : \kappa$  and  $\Sigma; \Delta \vdash_\rho \tau \text{ ok}$ , then  $\Sigma; \Gamma \vdash L_{\Sigma;\Gamma'}(\tau)_\rho : L_{\Sigma;\Gamma'}^L(\tau) \sim_\rho L_{\Sigma;\Gamma'}^R(\tau)$ .
2. If  $\Sigma; \Gamma' \vdash \phi \text{ ok}$  and  $\Sigma; \Delta \vdash_\rho \phi \text{ ok}$ , then  $\Sigma; \Gamma \vdash L_{\Sigma;\Gamma'}(\phi)_\rho : L_{\Sigma;\Gamma'}^L(\phi) \sim_\rho L_{\Sigma;\Gamma'}^R(\phi)$ .

*Proof.* By induction on the typing derivation  $\Sigma; \Gamma, |\Delta| \vdash \tau : \kappa$ .

**Case TY\_VAR:** We know  $\tau = a$ . We have several cases to consider here:

- $a \notin \text{dom}(L)$ : Straightforward application of typing rules.
- $a \mapsto \gamma \in L, \Sigma; \Gamma' \vdash \gamma : \sigma_1 \sim_\rho \sigma_2$ : Straightforward application of typing rules. Note that  $\gamma$  must not mention variables bound in  $\Delta$ , as per  $\Sigma; \Gamma \vdash L \Leftarrow \Delta$ .
- $a \mapsto \gamma \in L, \Sigma; \Gamma' \vdash \gamma : \sigma_1 \sim_N \sigma_2, \rho = \mathbf{R}$ : Straightforward application of typing rules.
- $a \mapsto \gamma \in L, \Sigma; \Gamma' \vdash \gamma : \sigma_1 \sim_R \sigma_2, \rho = \mathbf{N}$ : This case is impossible, given that  $\Sigma; \Gamma \vdash L \Leftarrow \Delta$  and  $\Sigma; \Delta \vdash_N a \text{ ok}$ .

**Case TY\_CONST:** Straightforward application of typing rules.

**Case TY\_ARROW:** We know  $\tau = \tau_1 \rightarrow \tau_2$ , and  $L_{\Sigma;\Gamma'}(\tau_1 \rightarrow \tau_2)_\rho = L_{\Sigma;\Gamma'}(\tau_1)_\rho \rightarrow L_{\Sigma;\Gamma'}(\tau_2)_\rho$ . We finish by induction, noting that the roles on  $(\rightarrow)$  are both representational, as required for us to satisfy the premises of the induction hypothesis in the  $\rho = \mathbf{R}$  case.

**Case TY\_APP:** We know  $\tau = \tau_1 \tau_2$ . We now have several cases:

$\tau = H \bar{\psi}, \rho = \mathbf{R}$ : We see that  $L_{\Sigma;\Gamma'}(H \bar{\psi})_R = H(\overline{L_{\Sigma;\Gamma'}(\psi_i)_{\rho_i}}^i)$  where  $\Sigma \vdash H$  has roles  $\bar{\rho}$ . Inversion on  $\Sigma; \Delta \vdash_\rho H \bar{\psi} \text{ ok}$  can go by either **R\_TYCONAPP** or **R\_APP**. In either case, we can finish via induction, perhaps invoking Lemma 1 in the **R\_APP** case.

**Other cases:** By induction. Here, there is no overlap when inverting  $\Sigma; \Delta \vdash_\rho \tau \text{ ok}$  to establish the premises of the inductive hypothesis. It is here that we need the extra conditions on  $\kappa_1$  in **TY\_APP** and **TY\_APPTY** in order to keep induction well-founded.

**Case TY\_APPTY:** Similar to previous case.

**Case TY\_APPCO:** We know  $\tau = \tau_0 \gamma$ . Let  $\gamma_0 = L_{\Sigma;\Gamma'}(\tau_0)_\rho$ ,  $\gamma_1 = L_{\Sigma;\Gamma'}^L(\gamma)$ ,  $\gamma_2 = L_{\Sigma;\Gamma'}^R(\gamma)$ , and  $\chi = L_{\Sigma;\Gamma'}(\phi)_\rho$ . We then know  $L_{\Sigma;\Gamma'}(\tau_0 \gamma)_\rho = \gamma_0 (\gamma_1, \gamma_2)_\chi$ . We are done by the induction hypothesis and **CO\_APPCO**.

