Type-checking Linearity in Core/System FC

Rodrigo Mesquita
Bernardo Toninho

August 6, 2023

Abstract

Linear types were added both to Haskell and to its Core intermediate language, which is used as an internal consistency tool to validate the transformations a Haskell program undergoes during compilation. However, the current Core type-checker rejects many linearly valid programs that originate from Core-to-Core optimizing transformations. As such, linearity typing is effectively disabled, for otherwise disabling optimizations would be far more devastating. The goal of our proposed dissertation is to develop an extension to Core's type system that accepts a larger amount of programs and verifies that optimizing transformations applied to well-typed linear Core produce well-typed linear Core. Our extension will be based on attaching variable *usage environments* to binders, which augment the type system with more fine-grained contextual linearity information, allowing the system to accept programs which seem to syntactically violate linearity but preserve linear resource usage. We will also develop a usage environment inference procedure and integrate the procedure with the type checker. We will validate our proposal by showing a range of Core-to-Core transformations can be typed by our system.

Resumo

Tipos lineares foram integrados ambos no Haskell e na sua linguagem intermédia, Core, que serve como uma ferramenta de consistência interna do compilador que valida as transformações feitas nos programas ao longo do processo de compilação. No entanto, o sistema de tipos do Core rejeita programas lineares válidos que são produto de optimizações Core-to-Core, de tal forma que a validação da linearidade ao nível do sistema de tipos não consegue ser desempenhada com sucesso, sendo que a alternativa, não aplicar optimizações, tem resultados bastante mais indesejáveis. O objetivo da dissertação que nos propomos a fazer é extender ao sistema de tipos do Core de forma a aceitar mais programas lineares, e verificar que as optimizações usadas não destroem a linearidade dos programas. A nossa extensão parte de adicionar *ambientes de uso* às variáveis, aumentando o sistema de tipos com informação de linearidade suficiente para aceitar programas que aparentemente violam linearidade sintaticamente, mas que a preservam a um nível semântico. Para além do sistema de tipos, vamos desenvolver um algoritmo de inferência de *ambientes de uso*. Vamos validar a nossa proposta através do conjunto de transformações Core-to-Core que o nosso sistema consegue tipificar.

Contents

List of Figures

CHAPTER 1

Introduction

Statically safe programming languages provide compile time correctness guarantees by having the compiler rule out certain classes of errors or invalid programs. Moreover, static typing allows programmers to state and enforce (compile-time) invariants relevant to their problem domain. In this sense, type safety entails that all possible executions of a type-correct program cannot exhibit behaviors deemed "wrong" by the type system design. This idea is captured in the motto "well-typed programs do not go wrong".

Linear type systems [**?**, **?**] add expressiveness to existing type systems by enforcing that certain *resources* (e.g. a file handle) must be used *exactly once*. In programming languages with a linear type system, not using certain resources or using them twice are flagged as type errors. Linear types can thus be used to, for example, statically guarantee that file handles, socket descriptors, and allocated memory is freed exactly once (leaks and double-frees become type errors), and channel-based communication protocols are deadlock-free [**?**], among other high-level correctness properties [**?**, **?**, **?**].

As an example, consider the following C-like program in which allocated memory is freed twice. We know this to be the dreaded double-free error which will crash the program at runtime. Regardless, a C-like type system will accept this program without any issue.

```
let p = malloc (4);
in free (p);
   free (p);
```

Under the lens of a linear type system, consider the variable p to be a linear resource created by the call to `malloc`. Since p is linear, it must be used *exactly once*. However, the program above uses p twice, in the two different calls to `free`. With a linear type system, the program above *does not typecheck*! In this sense, linear typing effectively ensures the program does not compile with a double-free error. In Section 2.1 we give a formal account of linear types and provide additional examples.

Despite their promise and their extensive presence in research literature [**?**, **?**, **?**], the effective design of the combination of linear and non-linear typing is both challenging and necessary to bring the advantages of linear typing to mainstream languages. Consequently, few general purpose programming languages have linear type systems. Among them are Idris 2 [**?**], a linearly and dependently typed language based on Quantitative Type Theory, Rust [**?**], a language whose ownership types build on linear types to guarantee memory safety without garbage collection or reference counting, and, more recently, Haskell [**?**], a *purely functional* and *lazy* language.

Linearity in Haskell stands out from linearity in Rust and Idris 2 due to the following reasons:

- Linear types were only added to the language roughly *31 years after* Haskell's inception, unlike Rust and Idris 2 which were designed with linearity from the start. It is an especially difficult endeavour to add linear types to a well-established language with a large library ecosystem and many active users, rather than to develop the language from the ground up with linear types in mind, and the successful approach as implemented in GHC 9.0, the leading Haskell compiler, was based on Linear Haskell [**?**], where a linear type system designed with retaining backwards-compatibility and allowing code reuse across linear and non-linear users of the same libraries in mind was described. We describe Linear Haskell in detail in Section 2.3.

- Linear types permeate Haskell down to (its) **Core**, the intermediate language into which Haskell is translated. **Core** is a minimal, explicitly typed, functional language, on which multiple Core-to-Core optimizing transformations are defined. Due to Core's minimal design, typechecking Core programs is very efficient and doing so serves as a sanity check to the correction of the source transformations. If the resulting optimized Core program fails to typecheck, the optimizing transformations (are very likely to) have introduced an error in the resulting program. We present Core (and its formal basis, System F_C [**?**]) in Section 2.4.

Aligned with the philosophy of having a *typed* intermediate language, the integration of linearity in Haskell required extending **Core** with linear types. Just as a *typed* Core ensures that the translation from Haskell (dubbed *desugaring*) and the subsequent optimizing transformations are correctly implemented, a *linearly typed* Core guarantees that linear resource usage in the source language is not violated by the translation process and the compiler optimization passes. It is crucial that the program behaviour enforced by linear types is *not* changed by the compiler in the desugaring or optimization stages (optimizations should not destroy linearity!) and a linearity aware Core typechecker is key in providing such guarantees. Additionally, a linear Core can inform Core-to-Core optimizing transformations [**?**, **?**, **?**] in order to produce more performant programs.

While the current version of Core is linearity-aware (i.e., Core has so-called multiplicity annotations in variable binders), its type system does not (fully) validate the linearity constraints in the desugared program and essentially fails to type-check programs resulting from several optimizing transformations that are necessary to produce efficient object code. The reason for this latter point is not evidently clear: if we can typecheck linearity in the surface level Haskell why do we fail to do so in Core? The desugaring process from surface level Haskell to Core, and the subsequent Core-to-Core optimizing transformations, eliminate and rearrange most of the syntactic constructs through which linearity checking is performed – often resulting in programs completely different from the original.

However, these transformed programs that no longer type-check because of linearity are *semantically linear*, that is, linear resources are still used exactly once, despite the type-system no longer accepting those programs. In order to maintain Core linearly-typed accross transformations, Core must be extended with additional linearity information to allow type-checking linearity in Core where we currently do not.

Concluding, by extending Core / System F_C with linearity and multiplicity annotations such that we can desugar all of Linear Haskell and validate it accross transformations taking into consideration Core's call-by-need semantics, we can validate the surface level linear type's implementation, we can guarantee optimizing transformations do not destroy linearity, and we might be able to inform optimizing transformations with linearity.

Goals

From a high-level view, our goals for the dissertation include:

- Extending Core's type system and type-checking algorithm with additional linearity information in order to successfully type-check linearity in Core across transformations;
- Validating that our type-system accepts programs before and after each transformation is applied;
- Arguing the soundness of the resulting system (i.e. no semantically non-linear programs are deemed linear);
- Implementing our extensions to Core in GHC, the leading Haskell Compiler.

CHAPTER 2

Background and Related Work

In this section we review the concepts required to understand our work. In short, we discuss linear types, the Haskell programming language, linear types as they exist in Haskell (dubbed Linear Haskell), Haskell's main intermediate language (Core) and its formal foundation (System F_C) and, finally, an overview of GHC's pipeline with explanations of some Core-to-Core optimizing transformations.

2.1 Linear Types

Much the same way type systems can statically eliminate various kinds of programs that would fail at runtime, such as a program that derreferences an integer value rather than a pointer, linear type systems can guarantee that certain errors (regarding resource usage) are forbidden.

In linear type systems [**?**, **?**], so called linear resources must be used *exactly once*. Not using a linear resource at all or using said resource multiple times will result in a type error. We can model many real-world resources such as file handles, socket descriptors, and allocated memory, as linear resources. This way, because a file handle must be used exactly once, forgetting to close the file handle is a type error, and closing the handle twice is also a type error. With linear types, avoiding leaks and double frees is no longer a programmer's worry because the compiler can guarantee the resource is used exactly once, or *linearly*.

To understand how linear types are defined and used in practice, we present two examples of anonymous functions that receive a handle to work with (that must be closed before returning), we explore how the examples could be disregarded as incorrect, and work our way up to linear types from them. The first function ignores the received file handle and returns $\star$ (read unit), which is equivalent to C's `void`.

$$\lambda h.\ \mathsf{return}\ \star; \qquad\qquad \lambda h.\ \mathsf{close}\ h;\ \mathsf{close}\ h;$$

Ignoring the file handle which should have been closed by the function makes the first function incorrect. Similarly, the second function receives the file handle and closes it twice, which is incorrect not because it falls short of the specification, but rather because the program will crash while executing it. Additionally, both functions share the same type, `Handle` $\to \star$, i.e. a function that takes a `Handle` and returns $\star$. The second function also shares this type because `close` has type `Handle` $\to \star$. Under a simple type system

such as C's, both functions are type correct (the compiler will happily succeed), but both have erroneous behaviours. The first forgets to close the handle and the second closes it twice. Our goal is to reach a type system that rejects these two programs.

The key observation to invalidating these programs is to focus on the function type going between `Handle` and $\star$ and augment it to indicate that *the argument must be used exactly once*, or, in other words, that the argument of the function must be linear. We take the function type $A \to B$ and replace the function arrow ($\to$) with the linear function arrow ($\multimap$)[1] operator to denote a function that uses its argument exactly once: $A \multimap B$. Providing the more restrictive linear function signature `Handle` $\multimap \star$ to the example programs would make both of them fail to typecheck because they do not satisfy the linearity specification that the function argument should only be used exactly once.

In order to further give well defined semantics to a linear type system, we present a linearly typed lambda calculus [**?**, **?**], a very simple language with linear types, by defining what are syntatically valid programs through the grammar in Fig. 2.1 and what programs are well typed through the typing rules in Fig. 2.2. The language features functions and function application ($\multimap$), two flavours of pairs, additive (&) and multiplicative ($\otimes$), a disjunction operator ($\oplus$) to construct sum types, and the ! modality operator which constructs an unrestricted type from a linear one, allowing values inhabiting $!A$ to be consumed unrestrictedly. A typing judgement for the linearly typed lambda calculus has the form

$$\Gamma; \Delta \vdash M : A$$

where Γ is the context of resources that may be used unrestrictedly, that is, any number of times, Δ is the context of resources that must be used linearly (*exactly once*), M is the program to type and A is its type. When resources from the linear context are used, they are removed from the context and no longer available, and all resources in the linear context must be used exactly once.

$$\begin{array}{rcl} A, B & ::= & \star \\ & | & A \multimap B \\ & | & A \oplus B \\ & | & A \otimes B \\ & | & A \,\&\, B \\ & | & !A \end{array} \qquad \begin{array}{rcl} M, N & ::= & \star \mid \mathsf{let}\ \star = M\ \mathsf{in}\ N \\ & | & u \\ & | & \lambda u.M \mid M\ N \\ & | & \mathrm{inl}\ M \mid \mathrm{inr}\ M \\ & | & \mathsf{case}\ M\ \mathsf{of}\ \mathrm{inl}\ u_1 \to N_1; \mathrm{inr}\ u_2 \to N_2 \\ & | & M \otimes N \mid \mathsf{let}\ u_1 \otimes u_2 = M\ \mathsf{in}\ N \\ & | & M \,\&\, N \mid \mathrm{fst}\ M \mid \mathrm{snd}\ M \\ & | & !M \mid \mathsf{let}\ !u = M\ \mathsf{in}\ N \end{array}$$

Figure 2.1: Grammar for a linearly-typed lambda calculus

The function abstraction is typed according to the linear function introduction rule ($\multimap I$). The rule states that a a function abstraction, written $\lambda u.M$, is a linear function (i.e. has type $A \multimap B$) given the unrestricted context Γ and the linear context Δ, if the program M has type B given the same unrestricted context Γ and the linear context $\Delta, u{:}A$. That is, if M has type B using u of type A exactly once besides the other resources in Δ, then the lambda abstraction has the linear function type.

$$\frac{\Gamma; \Delta, u{:}A \vdash M : B}{\Gamma; \Delta \vdash \lambda u.M : A \multimap B}\ (\multimap I) \qquad \frac{\Gamma; \Delta \vdash M : A \multimap B \qquad \Gamma; \Delta' \vdash N : A}{\Gamma; \Delta, \Delta' \vdash M\ N : B}\ (\multimap E)$$

[1] Since linear types are born from a correspondence with linear logic [**?**] (the Curry-Howard isomorphism [**?**, **?**]), we borrow the $\multimap$ symbol and other linear logic connectives to describe linear types.

Function application is typed according to the elimination rule for the same type ($\multimap E$). To type an application $M\ N$ as B, M must have type $A \multimap B$ and N must have type A. To account for the linear resources that might be used while proving both that $M{:}A \multimap B$ and $N{:}A$, the linear context must be split in two such that both typing judgments succeed using exactly once every resource in their linear context (while the resources in Γ might be used unrestrictedly), hence the separation of the linear context in Δ and Δ'.

The multiplicative pair ($M \otimes N$) is constructed from two linearly typed expressions that can each be typed with a division of the given linear context, as we see in its introduction rule ($\otimes I$). Upon deconstruction, the multiplicative pair elimination rule ($\otimes E$) requires that both of the pair constituents be consumed exactly once.

$$\frac{\Gamma; \Delta \vdash M : A \qquad \Gamma; \Delta' \vdash N : B}{\Gamma; \Delta, \Delta' \vdash (M \otimes N) : A \otimes B}\ (\otimes I) \qquad \frac{\Gamma; \Delta \vdash M : A \otimes B \qquad \Gamma; \Delta', u{:}A, v{:}B \vdash N : C}{\Gamma; \Delta, \Delta' \vdash \mathsf{let}\ u \otimes v\ \mathsf{in}\ N : C}\ (\otimes E)$$

On the other hand, the additive pair requires that both elements of the pair can be proved with the same linear context, and upon deconstruction only one of the pair elements might be used, rather than both simultaneously.