**Case TY\_FORALLTY:** We know  $\tau = \forall a:^\epsilon \kappa. \tau_0$ . Let  $\forall_\eta^\epsilon(a_1, a_2, c). \gamma = L_{\Sigma;\Gamma'}(\tau)_\rho$ . We can straightforwardly apply the induction hypothesis to learn about  $\eta$ . Let  $\Gamma_2 = \Gamma, |\Delta|, a_1: \kappa_1, a_2: \kappa_2, c: a_1 \sim_N a_2$ , where  $\kappa_1 = L_{\Sigma;\Gamma'}^L(\kappa)$  and  $\kappa_2 = L_{\Sigma;\Gamma'}^R(\kappa)$ . We wish to use the induction hypothesis to learn about  $\gamma = L'_{\Sigma;\Gamma_2}(\tau_0)_\rho$ , where  $L' = L, a \mapsto c$ . However, we have to fix the contexts. We can see that  $\text{fv}(\kappa_1) \# \Delta$  and  $\text{fv}(\kappa_2) \# \Delta$ , because all the variables in  $\Delta$  have been substituted away. Let  $\Gamma_1 = \Gamma, a_1: \kappa_1, a_2: \kappa_2, c: a_1 \sim_N a_2$ . We thus permute and weaken  $\Gamma_2$  to  $\Gamma_3 = \Gamma_1, |\Delta|, a: \kappa$ . Now, we set  $\Delta' = \Delta, a: \mathbb{E}_N \kappa$ , and we can see  $\Sigma; \Gamma_1 \vdash L' \Leftarrow \Delta', \Sigma; \Gamma_1, |\Delta'| \vdash \tau_0 : \star$ , and  $\Sigma; \Delta' \vdash_\rho \tau_0 \text{ ok}$ , allowing us to use the induction hypothesis to finish.

**Case TY\_FORALLCO:** Similar to last case.

**Case TY\_TYFAM:** Straightforward use of induction hypothesis and typing rules.

**Case TY\_CAST:** Straightforward use of induction hypothesis and typing rules.

**Case PROP\_EQUALITY:** Straightforward use of induction hypothesis and typing rules. □

## C. Consistency

The proof that follows is heavily based on the consistency proof in Breitner et al. [2], updated where necessary. Some text is copied verbatim from that previous paper, with permission.

Throughout this proof, I always assume that  $\vdash \Sigma \text{ ok}$ .

**Definition 6 (Value types).** Define value types as types that fit in the following grammar:

$$v ::= D \mid 'K \mid \text{TYPE} \mid (\rightarrow) \mid \forall \delta. \tau \mid v \tau$$

**Definition 7 (Type consistency).** Two types  $\tau_1$  and  $\tau_2$  are *consistent* if, whenever they are both value types:

1. If  $\tau_1 = H \bar{\sigma}$ , then  $\tau_2 = H \bar{\sigma}'$ ;
2. If  $\tau_1 = \forall \delta_1. \tau_1$  then  $\tau_2 = \forall \delta_2. \tau_2$ .

Note that if either  $\tau_1$  or  $\tau_2$  is *not* a value type, then they are vacuously consistent. Also, note that a type headed by a **newtype** is not a value type.

**Definition 8 (Context consistency).** A signature  $\Sigma$  is *consistent* if, whenever  $\Sigma; \emptyset \vdash \gamma : \tau_1 \sim_R \tau_2$ ,  $\tau_1$  and  $\tau_2$  are consistent.

In order to prove consistency, we define a type reduction relation  $\Sigma \vdash \tau \rightsquigarrow_\rho \sigma$ , show that the relation preserves value type heads, and then show that any well-typed coercion corresponds to a path in the rewrite relation.

Here is the type rewrite relation:

$$\boxed{\Sigma \vdash \tau \rightsquigarrow_\rho \sigma} \quad \text{Type reduction}$$

$$\frac{}{\Sigma \vdash \tau \rightsquigarrow_\rho \tau} \text{RED\_REFL}$$

$$\frac{\Sigma \vdash \tau_1 \rightsquigarrow_\rho \tau_2 \quad \Sigma \vdash \psi_1 \rightsquigarrow_N \psi_2}{\Sigma \vdash \tau_1 \psi_1 \rightsquigarrow_\rho \tau_2 \psi_2} \text{RED\_APP}$$

$$\frac{\Sigma \vdash \psi_i \rightsquigarrow_{\rho_i} \psi'_i \quad \Sigma \vdash H \text{ has roles } \bar{\rho}}{\Sigma \vdash H \bar{\psi} \rightsquigarrow_R H \bar{\psi}'} \text{RED\_TYCONAPP}$$

$$\frac{}{\Sigma \vdash \forall \delta_1. \tau_1 \rightsquigarrow_\rho \forall \delta_2. \tau_2} \text{RED\_FORALL}$$

$$\frac{\Sigma \vdash \tau_i \rightsquigarrow_N \sigma_i^i}{\Sigma \vdash F[\bar{\tau}_i^i] \rightsquigarrow_\rho F[\bar{\sigma}_i^i]} \text{RED\_TYFAM}$$

$$\frac{\mathcal{F} : \Psi \in \Sigma \quad \Psi[i] = [\Delta]. F[\bar{\xi}] \sim_N \sigma \quad \text{erase}_{\Sigma; \Gamma}(\bar{\xi}[\bar{\psi}/\Delta]) \rightsquigarrow \bar{t} \quad \Sigma \vdash \text{no.conflict}(\Psi, \Psi[i], \bar{t}, i)}{\Sigma \vdash F[\bar{\xi}[\bar{\psi}/\Delta]] \rightsquigarrow_\rho \sigma[\bar{\psi}/\Delta]} \text{RED\_TFAXIOM}$$

$$\frac{\mathcal{N} : [\bar{a}; \bar{\kappa}]. N \bar{a} \sim_R^{\bar{\kappa}} \sigma \in \Sigma}{\Sigma \vdash N \bar{\tau} \rightsquigarrow_R \sigma[\bar{\tau}/\bar{a}]} \text{RED\_NTAXIOM}$$

$$\frac{}{\Sigma \vdash \tau \triangleright \gamma \rightsquigarrow_\rho \tau} \text{RED\_CAST}$$

$$\boxed{\Sigma \vdash \gamma_1 \rightsquigarrow_\rho \gamma_2} \quad \text{Coercion "reduction"}$$

$$\frac{}{\Sigma \vdash \gamma_1 \rightsquigarrow_\rho \gamma_2} \text{RED\_COERCION}$$

**Lemma 9** (Simple rewrite substitution). *If  $\Sigma \vdash \tau_1 \rightsquigarrow_\rho \tau_2$ , then  $\Sigma \vdash \tau_1[\sigma/\alpha] \rightsquigarrow_\rho \tau_2[\sigma/\alpha]$ .*

**Lemma 10** (Rewrite substitution). *Let  $\bar{a}$  be the free type variables in a type  $\sigma$ . If  $\Sigma; \bar{a}_i :_{\rho_i}^E \kappa_i^i \vdash_R \sigma$  ok:*

1. *If  $\Sigma \vdash \tau_i \rightsquigarrow_{\rho_i} \tau'_i$ , then  $\Sigma \vdash \sigma[\bar{\tau}_i/\bar{a}_i] \rightsquigarrow_R \sigma[\bar{\tau}'_i/\bar{a}_i]$ ;*
2. *If  $\Sigma \vdash \tau_i \rightsquigarrow_N \tau'_i$ , then  $\Sigma \vdash \sigma[\bar{\tau}_i/\bar{a}_i] \rightsquigarrow_N \sigma[\bar{\tau}'_i/\bar{a}_i]$ .*

*Proof sketch.* Along the lines of the proof for the same lemma in Breitner et al. [2].  $\square$