Finally, the "of-course" operator (!) can be used to construct a resource that can be used unrestrictedly ($!M$). Its introduction rule ($!I$) states that to construct this resource means to add a resource to the unrestricted context, which can then be used freely. To construct an unrestricted value, however, the linear context *must be empty* – an unrestricted value can only be constructed if it does not depend on any linear resource.

$$\frac{\Gamma; \cdot \vdash M : A}{\Gamma; \cdot \vdash !M : !A}\ (!I) \qquad \frac{\Gamma; \Delta \vdash M : !A \qquad \Gamma, u{:}A; \Delta' \vdash N : C}{\Gamma; \Delta, \Delta' \vdash \mathsf{let}\ !u = M\ \mathsf{in}\ N : C}\ (!E)$$

To utilize an unrestricted value M, we must bind it to u with $\mathsf{let}\ !u = M\ \mathsf{in}\ N$ which can then be used in N unrestrictedly, because u extends the unrestricted context rather than the linear context as we have seen thus far.

In section 2.3 we describe how linear types are defined in Haskell, a programming language more featureful than the linearly typed lambda calculus. We will see that the theoretical principles underlying the linear lambda calculus and linear Haskell are the same, and by studying them in this minimal setting we can understand them at large.

2.2 Haskell

Haskell is a functional programming language defined by the Haskell Report [**?**, **?**] and whose *de-facto* implementation is GHC, the Glasgow Haskell Compiler [**?**]. Haskell is a *lazy*, *purely functional* language, i.e., functions cannot have side effects or mutate data, and, contrary to many programming languages, arguments are *not* evaluated when passed to functions, but rather are only evaluated when its value is needed. The combination of purity and laziness is unique to Haskell among mainstream programming languages.

Haskell is a large feature-rich language but its relatively small core is based on a typed lambda calculus. As such, there exist no statements and computation is done simply through the evaluation of functions. Besides functions, one can define types and their constructors and pattern match on said constructors. Function application is denoted by the juxtaposition of the function expression and its arguments, which often means empty space between terms (`f a` means `f` applied to `a`). Pattern matching is done with the `case` keyword followed by the enumerated alternatives. All variable names start with lower case

$$\frac{}{\Gamma; u{:}A \vdash u : A}\ (u) \qquad \frac{}{\Gamma, u{:}A; \cdot \vdash u : A}\ (u)$$

$$\frac{\Gamma; \Delta \vdash M : A \qquad \Gamma; \Delta' \vdash N : B}{\Gamma; \Delta, \Delta' \vdash (M \otimes N) : A \otimes B}\ (\otimes I) \qquad \frac{\Gamma; \Delta \vdash M : A \otimes B \qquad \Gamma; \Delta', u{:}A, v{:}B \vdash N : C}{\Gamma; \Delta, \Delta' \vdash \mathsf{let}\ u \otimes v\ \mathsf{in}\ N : C}\ (\otimes E)$$

$$\frac{\Gamma; \Delta, u{:}A \vdash M : B}{\Gamma; \Delta \vdash \lambda u.M : A \multimap B}\ (\multimap I) \qquad \frac{\Gamma; \Delta \vdash M : A \multimap B \qquad \Gamma; \Delta' \vdash N : A}{\Gamma; \Delta, \Delta' \vdash M\ N : B}\ (\multimap E)$$

$$\frac{\Gamma; \Delta \vdash M : A \qquad \Gamma; \Delta \vdash N : B}{\Gamma; \Delta \vdash M \,\&\, N : A \,\&\, B}\ (\&I) \qquad \frac{\Gamma; \Delta \vdash M : A \,\&\, B}{\Gamma; \Delta \vdash \mathrm{fst}\ M : A}\ (\&E_L) \qquad \frac{\Gamma; \Delta \vdash M : A \,\&\, B}{\Gamma; \Delta \vdash \mathrm{snd}\ M : B}\ (\&E_R)$$

$$\frac{\Gamma; \Delta \vdash M : A}{\Gamma; \Delta \vdash \mathrm{inl}\ M : A \oplus B}\ (\oplus I_L) \qquad \frac{\Gamma; \Delta \vdash M : B}{\Gamma; \Delta \vdash \mathrm{inr}\ M : A \oplus B}\ (\oplus I_R)$$

$$\frac{\Gamma; \Delta \vdash M : A \oplus B \qquad \Gamma; \Delta', w_1{:}A \vdash N_1 : C \qquad \Gamma; \Delta', w_2{:}B \vdash N_2 : C}{\Gamma; \Delta, \Delta' \vdash \mathsf{case}\ M\ \mathsf{of}\ \mathrm{inl}\ w_1 \to N_1 \mid \mathrm{inr}\ w_2 \to N_2 : C}\ (\oplus E)$$

$$\frac{}{\Gamma; \cdot \vdash \star : \star}\ (\star I) \qquad \frac{\Gamma; \Delta \vdash M : \star \qquad \Gamma; \Delta' \vdash N : B}{\Gamma; \Delta, \Delta' \vdash \mathsf{let}\ \star = M\ \mathsf{in}\ N : B}\ (\star E)$$

$$\frac{\Gamma; \cdot \vdash M : A}{\Gamma; \cdot \vdash !M : !A}\ (!I) \qquad \frac{\Gamma; \Delta \vdash M : !A \qquad \Gamma, u{:}A; \Delta' \vdash N : C}{\Gamma; \Delta, \Delta' \vdash \mathsf{let}\ !u = M\ \mathsf{in}\ N : C}\ (!E)$$

Figure 2.2: Typing rules for a linearly-typed lambda calculus

and types start with upper case (excluding type variables). To make explicit the type of an expression, the `::` operator is used (e.g. `f :: Int → Bool` is read `f` *has type* function from `Int` to `Bool`).

Because Haskell is a pure programming language, input/ouptut side-effects are modelled at the type-level through the non-nullary[2] type constructor `IO`. A value of type `IO a` represents a *computation* that when executed will perform side-effects and produce a value of type `a`. Computations that do I/O can be composed into larger computations using so-called monadic operators, which are like any other operators but grouped under the same abstraction. Some of the example programs will look though as if they had statements, but, in reality, the sequential appearence is just syntatic sugar to an expression using monadic operators. The main take away is that computations that do I/O may be sequenced together with other operations that do I/O while retaining the lack of statements and the language purity guarantees.

As an example, consider these functions that do I/O and their types. The first opens a file by path and returns its handle, the second gets the size of a file from its handle, and the third closes the handle. It is important that the handle be closed exactly once, but currently nothing enforces that usage policy.

```
openFile :: FilePath → IOMode → IO Handle
hFileSize :: Handle → IO Integer
hClose :: Handle → IO ()
```

The following function makes use of the above definitions to return the size of a file

[2] `IO` has kind `Type → Type`, that is, it is only a type after another type is passed as a parameter (e.g. `IO Int`, `IO Bool`); `IO` by itself is a *type constructor*

given its path. Note that the function silently leaks the handle to the file, despite compiling successfully.

```
countWords :: FilePath → IO Integer
countWords path = do
  handle ← openFile path ReadMode
  size ← hFileSize handle
  return size
```

Another defining feature of Haskell is its powerful type system. In contrast to most mainstream programming languages, such as OCaml and Java, Haskell supports a myriad of advanced type level features, such as:

- Multiple forms of advanced polymorphism: where languages with whole program type inference usually stick to Damas–Hindley–Milner type inference [**?**], Haskell goes much further with, e.g., arbitrary-rank types [**?**], type-class polymorphism [**?**], levity polymorphism [**?**], multiplicity polymorphism [**?**], and, more recently, impredicative polymorphism [**?**].
- Type level computation by means of type classes [**?**] and Haskell's type families [**?**, **?**, **?**], which permit a direct encoding of type-level functions resembling rewrite rules.
- Local equality constraints and existential types by using GADTs, which we explain ahead in more detail. A design for first class existential types with bi-directional type inference in Haskell has been published in [**?**], despite not being yet implemented in GHC.

These advanced features have become commonplace in Haskell code, enforcing application level invariants and program correctness through the types. As an example to work through this section while we introduce compile-time invariants with GADTs, consider the definition of `head` in the standard library, a function which takes the first element of a list by pattern matching on the list constructors.

```
head :: [a] → a
head [] = error "List is empty!"
head (x : xs) = x
```

When applied to the empty list, `head` terminates the program with an error. This function is unsafe – our program might crash if we use it on an invalid input. Leveraging Haskell's more advanced features, we can use more expressive types to assert properties about the values and get rid of the invalid cases (e.g. we could define a `NonEmpty` type to model a list that can not be empty). A well liked motto is "make invalid states unrepresentable". In this light, we introduce Generalized Algebraic Data Types (GADTs) and create a list type indexed by size for which we can write a completely safe `head` function by expressing that the size of the list must be at least one, at the type level.

2.2.1 Generalized Algebraic Data Types

GADTs [**?**, **?**, **?**] are an advanced Haskell feature that allows users to define data types as they would common algebraic data types, with the added abilitiy to give explicit type signatures for the data constructors where the result type may differ in the type parameters (e.g., we might have two constructors of the same data type `T a` return values of type

`T Bool` and `T Int`). This allows for additional type invariants to be represented with GADTs through their type parameters, which restricts the use of specific constructors and their subsequent deconstruction through pattern matching. Pattern matching against GADTs can introduce local type refinements, that is, refines the type information used for typechecking individual case alternatives. We develop the length-indexed lists example without discussing the type system and type inference details of GADTs as desribed in [**?**].

We define the data type in GADT syntax for length-index lists which takes two type parameters. The first type parameter is the length of the list and the type of the type parameter (i.e. the kind of the first type parameter) is `Nat`. To construct a type of kind `Nat` we can only use the type constructors `Z` and `S`. The second type parameter is the type of the values contained in the list, and any type is valid, hence the `Type` kind.

```
data Vec (n :: Nat) (a :: Type) where
  Nil :: Vec Z a
  Cons :: a → Vec m a → Vec (S m) a
```

The length-indexed list is defined inductively as either an empty list *of size zero*, or the construction of a list by appending a new element to an existing list *of size m* whose final size is $m + 1$ (`S m`). The list `Cons 'a' (Cons 'b' Nil)` has type `Vec (S (S Z)) Char` because `Nil` has type `Vec Z Char` and `Cons 'a' Nil` has type `Vec (S Z) Char`. GADTs make possible different data constructors being parametrized over different type parameters as we do with `Vec`'s size parameter being different depending on the constructor that constructs the list.

To define the safe `head` function, we must specify the type of the input list taking into account that the size must not be zero. To that effect, the function takes as input a `Vec (S n) a`, that is, a vector with size (n+1) for all possible n's, making a call to `head` on a list of type `Vec Z a` (an empty list) a compile-time type error.

```
head :: Vec (S n) a → a
head (Cons x xs) = x
```

Pattern matching on the `Nil` constructor is not needed, despite it being a constructor of `Vec`. The argument type doesn't match the type of the `Nil` constructor (`S n` $\neq$ `Z`), so the corresponding pattern case alternative is innacessible because the typechecker does not allow calling `head` on `Nil` (once again, its type, `Vec Z a`, does not match the input type of `head`, `Vec (S n) a`).

In practice, the idea of using more expressive types to enforce invariants at compile time, that is illustrated by this simple example, can be taken much further, e.g., to implement type-safe artificial neural networks[**?**], enforce size compatibility in operations between matrices and vectors[**?**], to implement red-black trees guaranteeing its invariants at compile-time, or to implement a material system in a game engine[**?**].

Linear types are, similarly, an extension to Haskell's type system that makes it even more expressive, by providing a finer control over the usage of certain resources at the type level.

2.3 Linear Haskell

The introduction of linear types to Haskell's type system is originally described in Linear Haskell [**?**]. While in Section 2.6 we discuss the reasoning and design choices behind retrofitting linear types to Haskell, here we focus on linear types solely as they exist in

the language, and re-work the file handle example seen in the previous section to make sure it doesn't typecheck.

A linear function ($f :: A \multimap B$) guarantees that if ($f\ x$) is consumed exactly once, then the argument x is consumed exactly once. The precise definition of *consuming a value* depends on the value as follows, paraphrasing Linear Haskell [**?**]:

- To consume a value of atomic base type (such as `Int` or `Ptr`) exactly once, just evaluate it.
- To consume a function value exactly once, apply it to one argument, and consume its result exactly once.
- To consume a value of an algebraic datatype exactly once, pattern-match on it, and consume all its linear components exactly once. For example, a linear pair (equivalent to $\otimes$) is consumed exactly once if pattern-matched on *and* both the first and second element are consumed once.

In Haskell, linear types are introduced through *linearity on the function arrow*. In practice, this means function types are annotated with a linearity that defines whether a function argument must be consumed *exactly once* or whether it can be consumed *unrestrictedly* (many times). As an example, consider the function f below, which doesn't typecheck because it is a linear function (annotated with `1`) that consumes its argument more than once, and the function g, which is an unrestricted function (annoted with `Many`) that typechecks because its type allows the argument to be consumed unrestrictedly.

```
f :: a %1 -> (a, a)
f x = (x, x)
```

```
g :: a %Many -> (a, a)
g x = (x, x)
```

The function annotated with the *multiplicity* annotation of `1` is equivalent to the linear function type ($\multimap$) seen in the linear lambda calculus (Section 2.1). Additionally, algebraic data type constructors can specify whether their arguments are linear or unrestricted, requiring that, when pattern matched on, linear arguments be consumed once while unrestricted arguments need not be consumed exactly once. To encode the multiplicative linear pair ($\otimes$) we must create a pair data type with two linear components. To consume an algebraic data type is to consume all its linear components once, so, to consume said pair data type, we need to consume both its linear components – successfully encoding the multiplicative pair elimination rule ($\otimes E$). To construct said pair data type we must provide two linear elements, each consuming some required resources to be constructed, thus encoding the multiplicative pair introduction rule ($\otimes I$). As such, we define `MultPair` as an algebraic data type whose constructor uses a linear arrow for each of the arguments[3].

```
data MultPair a b where
  MkPair :: a %1 -> b %1 -> MultPair a b
```

The linearity annotations `1` and `Many` are just a specialization of the more general so-called *multiplicity annotations*. A multiplicity of `1` entails that the function argument must be consumed once, and a function annotated with it ($\rightarrow_1$) is called a linear function (often written with $\multimap$). A function with multiplicity of `Many` ($\rightarrow_\omega$) is an unrestricted function,

[3] By default, constructors defined without GADT syntax have linear arguments. We could have written `data MultPair a b = MkPair a b` to the same effect.

which may consume its argument 0 or more times. Unrestricted functions are equivalent to the standard function type and, in fact, the usual function arrow ($\rightarrow$) implicitly has multiplicity `Many`. Multiplicities naturally allow for *multiplicity polymorphism*, which we explain below.