**Lemma 11** (Sub-rolling in the rewrite relation). *If  $\Sigma \vdash \tau_1 \rightsquigarrow_N \tau_2$ , then  $\Sigma \vdash \tau_1 \rightsquigarrow_\rho \tau_2$ .*

**Lemma 12** (RED\_APP/RED\_TYCONAPP). *Assume  $\Sigma \vdash H$  has roles  $\bar{\rho}$ . If  $\Sigma \vdash H \bar{\psi}_1 \psi'_1 \rightsquigarrow_R H \bar{\psi}_2 \psi'_2$  by RED\_APP, the length of  $\bar{\psi}_1$  is less than the length of  $\bar{\rho}$ , then  $\Sigma \vdash H \bar{\psi}_1 \psi'_1 \rightsquigarrow_R H \bar{\psi}_2 \psi'_2$  also by RED\_TYCONAPP.*

*Proof sketch.* Along the lines of the proof for the same lemma in Breitner et al. [2].  $\square$

**Lemma 13** (Pattern). *Let  $\bar{z}$  be the free variables in a type pattern  $\xi$ . We require that each variable  $z_i$  is mentioned exactly once in  $\xi$ . Then, if, for some  $\bar{\psi}$ ,  $\Sigma \vdash \xi[\bar{\psi}/\bar{z}] \rightsquigarrow_N \tau$ , then there exist  $\bar{\psi}'$  such that  $\tau \approx \xi[\bar{\psi}'/\bar{z}]$  and  $\Sigma \vdash \bar{\psi} \rightsquigarrow_N \bar{\psi}'$ . Here,  $\approx$  relates types that are the same, perhaps with the exception of the existence of casts.*

*Proof.* We proceed by induction on the structure of  $\xi$ .

**Case  $\xi = a$ :** There is just one free variable ( $a$ ), and thus just one type  $\sigma$ . We have  $\Sigma \vdash \sigma \rightsquigarrow_N \tau'$ . Let  $\sigma' = \tau'$  and we are done.

**Case  $\xi = \xi_1 \xi_2$ :** Partition the free variables into a list  $\bar{z}_1$  that appear in  $\xi_1$  and  $\bar{z}_2$  that appear in  $\xi_2$ . This partition must be possible by assumption. Similarly, partition  $\bar{\psi}$  into  $\bar{\psi}_1$  and  $\bar{\psi}_2$ . We can see that  $\Sigma \vdash \xi_1[\bar{\psi}_1/\bar{z}_1] \xi_2[\bar{\psi}_2/\bar{z}_2] \rightsquigarrow_N \tau$ . Thus must be by RED\_APP. Thus,  $\tau = \tau_1 \tau_2$  and  $\Sigma \vdash \xi_1[\bar{\psi}_1/\bar{z}_1] \rightsquigarrow_N \tau_1$  and  $\Sigma \vdash \xi_2[\bar{\psi}_2/\bar{z}_2] \rightsquigarrow_N \tau_2$ . We then use the induction hypothesis to get  $\bar{\psi}'_1$  and  $\bar{\psi}'_2$  such that  $\tau_1 \approx \xi_1[\bar{\psi}'_1/\bar{z}_1]$  and  $\tau_2 \approx \xi_2[\bar{\psi}'_2/\bar{z}_2]$ . We conclude that  $\bar{\psi}'$  is the combination of  $\bar{\psi}'_1$  and  $\bar{\psi}'_2$ , undoing the partition done earlier.

**Case  $\xi = \xi_0 c$ :** Similar to previous case. The coercion  $\gamma$  that corresponds to the variable  $c$  can step to any other coercion, but this does not pose a problem when constructing the  $\bar{\psi}'$ .

**Case  $\xi = H$ :** Trivial.

**Case  $\xi = \xi_0 \triangleright c$ :** Trivial.  $\square$

**Lemma 14** (Patterns). *Let  $\bar{z}$  be the free variables in a list of type patterns  $\bar{\xi}$ . Assume each variable  $z_i$  is mentioned exactly once in  $\bar{\xi}$ . If, for some  $\bar{\psi}$ ,  $\Sigma \vdash \bar{\xi}[\bar{\psi}/\bar{z}] \rightsquigarrow_N \bar{\tau}'$ , then there exist  $\bar{\psi}'$  such that  $\bar{\tau}' \approx \bar{\xi}[\bar{\psi}'/\bar{z}]$  and  $\Sigma \vdash \bar{\psi} \rightsquigarrow_N \bar{\psi}'$ .*

*Proof.* By induction on the length of  $\bar{\xi}$ .