Consider the functions f and g which take as an argument a function from `Bool` to `Int`. Function f expects a linear function ($Bool \ \rightarrow_1 \ Int$), whereas g expects an unrestricted function ($Bool \ \rightarrow_\omega \ Int$). Function h is a function from `Bool` to `Int` that we want to pass as an argument to both f and g.

```
f :: (Bool % 1 → Int) → Int
f c = c True
g :: (Bool → Int) → Int
g c = c False
```

```
h :: Bool % m → Int
h x = case x of
  False → 0
  True → 1
```

For the application of f and g to h to be well typed, the multiplicity of h ($\rightarrow_?$) should match the multiplicity of both f ($\rightarrow_1$) and g ($\rightarrow_\omega$). Multiplicity polymorphism allows us to use *multiplicity variables* when annotating arrows to indicate that the function can both be typed as linear and as an unrestricted function, much the same way type variables can be used to define polymorphic functions. Thus, we define h as a multiplicity polymorphic function ($\rightarrow_m$), making h a well-typed argument to both f and g (m will unify with 1 and ω at the call sites).

2.4 Core and System F_C

Haskell is a large and expressive language with many syntatic constructs and features. However, the whole of Haskell can be desugared down to a minimal, explicitly typed, intermediate language called **Core**. Desugaring allows the compiler to focus on the small desugared language rather than on the large surface one, which can greatly simplify the subsequent compilation passes. Core is a strongly-typed, lazy, purely functional intermediate language akin to a polymorphic lambda calculus, that GHC uses as its key intermediate representation. To illustrate the difference in complexity, in GHC's implementation of Haskell, the abstract syntax tree is defined through dozens of datatypes and hundreds of constructors, while the GHC's implementation of Core is defined in 3 types (expressions, types, and coercions) and 15 constructors [**?**]. The existence of Core and its use is a major design decision in GHC Haskell with significant benefits which have proved themselves in the development of the compiler.

- Core allows us to reason about the entirety of Haskell in a much smaller functional language. Performing analysis, optimizing transformations, and code generation is done on Core, not Haskell. The implementation of these compiler passes is significantly simplified by the minimality of Core.

- Since Core is an (explicitly) typed language (c.f. System F [**?**, **?**]), type-checking Core serves as an internal consistency check for the desugaring and optimization passes. The Core typechecker provides a verification layer for the correctness of desugaring and optimizing transformations (and their implementations) because both desugaring and optimizing transformations must produce well-typed Core.

- Finally, Core's expressiveness serves as a sanity-check for all the extensions to the source language – if we can desugar a feature into Core then the feature must be

sound by reducibility. Effectively, any feature added to Haskell is only syntatic sugar if it can be desugared to Core.

The implementation of Core's typechecker differs significantly from the Haskell typechecker because Core is explicitly typed and its type system is based on the *System* F_C [**?**] type system (i.e., System F extended with a notion of type coercion), while Haskell is implicitly typed and its type system is based on the constraint-based type inference system *OutsideIn*(X) [**?**]. Therefore, typechecking Core is simple, fast and requires no type inference, whereas Haskell's typechecker must account for almost the entirety of Haskell's syntax, and must perform type-inference in the presence of arbitrary-rank polymorphism, existential types, type-level functions, and GADTs, which are known to introduce significant challenges for type inference algorithms [**?**]. Haskell is typechecked in addition to Core to elaborate the user program. This might involve performing type inference to make implicit types explicit and solving constraints to pass implicit dictionary arguments explicitly. Furthermore, type-checking the source language allows us to provide meaningful type errors. If Haskell wasn't typechecked and instead we only typechecked Core, everything (e.g. all binders) would have to be explicitly typed and type error messages would refer to the intermediate language rather than the written program.

The Core language is based on *System* F_C, a polymorphic lambda calculus with explicit type-equality coercions that, like types, are erased at compile time (i.e. types and coercions alike don't incur any cost at run-time). The syntax of System F_C [**?**] terms is given in Figure 2.3, which corresponds exactly to the syntax of System F [**?**, **?**] with term and (kind-annotated) type abstraction as well as term and type application, extended with algebraic data types, let-bound expressions, pattern matching and coercions or casts.

u	::=	$x \mid K$	Variables and data constructors
e	::=	u	Term atoms
	$\mid$	$\Lambda a{:}\kappa.\ e \mid e\ \varphi$	Type abstraction/application
	$\mid$	$\lambda x{:}\sigma.\ e \mid e_1\ e_2$	Term abstraction/application
	$\mid$	$\mathsf{let}\ x{:}\sigma = e_1\ \mathsf{in}\ e_2$	
	$\mid$	$\mathsf{case}\ e_1\ \mathsf{of}\ \overline{p \to e_2}$	
	$\mid$	$e \blacktriangleright \gamma$	Cast
p	::=	$K\ \overline{b{:}\kappa}\ \overline{x{:}\sigma}$	Pattern

Figure 2.3: System F_C's Terms

Explicit type-equality coercions (or simply coercions), written $\sigma_1 \sim \sigma_2$, serve as evidence of equality between two types σ_1 and σ_2. A coercion $\sigma_1 \sim \sigma_2$ can be used to safely *cast* an expression e of type σ_1 to type σ_2, where casting e to σ_2 using $\sigma_1 \sim \sigma_2$ is written $e \blacktriangleright \sigma_1 \sim \sigma_2$. The syntax of *coercions* is given by Figure 2.4 and describes how coercions can be constructed to justify new equalities between types (e.g. using symmetry and transitivity). For example, given $\tau \sim \sigma$, the coercion $\mathbf{sym}\ (\tau \sim \sigma)$ denotes a type-equality coercion from σ to τ using the axiom of symmetry of equality. Through it, the expression $e{:}\sigma$ can be cast to $e{:}\tau$, i.e. $(e{:}\sigma \blacktriangleright \mathbf{sym}\ \tau \sim \sigma) : \tau$.

System F_C's coercions are key in desugaring advanced type-level Haskell features such as GADTs, type families and newtypes [**?**]. In short, these three features are desugared as follows:

$$
\begin{array}{lcll}
\sigma, \tau & ::= & d \mid \tau_1\ \tau_2 \mid S_n\ \overline{\tau}^n \mid \forall a{:}\kappa.\tau & \text{Types} \\
\gamma, \delta & ::= & g \mid \tau \mid \gamma_1\ \gamma_2 \mid S_n\ \overline{\gamma}^n \mid \forall a{:}\kappa.\gamma & \text{Coercions} \\
 & \mid & \mathbf{sym}\ \gamma \mid \gamma_1 \circ \gamma_2 \mid \gamma@\sigma \mid \mathbf{left}\ \gamma \mid \mathbf{right}\ \gamma & \\
\varphi & ::= & \tau \mid \gamma & \text{Types and Coercions}
\end{array}
$$

Figure 2.4: System F_C's Types and Coercions

- GADTs local equality constraints are desugared into explicit type-equality evidence that are pattern matched on and used to cast the branch alternative's type to the return type.

- Newtypes such as `newtype BoxI = BoxI Int` introduce a global type-equality `BoxI` $\sim$ `Int` and construction and deconstruction of said newtype are desugared into casts.

- Type family instances such as `type instance F Int = Bool` introduce a global coercion `F Int` $\sim$ `Bool` which can be used to cast expressions of type `F Int` to `Bool`.

Core further extends *System* F_C with *jumps* and *join points* [**?**], allowing new optimizations to be performed which ultimately result in efficient code using labels and jumps, and with a construct used for internal notes such as profiling information.

In the context of Linear Haskell, and recalling that Haskell is fully desugared into Core / System F_C as part of its validation and compilation strategy, we highlight the inherent incompatibility of linearity with Core / System F_C as a current flaw in GHC that invalidates all the benefits of Core wrt linearity. Thus, we must extend System F_C (and, therefore, Core) with linearity in order to adequately validate the desugaring and optimizing transformations as linearity preserving, ensuring we can reason about Linear Haskell in its Core representation.

2.5 GHC Pipeline

The GHC compiler processes Haskell source files in a series of phases that feed each other in a pipeline fashion, each transforming their input before passing it on to the next stage. This pipeline is crucial in the overall design of GHC. We now give a high-level overview of the phases.

2.5.1 Haskell to Core

Parser. The Haskell source files are first processed by the lexer and the parser. The lexer transforms the input file into a sequence of valid Haskell tokens. The parser processes the tokens to create an abstract syntax tree representing the original code, as long as the input is a syntactically valid Haskell program.

Renamer. The renamer's main tasks are to resolve names to fully qualified names, resolve name shadowing, and resolve namespaces (such as the types and terms namespaces), taking into consideration both existing identifiers in the module being compiled and identifiers exported by other modules. Additionally, name ambiguity, variables out of scope, unused bindings or imports, etc., are checked and reported as errors or warnings.

Type-checker. With the abstract syntax tree validated by the renamer and with the names fully qualified, the Haskell program is type-checked before being desugared into Core. Type-checking the Haskell program guarantees that the program is well-typed. Otherwise, type-checking fails with an error reporting where in the source typing failed. Furthermore, every identifier in the program is annotated with its type. Haskell is an implicitly typed language and, as such, type-inference must be performed to type-check programs. During type inference, every identifier is typed and we can use its type to decorate said identifier in the abstract syntax tree produced by the type-checker. First, annotating identifiers is *required* to desugar Haskell into Core because Core is explicitly typed – to construct a Core abstract syntax tree the types are indispensable (i.e. we cannot construct a Core expression without explicit types). Secondly, names annotated with their types are useful for tools manipulating Haskell, e.g. for an IDE to report the type of an identifier.

Desugaring. The type-checked Haskell abstract syntax tree is then transformed into Core by the desugarer. We've discussed in Section 2.4 the relationship between Haskell and Core in detail, so we refrain from repeating it here. It suffices to say that the desugarer transforms the large Haskell language into the small Core language by simplifying all syntactic constructs to their equivalent Core form (e.g. `newtype` constructors are transformed into coercions).

2.5.2 Core-To-Core Transformations

The Core-to-Core transformations are the most important set of optimizing transformations that GHC performs during compilation. By design, the frontend of the pipeline (parsing, renaming, typechecking and desugaring) does not include any optimizations – all optimizations are done in Core. The transformational approach focused on Core, known as *compilation by transformation*, allows transformations to be both modular and simple. Each transformation focuses on optimizing a specific set of constructs, where applying a transformation often exposes opportunities for other transformations to fire. Since transformations are modular, they can be chained and iterated in order to maximize the optimization potential (as shown in Figure 2.5).

However, due to the destructive nature of transformations (i.e. applying a transformation is not reversible), the order in which transformations are applied determines how well the resulting program is optimized. As such, certain orderings of optimizations can hide optimization opportunities and block them from firing. This phase-ordering problem is present in most optimizing compilers.

Foreshadowing the fact that Core is the main object of our study, we want to type-check linearity in Core before *and* after each optimizing transformation is applied (Section 2.4). In that light, we describe below some of the individual Core-to-Core transformations, using $\Longrightarrow$ to denote a program transformation. In the literature, the first set of Core-to-Core optimizations was described in [**?**, **?**]. These were subsequently refined and expanded [**?**, **?**, **?**, **?**, **?**]. In Figure 2.5 we present an example that is optimized by multiple transformations to highlight how the compilation by transformation process produces performant programs.

Inlining. Inlining is an optimization common to all compilers, but especially important in functional languages [**?**]. Given Haskell's pure and lazy semantics, inlining can be employed in Haskell to a much larger extent because we needn't worry about evaluation

order or side effects, contrary to most imperative and strict languages. *Inlining* consists of replacing an occurrence of a let-bound variable by its right-hand side:

$$\mathsf{let}\ x = e\ \mathsf{in}\ \ldots x \ldots \implies \mathsf{let}\ x = e\ \mathsf{in}\ \ldots e \ldots$$

Effective inlining is crucial to optimization because, by bringing the definition of a variable to the context in which it is used, many other local optimizations are unlocked. The work [**?**] further discusses the intricacies of inlining and provides algorithms used for inlining in GHC.

***β*-reduction.** β-reduction is an optimization that consists of reducing an application of a term λ-abstraction or type-level Λ-abstraction (Figure 2.3) by replacing the λ-bound variable with the argument the function is applied to:

$$(\lambda x{:}\tau.\ e)\ y \implies e[y/x] \qquad (\Lambda a{:}\kappa.\ e)\ \varphi \implies e[\varphi/a]$$

If the λ-bound variable is used more than once in the body of the λ-abstraction we must be careful not to duplicate work, and we can let-bound the argument, while still removing the λ-abstraction, to avoid doing so:

$$(\lambda x{:}\tau.\ e)\ y \implies \mathsf{let}\ x = y\ \mathsf{in}\ e$$

β-reduction is always a good optimization because it effectively evaluates the application at compile-time (reducing heap allocations and execution time) and unlocks other transformations.

Case-of-known-constructor. If a `case` expression is scrutinizing a known constructor $K\ \overline{x{:}\sigma}$, we can simplify the case expression to the branch it would enter, substituting the pattern-bound variables by the known constructor arguments ($\overline{x{:}\sigma}$):

$$\begin{array}{l}\textbf{case}\ K\ v_1\ \ldots\ v_n\ \textbf{of} \\ \quad K\ x_1\ \ldots\ x_n \to e \quad \implies e[v_i/x_i]_{i=1}^{n} \\ \quad \ldots\end{array}$$

Case-of-known-constructor is an optimization mostly unlocked by other optimizations such as inlining and β-reduction, more so than by code written as-is by the programmer. As β-reduction, this optimization is also always good – it eliminates evaluations whose result is known at compile time and further unblocks for other transformations.

Let-floating. A let-binding in Core entails performing *heap-allocation*, therefore, let-related transformations directly impact the performance of Haskell programs. In particular, let-floating transformations are concerned with best the position of let-bindings in a program in order to improve efficiency. Let-floating is an important group of transformations for non-strict (lazy) languages described in detail by [**?**]. We distinguish three let-floating transformations:

- *Float-in* consists of moving a let-binding as far *inwards* as possible. For example, it could be moving a let-binding outside of a case expression into the branch alternative that uses the let-bound variable:

$$\begin{array}{l}\mathsf{let}\ x = y + 1 \\ \ \mathsf{in\ case}\ z\ \mathsf{of} \\ \ \ [] \to x * x \\ \ \ (p : ps) \to 1\end{array} \implies \begin{array}{l}\mathsf{case}\ z\ \mathsf{of} \\ \ \ [] \to \mathsf{let}\ x = y + 1\ \mathsf{in}\ x * x \\ \ \ (p : ps) \to 1\end{array}$$

This can improve performance by not performing let-bindings (e.g. if the branch the let was moved into is never executed); improving strictness analysis; and further unlocking other optimizations such as [**?**]. However, care must be taken when floating a let-binding inside a λ-abstraction because every time that abstraction is applied the value (or thunk) of the binding will be allocated in the heap.

- *Full laziness* transformation, also known as *float-out*, consists of moving let-bindings outside of enclosing λ-abstractions. The warning above regarding λ-abstractions recomputing the binding every time they are applied is valid even if bindings are not purposefully pushed inwards. In such a situation, floating the let binding out of the enclosing lambda can make it readily available across applications of said lambda.

- The *local transformations* are the third type of let-floating optimizations. In this context, the local transformations are local rewrites that improve the placement of bindings. There are three local transformations:

  1. $(\mathsf{let}\ v = e\ \mathsf{in}\ b)\ a \implies \mathsf{let}\ v = e\ \mathsf{in}\ b\ a$
  2. $\mathsf{case}\ (\mathsf{let}\ v = e\ \mathsf{in}\ b)\ \mathsf{of}\ \ldots \implies \mathsf{let}\ v = e\ \mathsf{in}\ \mathsf{case}\ b\ \mathsf{of}\ \ldots$
  3. $\mathsf{let}\ x = (\mathsf{let}\ v = e\ \mathsf{in}\ b)\ \mathsf{in}\ c \implies \mathsf{let}\ v = e\ \mathsf{in}\ \mathsf{let}\ x = b\ \mathsf{in}\ c$

  These transformations do not change the number of allocations but potentially create opportunities for other optimizations to fire, such as expose a lambda abstraction [**?**].

η-expansion and η-reduction. η-expansion is a transformation that expands a function expression f to $(\lambda x.f\ x)$, where x is not free in f. This transformation can improve efficiency because it can fully apply functions which would previously be partially applied by using the variable bound to the expanded λ. A partially applied function is often more costly than a fully saturated one because it entails a heap allocation for the function closure, while a fully saturated one equates to a function call. η-reduction is the inverse transformation to η-expansion, i.e., a λ-abstraction $(\lambda x.f\ x)$ can be η-reduced to simply f.

Case-of-case. The case-of-case transformation fires when a case expression is scrutinizing another case expression. In this situation, the transformation duplicates the outermost case into each of the inner case branches:

$$\mathsf{case}\ \left(\begin{array}{c}\mathsf{case}\ e_c\ \mathsf{of}\\ alt_{c_1} \to e_{c_1}\\ \cdots\\ alt_{c_n} \to e_{c_n}\end{array}\right)\ \mathsf{of}\ \begin{array}{l} alt_1 \to e_1\\ \cdots\\ alt_n \to e_n\end{array} \implies \begin{array}{l}\mathsf{case}\ e_c\ \mathsf{of}\\ alt_{c_1} \to \left(\begin{array}{c}\mathsf{case}\ e_{c_1}\ \mathsf{of}\\ alt_1 \to e_1\\ \cdots\\ alt_n \to e_n\end{array}\right)\\ \cdots\\ alt_{c_n} \to \left(\begin{array}{c}\mathsf{case}\ e_{c_n}\ \mathsf{of}\\ alt_1 \to e_1\\ \cdots\\ alt_n \to e_n\end{array}\right)\end{array}$$

This transformation exposes other optimizations, e.g., if e_{c_n} is a known constructor we can readily apply the *case-of-known-constructor* optimization. However, this transformation also potentially introduces significant code duplication. To this effect, we apply a transformation that creates *join points* (i.e., shared bindings outside the case expressions that are used in the branch alternatives) that are compiled to efficient code using labels and jumps.

Common sub-expression elimination. Common sub-expression elimination (CSE) is a transformation that is effectively inverse to *inlining*. This transformation factors out expensive expressions into a shared binding. In practice, lazy functional languages don't benefit nearly as much as strict imperative languages from CSE and, thus, it isn't very important in GHC [**?**].

Static argument and lambda lifting. *Lambda lifting* is a transformation that abstracts over free variables in functions by making them λ-bound arguments [**?**, **?**]. This allows functions to be "lifted" to the top-level of the program (because they no longer have free variables). Lambda lifting may unlock inlining opportunities and allocate less function closures, since the definition is then created only once at the top-level and shared across uses. The *static argument* transformation identifies function arguments which are *static* across calls, and eliminates said *static argument* to avoid passing the same fixed value as an argument in every function call, which is especially significant in recursive functions. To this effect, the *static argument* is bound outside of the function definition and becomes a free variable in its body. It can be thought of as the transformation inverse to *lambda lifting*.

Strictness analysis and worker/wrapper split. The strictness analysis, in lazy programming languages, identifies functions that always evaluate their arguments, i.e. functions with (morally) *strict arguments*. Arguments passed to functions that necessarily evaluate them can be evaluated before the call and therefore avoid some heap allocations. The strictness analysis may be used to apply the worker/wrapper split transformation [**?**]. This transformation creates two functions from an original one: a worker and a wrapper. The worker receives unboxed values [**?**] as arguments, while the wrapper receives boxed values, unwraps them, and simply calls the worker function (hence the wrapper being named as such). This allows the worker to be called in expressions other than the wrapper, saving allocations and being possibly much faster, especially if the worker recursively ends up calling itself rather than the wrapper.

2.5.3 Code Generation

The code generation needn't be changed to account for the work we will do in the context of this thesis, so we only briefly describe it.

After the core-to-core pipeline is run on the Core program and produces optimized Core, the program is translated down to the Spineless Tagless G-Machine (STG) language [**?**]. STG language is a small functional language that serves as the abstract machine code for the STG abstract machine that ultimately defines the evaluation model and compilation of Haskell through operational semantics.

From the abstract state machine, we generate C-- (read C minus minus), a C-like language designed for native code generation, which is finally passed as input to one of the code generation backends[4], such as LLVM, x86 and x64, or (recently) JavaScript and WebAssembly.

[4]GHC is not *yet* runtime retargetable, i.e. to use a particular native code generation backend the compiler must be built targetting it.

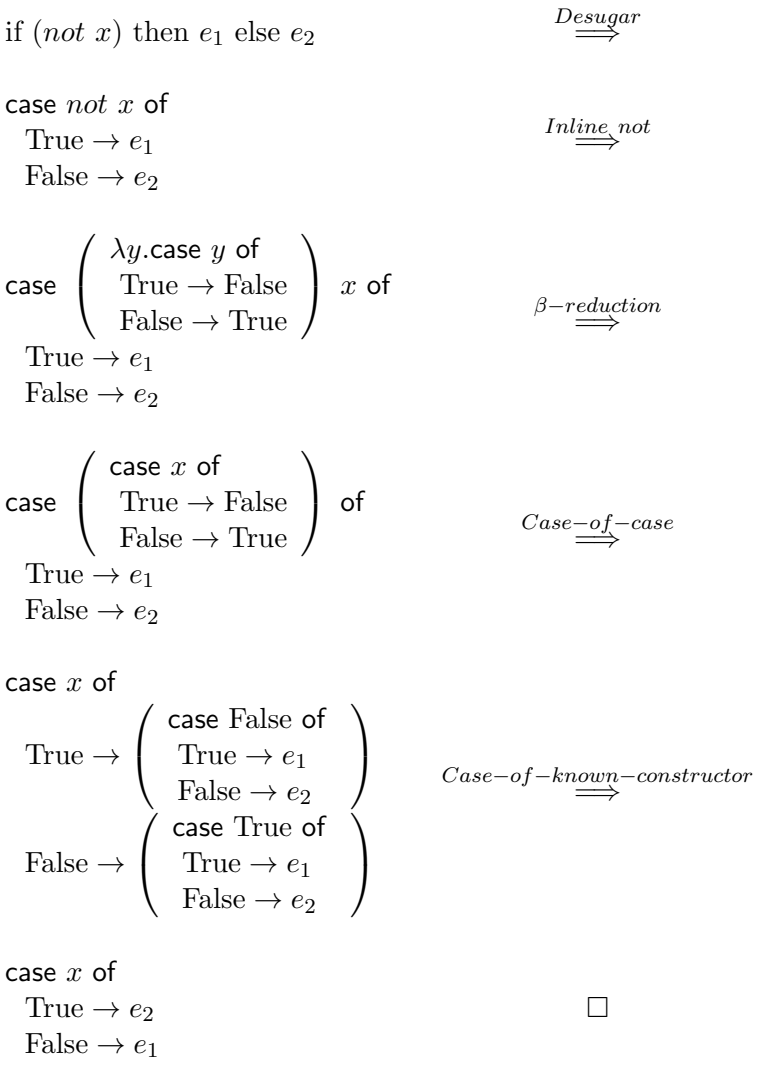

Figure 2.5: Example sequence of transformations

2.6 Related Work

Formalization of Core System F_C [**?**] (Section 2.4) does not account for linearity in its original design, and, to the best of our knowledge, no extension to System F_C with linearity and non-strict semantics exists. As such, there exists no formal definition of Core that accounts for linearity. In this context, we intend to introduce a linearly typed System F_C with multiplicity annotations and typing rules to serve as a basis for a linear Core. Critically, this Core linear language must account for call-by-need evaluation semantics and be valid in light of Core-to-Core optimizing transformations.

Linear Haskell Haskell, contrary to most programming languages with linear types, has existed for 31 years of its life *without* linear types. As such, the introduction of linear types to Haskell comes with added challenges that do not exist in languages that were designed with linear types from the start:

- Backwards compatibility. The addition of linear types shouldn't break all existing Haskell code.

- Code re-usability. The linearly-typed part of Haskell's ecosystem and its non-linearly-typed counterpart should fit in together and it must be possible to define functions readily usable by both sides simultaneously.
- Future-proofing. Haskell, despite being an industrial-strength language, is also a petri-dish for experimentation and innovation in the field of programming languages. Therefore, Linear Haskell takes care to accomodate possible future features, in particular, its design is forwards compatible with affine and dependent types.

Linear Haskell [**?**] is thus concerned with retrofitting linear types in Haskell, taking into consideration the above design goals, but is not concerned with extending Haskell's intermediate language(s), which presents its own challenges.

Nonetheless, while the Linear Haskell work keeps Core unchanged, its implementation in GHC does modify and extend Core with linearity/multiplicity annotations, and said extension of Core with linear types does not account for optimizing transformations and the non-strict semantics of Core.

Our work on linear Core intends to overcome the limitations of linear types as they exist in Core, i.e. integrating call-by-need semantics and validating the Core-to-Core passes, ultimately doubling as a validation of the implementation of Linear Haskell.

Linearity-influenced optimizations Core-to-Core transformations appear in many works across the research literature [**?**, **?**, **?**, **?**, **?**, **?**, **?**, **?**], all designed in the context of a typed language (Core) which does not have linear types. However, [**?**, **?**, **?**] observe that certain optimizations (in particular, let-floating and inlining) greatly benefit from linearity analysis and, in order to improve those transformation, linear-type-inspired systems were created specifically for the purpose of the transformation.

By fully supporting linear types in Core, these optimizing transformations could be informed by the language inherent linearity, and, consequently, avoid an ad-hoc or incomplete linear-type inference pass custom-built for optimizations. Additionally, the linearity information may potentially be used to the benefit of optimizing transformations that currently don't take any linearity into account.

CHAPTER 3

Proposed Work

3.1 Motivation

Since the publication of Linear Haskell [**?**] and its implementation in GHC 9.0, Haskell's type system supports linearity annotations in functions. Linear Haskell effectively brings linear types to a mainstream, pure, and lazy functional language. Concretely, Haskell function types can be annotated with a multiplicity, where a multiplicity of `1` requires the argument to be consumed exactly once and a multiplicity of `Many` allows the function argument to be consumed unrestrictedly, i.e., zero or more times.

As mentioned in Section 2.4, GHC Haskell features two typed languages in its pipeline: Haskell and its main intermediate language, Core (Core is a much smaller language than the whole of Haskell, even though we can compile the whole of Haskell to Core). The addition of linear types to GHC Haskell required changing the type system of both languages. However, Linear Haskell only describes an extension to the surface-level Haskell type system, not Core. Nonetheless, in practice, Core is linearity-aware.

We want Core and its type system to give us guarantees about desugaring and optimizing transformations with regard to linearity just as Core does for types – a linearly typed Core ensures that linearly-typed programs remain correct both after desugaring and across all GHC optimizing transformations, i.e. linearity is preserved when desugaring and optimisations should not destroy linearity.

In this sense, Core is already annotated with linearity, but its type-checker **currently ignores linearity annotations**. In spite of the strong formal foundations of linear types driving the implementation, their interaction with the whole of GHC is still far from trivial. The implemented type system cannot accomodate several optimising transformations that produce programs which violate linearity *syntactically* (i.e. multiple occurrences of linear variables in the program text), but ultimately preserve it in a *semantic* sense, where a linear term is still *consumed exactly once* – this is compounded by lazy evaluation driving a non-trivial mismatch between syntactic and semantic linearity.

Consider the example in Figure 3.1, an expression in which y and z are variables bound by a λ-abstraction, and both are annotated with a multiplicity of `1`. Note that let-binding x doesn't necessarily consume y and z because of Core's call-by-need semantics. In the example, it might not seem as though y and z are both being consumed linearly but, in fact, they both are. Given that in the first branch we use x – which entails using y and z linearly – and in the second branch we use y and z directly, in both branches we are consuming both y and z linearly.

```
let x = (y, z) in
case e of
  Pat1 → ... x ...
  Pat2 → ... y ... z ...
```

Figure 3.1: Example Inlining

Similarly, consider the program in Figure 3.1 with a let-binding that uses x, a linearly bound λ-variable. In surface level Haskell, let-bindings always consume linear variables `Many` times to avoid dealing with the complexity of call-by-need semantics, so this program would not type-check, because x is being consumed `Many` times instead of `1`. Despite not

```
f :: a %1 → a
f x = let y = x + 2 in y
```

Figure 3.2: Example Let

being accepted by the surface-level language, linear programs using lets occur naturally in Core due to optimising transformations that create let bindings, such as β-reduction. In a similar fashion, programs which violate syntatic linearity for other reasons other than let bindings are produced by Core transformations.

The current solution to valid programs being rejected by Core's linear type-checker is to effectively disable the linear type-checker since, alternatively, disabling optimizing transformations which violate linearity incurs significant performance costs. However, we believe that GHC's transformations are correct, and it is the linear type-checker and its underlying type system that cannot sufficiently accommodate the resulting programs.