**Base case:** Trivial.

**Inductive case:** We partition and recombine variables as in the  $\xi_1 \xi_2$  case in the previous proof and proceed by induction.  $\square$

**Lemma 15** (Local diamond). *If  $\Sigma \vdash \tau \rightsquigarrow_\rho \sigma_1$  and  $\Sigma \vdash \tau \rightsquigarrow_\rho \sigma_2$ , then there exists  $\sigma_3$  such that  $\Sigma \vdash \sigma_1 \rightsquigarrow_\rho \sigma_3$  and  $\Sigma \vdash \sigma_2 \rightsquigarrow_\rho \sigma_3$ .*

*Proof.* Along the lines of the proof of the same lemma in Breitner et al. [2]. The RED\_FORALL rule is liberalized here, but that does not pose a challenge in proving this lemma. In dealing with type family applications, we use Lemma 14, noting that no two axioms can exist with the same *erased* left-hand sides. This justifies the use of  $\approx$  in the conclusion of Lemmas 13 and 14.  $\square$

Let the notation  $\Sigma \vdash \tau_1 \Leftrightarrow_\rho \tau_2$  mean that there exists a  $\sigma$  such that  $\Sigma \vdash \tau_1 \rightsquigarrow_\rho^* \sigma$  and  $\Sigma \vdash \tau_2 \rightsquigarrow_\rho^* \sigma$ .

**Lemma 16** (Confluence). *The rewrite relation  $\rightsquigarrow_\rho$  is confluent. That is, if  $\Sigma \vdash \tau \rightsquigarrow_\rho^* \sigma_1$  and  $\Sigma \vdash \tau \rightsquigarrow_\rho^* \sigma_2$ , then  $\Sigma \vdash \sigma_1 \Leftrightarrow_\rho \sigma_2$ .*

*Proof.* Confluence is a consequence of the local diamond property, Lemma 15.  $\square$

**Lemma 17** (Stepping preserves value type heads). *If  $v_1$  is a value type and  $\Sigma \vdash v_1 \rightsquigarrow_R v_2$ , then  $v_2$  has the same head as  $v_1$ .*

*Proof.* By straightforward induction.  $\square$

**Lemma 18** (Rewrite relation consistency). *If  $\Sigma \vdash \tau_1 \Leftrightarrow_\rho \tau_2$ , then  $\tau_1$  and  $\tau_2$  are consistent.*

*Proof.* If either  $\tau_1$  or  $\tau_2$  is not a value type, then we are trivially done. So, we assume  $\tau_1$  and  $\tau_2$  are value types. By assumption, there exists  $\sigma$  such that  $\Sigma \vdash \tau_1 \rightsquigarrow_{\rho}^* \sigma$  and  $\Sigma \vdash \tau_2 \rightsquigarrow_{\rho}^* \sigma$ . By induction over the length of these reductions and the use of Lemma 17, we can see that  $\sigma$  must have the same head as both  $\tau_1$  and  $\tau_2$ . Thus,  $\tau_1$  and  $\tau_2$  have the same head, and are thus consistent.  $\square$

**Lemma 19** (Nominal rewriting preserves applications). *If  $\Sigma \vdash \tau_1 \Leftrightarrow_{\mathbb{N}} \tau_2$ , then if one of  $\tau_1$  or  $\tau_2$  is a type application, the other is, too.*

*Proof.* By inspection of the rewrite rules.  $\square$

**Lemma 20** (Admissibility of accessor coercions). *The coercion  $\eta$  in the rules below is existentially quantified. In each case, the typing derivation for  $\eta$  is strictly smaller than the typing derivation for  $\gamma$ . Furthermore, we assume that the types proved equal – say,  $\tau_1$  and  $\tau_2$  – by  $\gamma$  are joinable: that is,  $\Sigma \vdash \tau_1 \Leftrightarrow_{\rho} \tau_2$ .*