Additionally, some Core-to-Core transformations such as let-floating and inlining already depend on custom linear type systems to produce more performant programs. Valid linearity annotations in Core could potentially inform and define more optimizations.

3.2 Goals

In the upcoming dissertation we will:

- Propose an extension of Core's type system and type checking algorithm with additional linearity information in order to accommodate linear programs in Core that result from the optimising transformations described in Section 2.5;
- Argue the soundness of the resulting system (i.e. no semantically non-linear programs are deemed linear);
- Show how it validates Core-to-Core optimisation passes;
- Implement the extension into GHC's Core type-checker (internally known as the Core linter).

3.2.1 Extending Core's type system

The key design goal of the extension of Core's type system is to provide enough information so that *syntactically* non-linear but *semantically* linear programs are equipped with enough typing information so that they are deemed linearly well-typed, while ruling out programs

that violate linearity from being considered linearly typed. To this end, we propose to extend Core's linear type system with *usage annotations* for let, letrec and case binder bound variables. Given time, we will also explore a new kind of coercion for multiplicities to validate programs that combine GADTs with multiplicities.

3.2.2 Typing Usage Environments

A solution to a handful of type-checking issues regarding certain variable binders is to extend said binders with a *usage environment*. A usage environment is a mapping from variables to multiplicities. The idea is to annotate let, recursive lets and case binders with a usage environment rather than a multiplicity (in contrast, a λ-bound variable has a multiplicity instead of a usage environment).

There are two sides to the usage environment solution. First, our type system must be able to type-check Core programs in a context where let, recursive let and case binders have usage environments. Secondly, the usage environments must be inferred by the type-checking algorithm when relevant binders are created and maintained throughout the Core-to-Core passes to ultimately be used by the typing rules.

With usage environments, the example in Figure 3.1, in which x is a linear variable, would type-check by annotating y with a usage environment of $[x \to 1]$, because the expression bound by y uses x exactly once, *and* emitting that x is used once when y is used, that is, emitting y's usage environment upon using y.

The example in Figure 3.1 would similarly type-check by annotating x with the usage environment $[y \to 1, z \to 1]$ – to linearly type-check that y and z are used linearly, both branches must use y and z linearly. Using usage environments, in the first branch, using x amounts to using its usage environment (using y and z once) and, in the second branch, y and z are used exactly once; meaning y and z are used exactly once in both branches.

We have explored preliminary typing rules with usage environment inference rules for let, recursive let, and case binders. As we will show below, calculating usage environments is not trivial, especially for recursive let bindings. Yet, at a high level, computing the usage environment of a definition entails collecting the usages, where using a λ-bound variable emits a mapping from that variable to its multiplicity and using a variable annotated with a usage environment emits all mappings from variables to their corresponding multiplicities from that usage environment.

Let Binder Regardless of the original Haskell programs desugared to Core, let bindings are always common in Core due to a myriad of optimizing transformations that create and manipulate let-bindings (Section 2.5). Currently, every let-bound variable in Core is annotated with a multiplicity at its binding site. However, the multiplicity for let-bound variables must be ignored by the type-checker throughout the transformation pipeline (or otherwise too many valid programs would be rejected for violating linearity). Programs with let bindings can be correctly typed by annotating the let-bound variables with a usage environment. Instead of annotating every binder with a multiplicity, only λ-bound variables should be annotated with a multiplicity, while let-bound variables should be annotated with a usage environment. To compute a usage environment for a let-bound variable, compute the usages of free variables in the body of the binder. To type-check an occurrence of a let-bound variable, emit that binder's usage environment. The typing rule combines these two statements:

$$\frac{\Gamma \vdash t : A \rightsquigarrow \{U\} \qquad \Gamma; x :_U A \vdash u : C \rightsquigarrow \{V\}}{\Gamma \vdash \text{let } x :_U A = t \text{ in } u : C \rightsquigarrow \{V\}} \text{ (LET)}$$

Algorithm 1: computeRecUsages

$usageEnvs \leftarrow naiveUsageEnvs.map(fst)$;
for $(bind, U) \in naiveUsageEnvs^*$ **do**
  for $V \in usageEnvs$ **do**
    $V \leftarrow sup(V[bind] * U \setminus \{bind\}, V \setminus \{bind\})$

The rule is read "An expression $\mathsf{let}\ x = t\ \mathsf{in}\ u$ has type C with usage environment V under a Γ context, if the expression t has type A with usage environment U under Γ *and* the expression u has type C with usage environment V under the context Γ extended with the let-bound variable x which has type A and usage environment U".

Recursive Let Binder A variable bound by a recursive-let is in scope in its own definition, allowing for self-reference. Just as let bindings, recursive-let bindings with free linear variables in their assignment body can form in Core during the Core-to-Core passes, and, similarly, the linearity is ignored by the type-checker as the lesser of the two unfavorable options. When the recursive-let-binder is annotated with a usage environment, to type-check t in $\mathsf{letrec}\ x{:}_U A = v\ \mathsf{in}\ t$, where x has type A with usage environment U, simply emit x's usage environment when x occurs in t.

However, calculating the usage environment of a recursive-let binder is much more challenging – a recursive-let-bound variable in its own definition does not yet have a usage environment when it's being computed. The following example uses y linearly if we compute the usage environment of f to be $[y \to 1]$, but can we programmatically reach that solution?

```
letrec f z = case z of
  True → f False
  False → y
in f True
```

The preliminary idea to calculate the usage environment of a set of mutually recursive let binders is to perform the computation in two separate passes. First, calculate a *naive usage environment* by emitting a multiplicity when λ-bound variables are used, usage environments when let-bound and case-bound variables are used, and, conversily, a multiplicity for each recursive-let-bound variable (rather than a usage environment). Second, run algorithm 1 to produce a *final usage environment*. The algorithm receives the recursive binders names and their corresponding naive environment. Intuitively, the algorithm, for each recursive binder, iterates over all (initially naive) usage environments and substitutes the recursive binder by the corresponding usage environment (and possibly scaled up by the amount of times that recursive binder is used in the environment being updated[1]). The type-checking and usage environment inference algorithm combine in the following rule:

$$\frac{\begin{array}{c}\Gamma; x_1 : A_1 \ldots x_n : A_n \vdash t_i : A_i \rightsquigarrow \{U_{i_{\text{naive}}}\} \\ (U_1 \ldots U_n) = computeRecUsages(U_{1_{\text{naive}}} \ldots U_{n_{\text{naive}}}) \\ \Gamma; x_1 :_{U_1} A_1 \ldots x_n :_{U_n} A_n \vdash u : C \rightsquigarrow \{V\}\end{array}}{\Gamma \vdash \text{let } x_1 :_{U_1} A_1 = t_1 \ldots x_n :_{U_n} A_n = t_n \text{ in } u : C \rightsquigarrow \{V\}}\ (\textsc{letrec})$$

[1] A point of contention is using a usage-environment-annotated variable more than once, a problem for which a solution is not evidently clear. Let-bound variables are heap-allocated and executed only once when evaluated. Should using a let-bound variable twice entail using the resources of the binder's definition twice? Tentatively no, because the value is only effectively computed once.

Case Binder In Core, all case expressions create a bound variable, the value of which is the evaluated case scrutinee. This case binder is used by some optimizations to refer to the value pattern matched on. If the case scrutinee must be used linearly, we must consider how to type-check linearity when the case-binder is also used in the case alternatives.

Our preliminary idea is to annotate the case binder with *independent usage environments for each pattern match*. When type-checking the case alternatives, using the case binder equates to using the usage environment associated with that particular alternative. To construct the usage environment of the complete case expression, we take a usage environment which is a superset of the usage environment constructed in each branch. Finally, the usage environment of the case binder in a branch that matched a nullary data constructor is empty, while in branches that matched a non-nullary constructor, the usage environment is a mapping from the variables bound by the pattern to their multiplicities. The typing rule that merges these ideas is:

$$\frac{\Gamma \vdash t : D_{\pi_1 \ldots \pi_n} \rightsquigarrow \{U\} \qquad \Gamma; z :_{U_k} D_{\pi_1 \ldots \pi_n} \vdash b_k : C \rightsquigarrow \{V_k\} \qquad V_k \leqslant V}{\Gamma \vdash \mathsf{case}\ t\ \mathsf{of}\ z :_{(U_1 \ldots U_n)} D_{\pi_1 \ldots \pi_n} \{b_k\}_1^m : C \rightsquigarrow \{U + V\}}\ (\textsc{case})$$

3.2.3 Validating the Work

The greatest measure of success is validating linearity in all programs compiled with GHC, by enabling the linear type-checker after desugaring and each Core-to-Core transformation. In its current implementation, the linear Core type-checker, which is enabled through a flag, rejects many linearly valid programs. Ideally, by the end of our research and implementation, this flag could be enabled by default and accommodate all programs to which existing transformations are applied. Realistically, we want to accept as many diverse transformations as possible while still preserving linearity, even if we are unable to account for all of them.

For each transformation we successfully support in our type system, we will argue that it does indeed preserve linearity by type-checking the input program to the transformation and the ouptut program.

Quantitively, we will benchmark the variation in compilation time and heap-allocations when our extended type-checker is enabled, in comparison to the compiler with the Core type-checker that ignores linearity annotations being run.

The linear Core type-checker validation and benchmarks will be done by running the GHC testsuite and compiling the *head.hackage* package set[2] with the flag which enables the linear Core type-checker. The GHC project also automatically runs tests and benchmarks through its continuous integration (CI) pipeline, which we intend to use to further validate our implementation continuously.

3.2.4 Tasks and Chronogram

In the dissertation, we will propose an extension to Core / System F_C's type system and type-checking algorithm with additional linearity information (such as *usage environments*) in order to accommodate linear programs in Core throughout the GHC pipeline (Section 2.5) stages of desugaring and optimization. This type-system entails augmenting Core's syntax to support additional linearity information and extending existing typing judgments and rules to account for linearity.

[2] *head.hackage* is a package set comprised of relevant libraries of the Haskell ecosystem which are compiled by, and patched against, GHC's latest commit.

Furthermore, we will argue the soundness of our system, that is, our type-system must provably not accept any programs which aren't linear.

Because we want to ensure our type system validates programs before and after optimizing transformations are applied, we will validate that each optimizing transformation does not destroy linearity in programs wrt our type system.

We will implement this extension to Core in GHC, the leading Haskell compiler. Core's type-system implementation, internally known as the Core linter, will serve as the base for our extension. Running the Core linter will enforce an iterative approach to implementing the extensions and allow us to validate our progress continuously.

Defining and implementing this type-system in GHC can be done iteratively because each binder can be handled separately. The typing rules for let bindings, recursive let bindings, and case bindings are distinct, and optimizing transformations seldom interact with all three at the same time. Consequently, we can interweave the formal specification, implementation in Core, and validation of individual optimizations and of our implementation.

Throughout this, we will write the final dissertation document, using it as a driving force for the research which will cristalize our ideas and help communicate them. GHC is a large project with many involved parties – it is crucial that we communicate our ideas and changes clearly, so we can benefit from other contributors expert feedback, and ultimately merge our changes to Core upstream.

CHAPTER 4

Linear Core, again, again, again

For this last version we get rid of the delta-affine context and make delta-variables completely unrestricted, and remove the CaseVar transformation which wasn't sound when beta-reduction for linear-lambdas interacted with the reverse binder swap c.f. Chapter "Why I hate reverse-binder-swap".

No entanto, não parece ser uma limitação do sistema de tipos, mas sim uma duplicação verdadeira de recursos, pela primeira vez. Isso significa que temos de encontrar umas condições para as quais o reverse binder swap não é linear mesmo.

c.f. call-notes de 28-07

Ou seja, isto se calhar é uma falha verdadeira na transformação que pode duplicar recursos! Open a ticket about it!

> $(\lambda x \to \textbf{case}\ x\ \textbf{of}\ \_ \to x)\ (\mathit{close}\ h\ \mathit{rw})$
> $==>$
> $\textbf{case}\ \mathit{close}\ h\ \mathit{rw}\ \textbf{of}\ \_ \to \mathit{close}\ h$

Write that, in practice, we have 4 contexts (2 linear, 2 unrestrited) + mult. var context

- Write ticket about unsoundness of reverse-binder-swap in face of beta-reduction without binding
- On second thought, there's another way: We have two distinct linear type systems, one for optimisations and another for other linting. But the former system is much weaker, and won't trigger call-by-name beta-reduction on as many cases as the latter system can. However, it would be valid to have beta-reduction and case-var, since beta-reduction would still see the reverse binder swap as non-linear, so would still bind...