1. **CO\_NTH:** *If  $\Sigma; \emptyset \vdash \gamma : H \bar{\psi} \sim_{\mathbb{R}} H \bar{\psi}'$ ,  $\psi_i$  is a type  $\tau$ , and  $H$  is not a newtype, then  $\Sigma; \emptyset \vdash \eta : \tau_i \sim_{\rho_i} \tau'_i$ , where  $\Sigma \vdash H$  has roles  $\bar{\rho}$ .*
2. **CO\_NTHTY:** *If  $\Sigma; \emptyset \vdash \gamma : \forall a_1: \kappa_1. \tau_1 \sim_{\rho} \forall a_2: \kappa_2. \tau_2$ , then  $\Sigma; \emptyset \vdash \eta : \kappa_1 \sim_{\rho} \kappa_2$ .*
3. **CO\_NTHOCO:** *If  $\Sigma; \emptyset \vdash \gamma : \forall c_1: \tau_1 \sim_{\rho'} \tau'_1. \sigma_1 \sim_{\rho} \forall c_2: \tau_2 \sim_{\rho'} \tau'_2. \sigma_2$ , then  $\Sigma; \emptyset \vdash \eta : \tau_1 \sim_{\rho} \tau_2$ .*
4. **CO\_NTHICO:** *If  $\Sigma; \emptyset \vdash \gamma : \forall c_1: \tau_1 \sim_{\rho'} \tau'_1. \sigma_1 \sim_{\rho} \forall c_2: \tau_2 \sim_{\rho'} \tau'_2. \sigma_2$ , then  $\Sigma; \emptyset \vdash \eta : \tau'_1 \sim_{\rho} \tau'_2$ .*
5. **CO\_LEFT:** *If  $\Sigma; \emptyset \vdash \gamma : \tau_1 \psi_1 \sim_{\mathbb{N}} \tau_2 \psi_2$ , then  $\Sigma; \emptyset \vdash \eta : \tau_1 \sim_{\mathbb{N}} \tau_2$ .*
6. **CO\_RIGHT:** *If  $\Sigma; \emptyset \vdash \gamma : \tau_1 \sigma_1 \sim_{\mathbb{N}} \tau_2 \sigma_2$ , then  $\Sigma; \emptyset \vdash \eta : \sigma_1 \sim_{\mathbb{N}} \sigma_2$ .*
7. **CO\_INSTTY:** *If  $\Sigma; \emptyset \vdash \gamma : \forall a_1: \kappa_1. \tau_1 \sim_{\rho} \forall a_2: \kappa_2. \tau_2$ ,  $\Sigma; \emptyset \vdash \gamma' : \sigma_1 \sim_{\mathbb{N}} \sigma_2$ ,  $\Sigma; \emptyset \vdash \sigma_1 : \kappa_1$ , and  $\Sigma; \emptyset \vdash \sigma_2 : \kappa_2$ , then  $\Sigma; \emptyset \vdash \eta : \tau_1[\sigma_1/a_1] \sim_{\rho} \tau_2[\sigma_2/a_2]$ .*
8. **CO\_INSTCO:** *If  $\Sigma; \emptyset \vdash \gamma : \forall c_1: \phi_1. \tau_1 \sim_{\rho} \forall c_2: \phi_2. \tau_2$ ,  $\Sigma; \emptyset \vdash \gamma_1 : \phi_1$ , and  $\Sigma; \emptyset \vdash \gamma_2 : \phi_2$ , then  $\Sigma; \emptyset \vdash \eta : \tau_1[\gamma_1/c_1] \sim_{\rho} \tau_2[\gamma_2/c_2]$ .*
9. **CO\_KIND:** *If  $\Sigma; \emptyset \vdash \gamma : \tau_1 \sim_{\rho} \tau_2$ ,  $\Sigma; \emptyset \vdash \tau_1 : \kappa_1$ , and  $\Sigma; \emptyset \vdash \tau_2 : \kappa_2$ , then  $\Sigma; \emptyset \vdash \eta : \kappa_1 \sim_{\mathbb{R}} \kappa_2$ .*
10. **CO\_KAPPTY:** *If  $\Sigma; \emptyset \vdash \gamma : \tau_1 \sigma_1 \sim_{\mathbb{N}} \tau_2 \sigma_2$ ,  $\Sigma; \emptyset \vdash \sigma_1 : \kappa_1$ , and  $\Sigma; \emptyset \vdash \sigma_2 : \kappa_2$ , then  $\Sigma; \emptyset \vdash \eta : \kappa_1 \sim_{\mathbb{N}} \kappa_2$ .*
11. **CO\_KAPPCO1:** *If  $\Sigma; \emptyset \vdash \gamma : \tau_1 \gamma_1 \sim_{\mathbb{N}} \tau_2 \gamma_2$ ,  $\Sigma; \emptyset \vdash \gamma_1 : \sigma_1 \sim_{\rho} \sigma_2$ , and  $\Sigma; \emptyset \vdash \gamma_2 : \sigma_3 \sim_{\rho} \sigma_4$ , then  $\Sigma; \emptyset \vdash \eta : \sigma_1 \sim_{\mathbb{N}} \sigma_3$ .*
12. **CO\_KAPPCO2:** *If  $\Sigma; \emptyset \vdash \gamma : \tau_1 \gamma_1 \sim_{\mathbb{N}} \tau_2 \gamma_2$ ,  $\Sigma; \emptyset \vdash \gamma_1 : \sigma_1 \sim_{\rho} \sigma_2$ , and  $\Sigma; \emptyset \vdash \gamma_2 : \sigma_3 \sim_{\rho} \sigma_4$ , then  $\Sigma; \emptyset \vdash \eta : \sigma_2 \sim_{\mathbb{N}} \sigma_4$ .*