Types

φ, σ	$::=$	$T\ \overline{p}$	Datatype
	$\mid$	$\varphi \to_\pi \sigma$	Function with multiplicity
	$\mid$	$\forall p.\ \varphi$	Multiplicity universal scheme

Terms

u	$::=$	$x, y, z \mid K$	Variables and data constructors
e	$::=$	u	Term atoms
	$\mid$	$\Lambda p.\ e \mid e\ \pi$	Multiplicity abstraction/application
	$\mid$	$\lambda x{:}_\pi \sigma.\ e \mid e\ e'$	Term abstraction/application
	$\mid$	$\textbf{let}\ x{:}_\Delta \sigma = e\ \textbf{in}\ e'$	Let
	$\mid$	$\textbf{let rec}\ \overline{x{:}_\Delta \sigma = e}\ \textbf{in}\ e'$	Recursive Let
	$\mid$	$\textbf{case}\ e\ \textbf{of}\ z{:}_\Delta \sigma\ \{\overline{\rho \to e'}\}$	Case
ρ	$::=$	$K\ \overline{x{:}_\pi \sigma} \mid \_$	Pattern and wildcard

Environments

Γ	$::=$	$\cdot \mid \Gamma, x{:}_\omega \sigma \mid \Gamma, K{:}\sigma \mid \Gamma, p \mid z{:}_\Delta \sigma$	Unrestricted (delta-)variables
Δ	$::=$	$\cdot \mid \Delta, x{:}_\pi \sigma \mid \Delta, [x{:}_\pi \sigma]$	Linear (and irrelevant) resources

Multiplicities

$\pi, \mu \quad ::= \quad 1 \mid \omega \mid p \mid \pi + \mu \mid \pi \cdot \mu$

Usage Environments

$\Delta \quad ::= \cdot \mid \Delta_1 + \Delta_2 \mid \pi\Delta$

Declarations

pgm	$::=$	$\overline{decl}; e$
$decl$	$::=$	$\textbf{data}\ T\ \overline{p}\ \textbf{where}\ \overline{K : \overline{\sigma \to_\pi}\ T\ \overline{p}}$

Figure 4.1: Linear Core* Syntax

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

$$\frac{\Gamma, p; \Delta \vdash e : \sigma \qquad p \notin \Gamma}{\Gamma; \Delta \vdash \Lambda p.\ e : \forall p.\ \sigma}\ (\Lambda I) \qquad \frac{\Gamma; \Delta \vdash e : \forall p.\ \sigma \qquad \Gamma \vdash_{mult} \pi}{\Gamma; \Delta \vdash e\ \pi : \sigma[\pi/p]}\ (\Lambda E)$$

$$\frac{\Gamma; \Delta, x{:}_1\sigma \vdash e : \varphi \qquad x \notin \Delta}{\Gamma; \Delta \vdash \lambda x{:}_1\sigma.\ e : \sigma \to_1 \varphi}\ (\lambda I_1) \qquad \frac{\Gamma, x{:}_\omega\sigma; \Delta \vdash e : \varphi \qquad x \notin \Delta}{\Gamma; \Delta \vdash \lambda x{:}_\omega\sigma.\ e : \sigma \to_\omega \varphi}\ (\lambda I_\omega)$$

$$\frac{}{\Gamma, x{:}_\Delta\sigma; \Delta \vdash x : \sigma}\ (Var_\Delta) \qquad \frac{\Gamma; \Delta, x{:}_1\sigma \vdash e : \varphi \qquad K \text{ has } n \text{ linear arguments}}{\Gamma; \Delta, \overline{x{:}_1\sigma \# K_i}^{\,n} \vdash x : \sigma}\ (Split)$$

$$\frac{}{\Gamma, x{:}_\omega\sigma; \cdot \vdash x : \sigma}\ (Var_\omega) \qquad \frac{\Gamma; \Delta \vdash e : \sigma \to_1 \varphi \qquad \Gamma; \Delta' \vdash e' : \sigma}{\Gamma; \Delta, \Delta' \vdash e\ e' : \varphi}\ (\lambda E_1)$$

$$\frac{}{\Gamma; x{:}_1\sigma \vdash x : \sigma}\ (Var_1) \qquad \frac{\Gamma; \Delta \vdash e : \sigma \to_\omega \varphi \qquad \Gamma; \cdot \vdash e' : \sigma}{\Gamma; \Delta \vdash e\ e' : \varphi}\ (\lambda E_\omega)$$

(Let)
$$\frac{\Gamma; \Delta \vdash e : \sigma \qquad \Gamma, x{:}_\Delta\sigma; \Delta, \Delta' \vdash e' : \varphi}{\Gamma; \Delta, \Delta' \vdash \textbf{let } x{:}_\Delta\sigma = e \textbf{ in } e' : \varphi}$$

(LetRec)
$$\frac{\overline{\Gamma, \overline{x{:}_\Delta\sigma}; \Delta \vdash e : \sigma} \qquad \Gamma, \overline{x{:}_\Delta\sigma}; \Delta, \Delta' \vdash e' : \varphi}{\Gamma; \Delta, \Delta' \vdash \textbf{let rec } \overline{x{:}_\Delta\sigma = e} \textbf{ in } e' : \varphi}$$

(CaseWHNF)
$$\frac{\text{e is in } \textit{WHNF} \qquad \Gamma; \Delta \vdash e : \sigma \qquad \overline{\Gamma, z{:}_\Delta\sigma; \Delta, \Delta' \vdash_{alt} \rho \to e' :^z_\Delta \sigma \Longrightarrow \varphi}}{\Gamma; \Delta, \Delta' \vdash \textbf{case } e \textbf{ of } z{:}_\Delta\sigma\ \{\overline{\rho \to e'}\} : \varphi}$$

(CaseNotWHNF)
$$\frac{\text{e is definitely not in } \textit{WHNF} \qquad \Gamma; \Delta \vdash e : \sigma \qquad \overline{\Gamma, z{:}_{[\Delta]}\sigma; [\Delta], \Delta' \vdash_{alt} \rho \to e' :^z_{[\Delta]} \sigma \Longrightarrow \varphi}}{\Gamma; \Delta, \Delta' \vdash \textbf{case } e \textbf{ of } z{:}_{[\Delta]}\sigma\ \{\overline{\rho \to e'}\} : \varphi}$$

$$\boxed{\Gamma; \Delta \vdash_{alt} \rho \to e :^z_{\Delta_s} \sigma \Rightarrow \varphi}$$

(AltN)
$$\frac{\Gamma, \overline{x{:}_\omega\sigma}, \overline{y_i{:}_{\Delta_i}\sigma_i}; \Delta \vdash e : \varphi \qquad \overline{\Delta_i} = \overline{\Delta_s \# K_j}^{\,n} \qquad \overline{\Delta_i \neq \cdot} \qquad n > 0 \qquad K : \overline{\sigma_i \to_\pi} \sigma \in \Gamma}{\Gamma; \Delta \vdash_{alt} K\ \overline{x{:}_\omega\sigma}, \overline{y_i{:}_1\sigma_i}^{\,n} \to e :^z_{\Delta_s} \sigma \Longrightarrow \varphi}$$

(Alt0)
$$\frac{\Gamma\,[\cdot/\Delta_s]_z, \overline{x{:}_\omega\sigma}; \Delta\,[\cdot/\Delta_s] \vdash e : \varphi \qquad K : \overline{\sigma_i \to_\omega} \sigma \in \Gamma}{\Gamma; \Delta \vdash_{alt} K\ \overline{x{:}_\omega\sigma} \to e :^z_{\Delta_s} \sigma \Longrightarrow \varphi}$$

(Alt_)
$$\frac{\Gamma; \Delta \vdash e : \varphi}{\Gamma; \Delta \vdash_{alt} \_ \to e :^z_{\Delta_s} \sigma \Longrightarrow \varphi}$$

$$\boxed{\Gamma \vdash_{mult} \pi}$$

$$\frac{}{\Gamma \vdash 1}\ (1) \qquad \frac{}{\Gamma \vdash \omega}\ (\omega) \qquad \frac{}{\Gamma, \rho \vdash \rho}\ (\rho)$$

$$\boxed{\Gamma \vdash \textit{decl} : \Gamma'} \qquad \boxed{\Gamma \vdash \textit{pgm} : \sigma}$$

$$\frac{}{\Gamma \vdash (\textbf{data } T\ \overline{p} \textbf{ where } \overline{K : \sigma}) : (\overline{K : \sigma})}\ (Data) \qquad \frac{\overline{\Gamma \vdash \textit{decl} : \Gamma_d} \qquad \Gamma = \Gamma_0, \overline{\Gamma_d} \qquad \Gamma \text{ is consistent?} \qquad \Gamma \vdash e : \sigma}{\Gamma_0 \vdash \overline{\textit{decl}}; e : \sigma}\ (Pgm)$$

Figure 4.2: Linear Core* Typing Rules

Values

$v \quad ::= \quad \Lambda p.\ e \mid \lambda x.\ e \mid K\ \overline{v}$

Evaluation Contexts

$$\frac{e \longrightarrow e'}{E[e] \longrightarrow E[e']} \qquad E \quad ::= \quad \Box \mid E\ e \mid E\ \pi \mid \textbf{case}\ E\ \textbf{of}\ z{:}_\Delta\sigma\{\overline{\rho \to e}\}$$

Expression Reductions

$$\begin{array}{lcl}
(\Lambda p.\ e)\ \pi & \longrightarrow & e[\pi/p] \\
(\lambda x.\ e)\ e' & \longrightarrow & e[e'/x] \\
\textbf{let}\ x{:}_\Delta\sigma = e\ \textbf{in}\ e' & \longrightarrow & e'[e/x] \\
\textbf{let rec}\ \overline{x_i{:}_\Delta\sigma_i = e_i}\ \textbf{in}\ e' & \longrightarrow & e'[\overline{\textbf{let rec}\ x_i{:}_\Delta\sigma_i = e_i\ \textbf{in}\ e_i/x}] \\
\textbf{case}\ K\ \overline{e}\ \textbf{of}\ z{:}_\Delta\sigma'\{\ldots, K\ \overline{x{:}_\pi\sigma} \to e'\} & \longrightarrow & e'[\overline{e/x}][K\ \overline{e}/z] \\
\textbf{case}\ K\ \overline{e}\ \textbf{of}\ z{:}_\Delta\sigma'\{\ldots, _ \to e'\} & \longrightarrow & e'[K\ \overline{e}/z]
\end{array}$$

Figure 4.3: Linear Core* Operational Semantics (call-by-name)

4.1 Type Safety

Theorem 1 (Type preservation)**.** If $\Gamma; \Delta \vdash e : \sigma$ and $e \longrightarrow e'$ then $\Gamma; \Delta \vdash e' : \sigma$

Proof. By structural induction on the small-step reduction.

Case: $(\lambda x{:}_\pi \sigma.\ e)\ e' \longrightarrow e[e'/x]$

(1) $\Gamma; \Delta, \Delta' \vdash (\lambda x{:}_\pi \sigma.\ e)\ e' : \varphi$
(2) $\Gamma; \Delta \vdash (\lambda x{:}_\pi \sigma.\ e) : \sigma \to_\pi \varphi$ — by inversion on (λE)
(3) $\Gamma; \Delta' \vdash e' : \sigma$ — by inversion on (λE)
Subcase $\pi = 1, p$:
(4) $\Gamma; \Delta, x{:}_{1,p}\sigma \vdash e : \varphi$ — by inversion on (λI)
(5) $\Gamma[\Delta'/x]; \Delta, \Delta' \vdash e[e'/x] : \varphi$ — by linear subst. lemma (3,4)
(6) $\Gamma[\Delta'/x] = \Gamma$ — since Γ is well defined before x's binding (1)
Subcase $\pi = \omega$:
(4) $\Delta' = \cdot$ — by inversion on (λE_ω)
(5) $\Gamma, x{:}_\omega \sigma; \Delta \vdash e : \varphi$ — by inversion on (λI)
(6) $\Gamma; \Delta, \cdot \vdash e[e'/x] : \varphi$ — by unrestricted subst. lemma (3,4,5)

Case: $(\Lambda p.\ e)\ \pi \longrightarrow e[\pi/p]$

(1) $\Gamma; \Delta \vdash (\Lambda p.\ e)\ \pi : \sigma[\pi/p]$
(2) $\Gamma; \Delta \vdash (\Lambda p.\ e) : \forall p.\ \sigma$ — by inversion on (ΛE)
(3) $\Gamma \vdash_{mult} \pi$ — by inversion on (ΛE)
(4) $\Gamma, p; \Delta \vdash e : \sigma$ — by inversion on (ΛI)
(5) $\Gamma; \Delta \vdash e[\pi/p] : \sigma[\pi/p]$ — by mult. subst. lemma (3,4)

Case: **let** $x{:}_\Delta \sigma = e$ **in** $e' \longrightarrow e'[e/x]$

(1) $\Gamma; \Delta, \Delta' \vdash$ **let** $x{:}_\Delta \sigma = e$ **in** $e' : \varphi$
(2) $\Gamma; \Delta \vdash e : \sigma$ — by inversion on *Let*
(3) $\Gamma, x{:}_\Delta \sigma; \Delta, \Delta' \vdash e' : \varphi$ — by inversion on *Let*
(4) $\Gamma; \Delta, \Delta' \vdash e'[e/x] : \varphi$ — by Δ-var subst. lemma (2,3)

Case: **let rec** $\overline{x_i{:}_\Delta \sigma_i = e_i}$ **in** $e' \longrightarrow e'[\overline{\textbf{let rec } \overline{x_i{:}_\Delta \sigma_i = e_i} \textbf{ in } e_i}/x]$

(1) $\Gamma; \Delta, \Delta' \vdash$ **let rec** $\overline{x_i{:}_\Delta \sigma_i = e_i}$ **in** $e' : \varphi$
(2) $\overline{\Gamma, \overline{x_i{:}_\Delta \sigma_i}; \Delta \vdash e_i : \sigma_i}$ — by inversion on *LetRec*
(3) $\Gamma, \overline{x_i{:}_\Delta \sigma_i}; \Delta, \Delta' \vdash e' : \varphi$ — by inversion on *LetRec*
(4) $\overline{\Gamma; \Delta, \cdot \vdash \textbf{let rec } \overline{x_i{:}_\Delta \sigma_i = e_i} \textbf{ in } e_i : \sigma_i}$ — by *LetRec* (2,2)
(6) $\Gamma; \Delta, \Delta' \vdash e'[\overline{\textbf{let rec } \overline{x_i{:}_\Delta \sigma_i = e_i} \textbf{ in } e_i}/x] : \varphi$ — by Δ-var subst. (3,4)

Case: **case** $K\ \overline{e}$ **of** $z{:}_\Delta \sigma\ \{\ldots, K\ \overline{x{:}_\pi \sigma} \to e'\} \longrightarrow e'[\overline{e/x}][K\ \overline{e}/z]$ This is definitely another of the most interesting cases. We must invoke split, use Alt0 or AltN, use delta and unr. substitution, subcases where the case binder is used and isn't, use CaseWHNF

and realize that if it were an expression reduced first with CaseNotWHNF then the usage environment is proof irrelevant, rearrange the usage environments of the case pattern alternatives, etc...

(1) $\Gamma; \Delta, \Delta' \vdash \textbf{case}\ K\ \overline{e_i}\ \textbf{of}\ z{:}_\Delta\sigma\ \{\ldots, K\ w{:}_\pi\sigma \to e'\} : \varphi$
(2) $K\ \overline{e_i}$ is in WHNF — by def. of WHNF
(3) $\Gamma; \Delta \vdash K\ \overline{e_i} : \sigma$ — by inv. on $CaseWHNF$
(4) $\Gamma, z{:}_\Delta\sigma; \Delta, \Delta' \vdash_{alt} K\ \overline{w{:}_\pi\sigma} \to e' :^z_\Delta \sigma \Rightarrow \varphi$ — by inv. on $CaseWHNF$
Subcase $K\ \overline{w{:}_\pi\sigma} = K\ \overline{x{:}_\omega\sigma}, \overline{y_i{:}_1\sigma_i}^n, n > 0$
(5) $K : \overline{\sigma_i \to_\pi}\sigma \in \Gamma$ — by inv. on $AltN$
(6) $\overline{\Gamma; \cdot \vdash e_i : \sigma}, \overline{\Gamma; \Delta_i \vdash e_i : \sigma}, \overline{\Delta_i} = \Delta$ — by constructor application lemma (3,5)
(7) $\Gamma, z{:}_\Delta\sigma, \overline{x{:}_\omega\sigma}, \overline{y_i{:}_{\Delta_i}\sigma_i}; \Delta, \Delta' \vdash e' : \varphi$ — by inv. on $AltN$
(8) $\Gamma, z{:}_\Delta\sigma, \overline{y_i{:}_{\Delta_i}\sigma_i}; \Delta, \Delta' \vdash e' : \varphi$ — by inv. on $AltN$
TODO: Δ_i must be empty in order to type AltN/invoke substitution

Case: $\textbf{case}\ K\ \overline{e}\ \textbf{of}\ z{:}_\Delta\sigma\ \{\ldots, \_ \to e'\} \longrightarrow e'[K\ \overline{e}/z]$

(1) $\Gamma; \Delta, \Delta' \vdash \textbf{case}\ K\ \overline{e}\ \textbf{of}\ z{:}_\Delta\sigma\ \{\ldots, \_ \to e'\} : \varphi$
(2) $\Gamma; \Delta \vdash K\ \overline{e} : \sigma$
(3) $K\ \overline{e}$ is in WHNF
(4) $\Gamma, z{:}_\Delta\sigma; \Delta, \Delta' \vdash_{alt\ \_} \to e' :^z_\Delta \sigma \Rightarrow \varphi$ — by inv on $CaseWHNF$
(5) $\Gamma, z{:}_\Delta\sigma; \Delta, \Delta' \vdash e' : \varphi$ — by inv on $Alt_\_$
(6) $\Gamma; \Delta, \Delta' \vdash e'[K\ \overline{e}/z] : \varphi$ — by Δ-subst.

Case: $e_1\ e_2 \longrightarrow e_1'\ e_2$

(1) $e_1 \longrightarrow e_1'$ — by inversion on β-reduction
(2) $\Gamma; \Delta, \Delta' \vdash e_1\ e_2 : \varphi$ — by assumption
(3) $\Gamma; \Delta \vdash e_1 : \sigma \to_\pi \varphi$ — by inversion on (λE)
(4) $\Gamma; \Delta' \vdash e_2 : \sigma$ — by inversion on (λE)
(5) $\Gamma; \Delta \vdash e_1' : \sigma \to_\pi \varphi$ — by induction hypothesis in (3,1)
(6) $\Gamma; \Delta, \Delta' \vdash e_1'\ e_2 : \varphi$ — by (λE) (4,5)

Case: $e\ \pi \longrightarrow e'\ \pi$

(1) $e \longrightarrow e'$ — by inversion on mult. β-reduction
(2) $\Gamma; \Delta \vdash e\ \pi : \sigma[\pi/p]$ — by assumption
(3) $\Gamma; \Delta \vdash e : \forall p.\ \sigma$ — by inversion on (ΛE)
(4) $\Gamma; \Delta \vdash_{mult} \pi$ — by inversion on (ΛE)
(5) $\Gamma; \Delta \vdash e' : \forall p.\ \sigma$ — by induction hypothesis (3,1)
(6) $\Gamma; \Delta \vdash e'\ \pi : \sigma[\pi/p]$ — by (ΛE) (5,4)

Case: $\textbf{case}\ e\ \textbf{of}\ z{:}_\Delta\sigma\ \{\rho_i \to e_i'\} \longrightarrow \textbf{case}\ e'\ \textbf{of}\ z{:}_\Delta\sigma\ \{\rho_i \to e_i'\}$

(1) $e \longrightarrow e'$ — by inversion on case reduction
(2) $\Gamma; \Delta, \Delta' \vdash \textbf{case}\ e\ \textbf{of}\ z{:}_\Delta\sigma\ \{\rho_i \to e_i'\} : \varphi$
(3) e is not in WHNF — since it can evaluate further by (1)

TODO: that's not quite the definition of WHNF!

(4) $\Gamma; \Delta \vdash e : \sigma$ by inv.
(5) $\overline{\Gamma, z{:}_{[\Delta]}\sigma; [\Delta], \Delta' \vdash_{alt} \rho \to e'' :^{z}_{[\Delta]} \sigma \Rightarrow \varphi}$
(6) $\Gamma; \Delta \vdash e' : \sigma'$ by i.h. (1,4)
(7) $\Gamma; \Delta, \Delta' \vdash \mathbf{case}\ e'\ \mathbf{of}\ z{:}_{\Delta}\sigma\ \{\rho_i \to e'_i\} : \varphi$ by $CaseNotWHNF$

□

Theorem 2 (Progress)**.** Evaluation of a well-typed term does not block. If $\cdot;\cdot \vdash e : \sigma$ then e is a value or there exists e' such that $e \longrightarrow e'$.

Proof. By structural induction on the (only) typing derivation

Case: ΛI

(1) $\cdot;\cdot \vdash (\Lambda p.\ e) : \forall p.\ \sigma$ by assumption
(2) $(\Lambda p.\ e)$ is a value by definition

Case: ΛE

(1) $\cdot;\cdot \vdash e_1\ \pi : \sigma[\pi/p]$ by assumption
(2) $\cdot;\cdot \vdash e_1 : \forall p.\ \sigma$ by inversion on (ΛE)
(3) $\cdot;\cdot \vdash_{mult} \pi$ by inversion on (ΛE)
(4) e_1 is a value or $\exists e'_1.\ e_1 \longrightarrow e'_1$ by the induction hypothesis (2)
Subcase e_1 is a value:
(5) $e_1 = \Lambda p.\ e_2$ by the canonical forms lemma (2)
(6) $(\Lambda p.\ e_2)\ \pi \longrightarrow e_2[\pi/p]$ by β-reduction on multiplicity (5,3)
Subcase $e_1 \longrightarrow e'_1$:
(5) $e_1\ \pi \longrightarrow e'_1\ \pi$ by context reduction on mult. application

Case: λI

(1) $\cdot;\cdot \vdash (\lambda x{:}_{\pi}\sigma.\ e) : \sigma \to_{\pi} \varphi$ by assumption
(2) $(\lambda x{:}_{\pi}\sigma.\ e)$ is a value by definition

Case: λE

(1) $\cdot;\cdot \vdash e_1\ e_2 : \varphi$ by assumption
(2) $\cdot;\cdot \vdash e_1 : \sigma \to_{\pi} \varphi$ by inversion on (λE)
(3) $\cdot;\cdot \vdash e_2 : \sigma$ by inversion on (λE)
(4) e_1 is a value or $\exists e'_1.\ e_1 \longrightarrow e'_1$ by the induction hypothesis (2)
Subcase e_1 is a value:
(5) $e_1 = \lambda x{:}_{\pi}\sigma.\ e$ by the canonical forms lemma
(6) $e_1\ e_2 \longrightarrow e[e_2/x]$ by term β-reduction (5,3)
Subcase $e_1 \longrightarrow e'_1$:
(5) $e_1\ e_2 \longrightarrow e'_1\ e_2$ by context reduction on term application

Case: *Let*

(1) $\cdot \vdash \mathbf{let}\ x{:}_\Delta\sigma = e\ \mathbf{in}\ e' : \varphi$ by assumption
(2) $\mathbf{let}\ x{:}_\Delta\sigma = e\ \mathbf{in}\ e' \longrightarrow e'[e/x]$ by definition

Case: *LetRec*

(1) $\cdot;\cdot \vdash \mathbf{let\ rec}\ \overline{x_i{:}_\Delta\sigma_i = e_i}\ \mathbf{in}\ e' : \varphi$ by assumption
(2) $\mathbf{let\ rec}\ \overline{x_i{:}_\Delta\sigma_i = e_i}\ \mathbf{in}\ e' \longrightarrow e'[\mathbf{let\ rec}\ \overline{x_i{:}_\Delta\sigma_i = e_i}\ \mathbf{in}\ e_i/x]$ by definition

Case: $CaseWHNF$ and $CaseNotWHNF$

(1) $\cdot;\cdot \vdash \mathbf{case}\ e\ \mathbf{of}\ z{:}.\sigma\ \{\overline{\rho_i \to e_i}\} : \varphi$ by assumption
(2) $\cdot;\cdot \vdash e : \sigma$ by inversion of $CaseWHNF$ or $CaseNotWHNF$
(4) $\cdot, z{:}.;\cdot\sigma \vdash_{alt} \rho_i \to e_i :^z \sigma \Rightarrow \varphi$ by inversion of $CaseWHNF$ or $CaseNotWHNF$
(5) e is a value or $\exists e'.\ e \longrightarrow e'$ by induction hypothesis (2)
Subcase e is a value
TODO: this should rather be whether e is in WHNF,
and there should be a better connection between values and WHNF explicit.
(6) $e_1 = K\ \overline{e}$ by canonical forms lemma
(7) e is in WHNF by (6) (TODO: match correctly value and WHNF)
(8) $\overline{\rho_i \to e_i}$ is a complete pattern by coverage checker
(9) $\mathbf{case}\ K\ \overline{e}\ \mathbf{of}\ z{:}.\sigma\ \{\overline{\rho_i \to e_i}\} \longrightarrow e_i\overline{[e/x]}[K\ \overline{e}/z]$
by case reduction on pattern or wildcard
Subcase $\exists e'.\ e \longrightarrow e'$
(6) e is definitely not in WHNF
(7) $\mathbf{case}\ e\ \mathbf{of}\ z{:}.\sigma\ \{\overline{\rho_i \to e_1}\} \longrightarrow \mathbf{case}\ e'\ \mathbf{of}\ z{:}.\sigma\ \{\rho_i \to e_i\}$ by ctx. case reduction

□

Lemma 1 (Substitution of linear variables preserves typing)**.** *If* $\Gamma;\Delta, x{:}_1\sigma \vdash e : \varphi$ *and* $\Gamma;\Delta' \vdash e : \sigma$ *then* $\Gamma\,[\Delta'/x]\,;\Delta,\Delta' \vdash e[e'/x] : \varphi$*, where* $\Gamma[\Delta'/x]$ *substitutes all occurrences of* x *in the usage environments of variables in* Γ *by the linear variables in* Δ'*. (really,* x *couldn't appear anywhere else since* x *is linear).*

Proof. By structural induction on the first derivation.

Case: ΛI

(1) $\Gamma;\Delta, x{:}_1\sigma \vdash \Lambda p.\ e : \forall p.\ \varphi$
(2) $\Gamma;\Delta' \vdash e' : \sigma$
(3) $\Gamma, p;\Delta, x{:}_1\sigma \vdash e : \varphi$ by inversion on ΛI
(4) $p \notin \Gamma$ by inversion on ΛI
(5) $\Gamma[\Delta'/x], p;\Delta,\Delta' \vdash e[e'/x] : \varphi$ by induction hypothesis by (2,3)
(6) $\Gamma[\Delta'/x];\Delta,\Delta' \vdash \Lambda p.\ e[e'/x] : \forall p.\ \varphi$ by ΛI (4,5)
(7) $(\Lambda p.\ e)[e'/x] = (\Lambda p.\ e[e'/x])$ by def. of substitution

Case: ΛE

(1) $\Gamma; \Delta, x{:}_1\sigma \vdash e\ \pi : \varphi[\pi/p]$
(2) $\Gamma; \Delta' \vdash e' : \sigma$
(3) $\Gamma; \Delta, x{:}_1\sigma \vdash e : \forall p.\ \varphi$ by inversion on ΛE
(4) $\Gamma \vdash_{mult} \pi$ by inversion on ΛE
(5) $\Gamma[\Delta'/x]; \Delta, \Delta' \vdash e[e'/x] : \forall p.\ \varphi$ by induction hypothesis by (2,3)
(6) $\Gamma[\Delta'/x]; \Delta, \Delta' \vdash e[e'/x]\ \pi : \varphi[\pi/p]$ by ΛE (4,5)
(7) $(e\ \pi)[e'/x] = e[e'/x]\pi$ by def. of substitution

Case: λI_1

(1) $\Gamma; \Delta, x{:}_1\sigma \vdash \lambda y{:}_1\sigma'.\ e : \sigma' \to_1 \varphi$
(2) $\Gamma; \Delta' \vdash e' : \sigma$
(3) $\Gamma; \Delta, x{:}_1\sigma, y{:}_1\sigma' \vdash e : \varphi$ by inversion on λI
(4) $\Gamma[\Delta'/x]; \Delta, y{:}_1\sigma', \Delta' \vdash e[e'/x] : \varphi$ by induction hypothesis by (2,3)
(5) $\Gamma[\Delta'/x]; \Delta, \Delta' \vdash \lambda y{:}_1\sigma'.\ e[e'/x] : \sigma' \to_1 \varphi$ by λI (4)
(6) $(\lambda y{:}_1\sigma'.\ e)[e'/x] = (\lambda y{:}_1\sigma'.\ e[e'/x])$ by def. of substitution

Case: λI_ω

(1) $\Gamma; \Delta, x{:}_1\sigma \vdash \lambda y{:}_\omega\sigma'.\ e : \sigma' \to_\omega \varphi$
(2) $\Gamma; \Delta' \vdash e' : \sigma$
(3) $\Gamma, y{:}_\omega\sigma'; \Delta, x{:}_1\sigma \vdash e : \varphi$ by inversion on λI
(4) $\Gamma[\Delta'/x], y{:}_\omega\sigma'; \Delta, \Delta' \vdash e[e'/x] : \varphi$ by induction hypothesis by (2,3)
(5) $\Gamma[\Delta'/x]; \Delta, \Delta' \vdash \lambda y{:}_\omega\sigma'.\ e[e'/x] : \sigma' \to_1 \varphi$ by λI (4)
(6) $(\lambda y{:}_\omega\sigma'.\ e)[e'/x] = (\lambda y{:}_\omega\sigma'.\ e[e'/x])$ by def. of substitution

Case: Var_1

(1) $\Gamma; x{:}_1\sigma \vdash x : \sigma$
(2) $\Gamma; \Delta' \vdash e' : \sigma$
(3) $\Gamma[\Delta'/x]; \Delta' \vdash e' : \sigma$ by weaken
(4) $x[e'/x] = e'$ by def. of substitution
(5) $\Gamma[\Delta'/x]; \Delta' \vdash e' : \sigma$ by (3)

Case: Var_ω

(1) Impossible. $x{:}_1\sigma$ can't be in the context.