*Proof sketch.* By induction on the typing derivation for  $\gamma$ , using Lemmas 18 and 19 in the **CO\_TRANS** case.  $\square$

**Lemma 21** (Completeness of the rewrite relation). *If  $\Sigma; \emptyset \vdash \gamma : \tau_1 \sim_{\rho} \tau_2$ , then  $\Sigma \vdash \tau_1 \Leftrightarrow_{\rho} \tau_2$ .*

*Proof.* By induction on  $\Sigma; \emptyset \vdash \gamma : \tau_1 \sim_{\rho} \tau_2$ .

**Case CO\_REFL:** Trivial –  $\Leftrightarrow_{\rho}$  is reflexive.

**Case CO\_SYM:** Trivial –  $\Leftrightarrow_{\rho}$  is symmetric.

**Case CO\_TRANS:** Consequence of confluence (Lemma 16).

**Case CO\_ARROW:** By induction.

**Case CO\_TYCONAPP:** By induction.

**Case CO\_APPTY:** By induction.

**Case CO\_APPCO:** By induction.

**Case CO\_FORALLTY:** Trivial.

**Case CO\_FORALLCO:** Trivial.

**Case CO\_TYFAM:** By induction.

**“Accessor” coercions:** By Lemma 20 and then induction.

**Case CO\_VAR:** Impossible in an empty context.

**Case CO\_TFAXIOM:** Trivial.

**Case CO\_NTAXIOM:** Trivial.

**Case CO\_SUB:** By induction and Lemma 11.

**Case CO\_COHERENCE:** Trivial.  $\square$

**Lemma 22** (Consistency). *If  $\vdash \Sigma$  ok, then  $\Sigma$  is consistent.*

*Proof.* Take a  $\gamma$  such that  $\Sigma; \emptyset \vdash \gamma : \tau_1 \sim_{\mathbb{R}} \tau_2$ . By the completeness of the rewrite relation (Lemma 21), we see that  $\Sigma \vdash \tau_1 \Leftrightarrow_{\mathbb{R}} \tau_2$ . But, the rewrite relation consistency lemma (Lemma 18) tells us that  $\tau_1$  and  $\tau_2$  are consistent. Thus, the context admits only consistent coercions and is itself consistent.  $\square$