Case: Var_Δ

(1) $\Gamma, y{:}_{\Delta, x{:}_1\sigma}\varphi; \Delta, x{:}_1\sigma \vdash y : \varphi$
(2) $\Gamma; \Delta' \vdash e' : \sigma$
(3) $y[e'/x] = y$
(4) $\Gamma[\Delta'/x], y{:}_{\Delta,\Delta'}\varphi; \Delta, \Delta';\vdash y : \varphi$ by Var_Δ

Case: *Split*

Trivial induction

Case: λE_1

(1) $\Gamma; \Delta, \Delta'', x{:}_1\sigma \vdash e\ e'' : \varphi$
(2) $\Gamma; \Delta' \vdash e' : \sigma$
Subcase x occurs in e
(3) $\Gamma; \Delta, x{:}_1\sigma \vdash e : \sigma' \to_1 \varphi$ by inversion on λE_1
(4) $\Gamma; \Delta'' \vdash e'' : \sigma'$ by inversion on λE_1
(5) $\Gamma[\Delta'/x]; \Delta, \Delta' \vdash e[e'/x] : \sigma' \to_1 \varphi$ by induction hypothesis (2,3)
(6) $\Gamma[\Delta'/x]; \Delta, \Delta', \Delta'' \vdash e[e'/x]\ e'' : \varphi$ by λE_1
(7) $(e[e'/x]\ e'') = (e\ e'')[e'/x]$ because x does not occur in e''
Subcase x occurs in e''
(3) $\Gamma; \Delta \vdash e : \sigma' \to_1 \varphi$ by inversion on λE_1
(4) $\Gamma; \Delta'', x{:}_1\sigma \vdash e'' : \sigma'$ by inversion on λE_1
(5) $\Gamma[\Delta'/x]; \Delta'', \Delta' \vdash e''[e'/x] : \sigma'$ by induction hypothesis (2,4)
(6) $\Gamma[\Delta'/x]; \Delta, \Delta', \Delta'' \vdash e\ e''[e'/x] : \varphi$ by λE_1
(7) $(e\ e''[e'/x]) = (e\ e'')[e'/x]$ because x does not occur in e

Case: λE_ω

(1) $\Gamma; \Delta, x{:}_1\sigma \vdash e\ e'' : \varphi$
(2) $\Gamma; \Delta' \vdash e' : \sigma$
(3) x does not occur in e'' by e'' linear context is empty
(4) $\Gamma; \Delta, x{:}_1\sigma \vdash e : \sigma' \to_\omega \varphi$ by inversion on λE_ω
(5) $\Gamma; \cdot \vdash e'' : \sigma'$ by inversion on λE_ω
(6) $\Gamma[\Delta'/x]; \Delta, \Delta' \vdash e[e'/x] : \sigma' \to_\omega \varphi$ by induction hypothesis (2,4)
(7) $\Gamma[\Delta'/x]; \Delta, \Delta' \vdash e[e'/x]\ e'' : \varphi$ by λE_ω
(8) $(e[e'/x]\ e'') = (e\ e'')[e'/x]$ because x does not occur in e''

Case: *Let*

(1) $\Gamma; \Delta' \vdash e' : \sigma$
Subcase x occurs in e
(2) $\Gamma; \Delta, x{:}_1\sigma, \Delta'' \vdash \mathbf{let}\ y{:}_{\Delta, x:_1\sigma}\sigma' = e\ \mathbf{in}\ e'' : \varphi$
(3) $\Gamma, y{:}_{\Delta, x:_1\sigma}\sigma'; \Delta, x{:}_1\sigma, \Delta'' \vdash e'' : vp$ by inversion on *Let*
(4) $\Gamma; \Delta, x{:}_1\sigma \vdash e : \sigma'$ by inversion on *Let*
(5) $\Gamma[\Delta'/x], y{:}_{\Delta,\Delta'}\sigma'; \Delta, \Delta', \Delta'' \vdash e''[e'/x]$ by induction hypothesis $(1, 3)$
(6) $\Gamma[\Delta'/x]; \Delta, \Delta' \vdash e[e'/x] : \sigma'$ by induction hypothesis $(1, 4)$
(7) $\Gamma[\Delta'/x]; \Delta, \Delta', \Delta'' \vdash \mathbf{let}\ y{:}_{\Delta,\Delta'}\sigma' = e[e'/x]\ \mathbf{in}\ e''[e'/x] : \varphi$ (5,6) by *Let*
(8) $(\mathbf{let}\ y{:}_{\Delta,\Delta'}\sigma' = e[e'/x]\ \mathbf{in}\ e''[e'/x]) = (\mathbf{let}\ y{:}_{\Delta,\Delta'}\sigma' = e\ \mathbf{in}\ e'')[e'/x]$ by subst.
Subcase x does not occur in e
(2) $\Gamma; \Delta, \Delta'', x{:}_1\sigma \vdash \mathbf{let}\ y{:}_\Delta\sigma' = e\ \mathbf{in}\ e'' : \varphi$
(3) $\Gamma, y{:}_\Delta\sigma'; \Delta, \Delta'', x{:}_1\sigma \vdash e'' : \varphi$ by inversion on *Let*
(4) $\Gamma; \Delta \vdash e : \sigma'$ by inversion on *Let*
(5) $\Gamma[\Delta'/x], y{:}_\Delta\sigma'; \Delta, \Delta', \Delta'' \vdash e''[e'/x] : \varphi$ by induction hypothesis (1,3)

(6) $\Gamma[\Delta'/x]; \Delta, \Delta', \Delta'' \vdash \textbf{let}\ y{:}_\Delta \sigma' = e\ \textbf{in}\ e''[e'/x] : \varphi$ by *Let* (2,5,6)
(7) $\textbf{let}\ y{:}_\Delta \sigma' = e\ \textbf{in}\ e''[e'/x] = (\textbf{let}\ y{:}_\Delta \sigma' = e\ \textbf{in}\ e'')[e'/x]$ by x does not occur in e

Case: *LetRec*

(1) $\Gamma; \Delta' \vdash e' : \sigma$
Subcase $x{:}_1\sigma$ occurs in some e_i
(2) $\Gamma; \Delta, x{:}_1\sigma, \Delta'' \vdash \textbf{let rec}\ \overline{y_i{:}_{\Delta, x:_1\sigma} \sigma_i = e_i}\ \textbf{in}\ e'' : \varphi$
(3) $\Gamma, \overline{y_i{:}_{\Delta, x:_1\sigma} \sigma_i}; \Delta, x{:}_1\sigma, \Delta'' \vdash e'' : \varphi$ by inversion on *LetRec*
(4) $\overline{\Gamma, \overline{y_i{:}_{\Delta, x:_1\sigma} \sigma_i}; \Delta, x{:}_1\sigma \vdash e_i : \sigma_i}$ by inversion on *LetRec*
(5) $\Gamma[\Delta'/x], \overline{y_i{:}_{\Delta, \Delta'} \sigma_i}; \Delta, \Delta', \Delta'' \vdash e''[e'/x] : \varphi$ by induction hypothesis (1,3)
(6) $\overline{\Gamma, \overline{y_i{:}_{\Delta, \Delta'} \sigma_i}; \Delta, \Delta' \vdash e_i[e'/x] : \sigma_i}$ by induction hypothesis (1,4)
(7) $\Gamma[\Delta'/x]; \Delta, \Delta', \Delta'' \vdash \textbf{let rec}\ \overline{y_i{:}_{\Delta, \Gamma_1'} \sigma_i = e_i[e'/x]}\ \textbf{in}\ e''[e'/x] : \varphi$ by *LetRec*
(8) $(\textbf{let rec}\ \overline{y_i{:}_{\Delta, \Delta'} \sigma_i = e_i}\ \textbf{in}\ e'')[e'/x] = \textbf{let rec}\ \overline{y_i{:}_{\Delta, \Delta'} \sigma_i = e_i[e'/x]}\ \textbf{in}\ e''[e'/x]$
Subcase $x{:}_1\sigma$ does not occur in any e_i
(2) $\Gamma; \Delta, x{:}_1\sigma, \Delta'' \vdash \textbf{let rec}\ \overline{y_i{:}_\Delta \sigma_i = e_i}\ \textbf{in}\ e'' : \varphi$
(3) $\Gamma, \overline{y_i{:}_\Delta \sigma_i}; \Delta, x{:}_1\sigma, \Delta'' \vdash e'' : \varphi$ by inversion on *LetRec*
(4) $\overline{\Gamma, \overline{y_i{:}_\Delta \sigma_i}; \Delta \vdash e_i : \sigma_i}$ by inversion on *LetRec*
(5) $\Gamma[\Delta'/x], \overline{y_i{:}_\Delta \sigma_i}; \Delta, \Delta', \Delta'' \vdash e''[e'/x] : \varphi$ by i.h. (1,3)
(6) $\Gamma[\Delta'/x]; \Delta, \Delta', \Delta'' \vdash \textbf{let rec}\ \overline{y_i{:}_\Delta \sigma_i = e_i}\ \textbf{in}\ e''[e'/x] : \varphi$ by *LetRec*
(7) $\textbf{let rec}\ \overline{y_i{:}_\Delta \sigma_i = e_i}\ \textbf{in}\ e''[e'/x] = (\textbf{let rec}\ \overline{y_i{:}_\Delta \sigma_i = e_i}\ \textbf{in}\ e'')[e'/x]$ by subcase

Case: *CaseWHNF*

(1) $\Gamma; \Delta' \vdash e' : \sigma$
Subcase x occurs in e
(2) $\Gamma; \Delta, x{:}_1\sigma, \Delta'' \vdash \textbf{case}\ e\ \textbf{of}\ z{:}_{\Delta, x:_1\sigma} \sigma'\ \{\overline{\rho \to e''}\} : \varphi$
(3) e is in WHNF
(4) $\Gamma; \Delta, x{:}_1\sigma \vdash e : \sigma'$
(5) $\overline{\Gamma, z{:}_{\Delta, x:_1\sigma} \sigma'; \Delta, x{:}_1\sigma, \Delta'' \vdash_{alt} \rho \to e'' :^z_{\Delta, x:_1\sigma} \sigma' \Longrightarrow \varphi}$
(6) $\Gamma\,[\Delta'/x]\,; \Delta, \Delta' \vdash e[e'/x] : \varphi$ by i.h.
(7) $\overline{\Gamma\,[\Delta'/x]\,, z{:}_{\Delta, \Delta'} \sigma'; \Delta, \Delta', \Delta'' \vdash_{alt} \rho \to e''[e'/x] :^z_{\Delta, \Delta'} \sigma' \Longrightarrow \varphi}$ by lin. subst. alts.
(8) $\Gamma\,[\Delta'/x]\,; \Delta, \Delta', \Delta'' \vdash \textbf{case}\ e[e'/x]\ \textbf{of}\ z{:}_{\Delta, \Delta'} \sigma'\ \{\overline{\rho \to e''[e'/x]}\} : \varphi$
Subcase x occurs in $\overline{e''}$
(2) $\Gamma; \Delta, \Delta'', x{:}_1\sigma \vdash \textbf{case}\ e\ \textbf{of}\ z{:}_\Delta \sigma'\ \{\overline{\rho \to e''}\} : \varphi$
(3) e is in WHNF
(4) $\Gamma; \Delta \vdash e : \sigma'$
(5) $\overline{\Gamma, z{:}_\Delta \sigma'; \Delta, \Delta'', x{:}_1\sigma \vdash_{alt} \rho \to e'' :^z_\Delta \sigma' \Longrightarrow \varphi}$
(6) $e[e'/x] = e$ by x does not occur in e
(7) $\overline{\Gamma\,[\Delta'/x]\,, z{:}_\Delta \sigma'; \Delta, \Delta'', \Delta' \vdash_{alt} \rho \to e''[e'/x] :^z_\Delta \sigma' \Longrightarrow \varphi}$ by i.h.
(8) $\Gamma\,[\Delta'/x]\,; \Delta, \Delta'', \Delta' \vdash \textbf{case}\ e\ \textbf{of}\ z{:}_\Delta \sigma'\ \{\overline{\rho \to e''[e'/x]}\} : \varphi$

Case: *CaseNotWHNF*

(1) $\Gamma; \Delta' \vdash e' : \sigma$
Subcase x occurs in e

(2) $\Gamma; \Delta, x{:}_1\sigma, \Delta'' \vdash \mathbf{case}\ e\ \mathbf{of}\ z{:}_{[\Delta, x:_1\sigma]}\sigma'\ \{\overline{\rho \to e''}\} : \varphi$
(3) e is definitely not in WHNF
(4) $\Gamma; \Delta, x{:}_1\sigma \vdash e : \sigma'$ by inv.
(5) $\overline{\Gamma, z{:}_{[\Delta, x:_1\sigma]}\sigma'; [\Delta, x{:}_1\sigma], \Delta'' \vdash_{alt} \rho \to e'' :^z_{[\Delta, x:_1\sigma]} \sigma' \Longrightarrow \varphi}$ by inv.
(6) $\Gamma\,[\Delta'/x]\,; \Delta, \Delta' \vdash e[e'/x] : \varphi$ by i.h.
(7) $\overline{\Gamma\,[\Delta'/x], z{:}_{[\Delta, \Delta']}\sigma'; [\Delta, \Delta'], \Delta'' \vdash_{alt} \rho \to e''[e'/x] :^z_{[\Delta, \Delta']} \sigma' \Longrightarrow \varphi}$
by subst. of p. irr. vars in alt.
or, simply, congruence?
(x only occurs in ctxts, so replace all xs by Δ', starting by Γ)?
(8) $\Gamma\,[\Delta'/x]\,; \Delta, \Delta', \Delta'' \vdash \mathbf{case}\ e[e'/x]\ \mathbf{of}\ z{:}_{\Delta, \Delta'}\sigma'\ \{\overline{\rho \to e''[e'/x]}\} : \varphi$
Subcase x occurs in $\overline{e''}$
(2) $\Gamma; \Delta, \Delta'', x{:}_1\sigma \vdash \mathbf{case}\ e\ \mathbf{of}\ z{:}_{[\Delta]}\sigma'\ \{\overline{\rho \to e''}\} : \varphi$
(3) e is definitely not in WHNF
(4) $\Gamma; \Delta \vdash e : \sigma'$ by inv.
(5) $\overline{\Gamma, z{:}_{[\Delta]}\sigma'; [\Delta], \Delta'', x{:}_1\sigma \vdash_{alt} \rho \to e'' :^z_{[\Delta]} \sigma' \Longrightarrow \varphi}$ by inv.
(6) $e[e'/x] = e$ by x does not occur in e
(7) $\overline{\Gamma\,[\Delta'/x], z{:}_{[\Delta]}\sigma'; [\Delta], \Delta'', \Delta' \vdash_{alt} \rho \to e''[e'/x] :^z_{[\Delta]} \sigma' \Longrightarrow \varphi}$ by lin. subst. on alts
(8) $\Gamma\,[\Delta'/x]\,; \Delta, \Delta'', \Delta' \vdash \mathbf{case}\ e\ \mathbf{of}\ z{:}_{[\Delta]}\sigma'\ \{\overline{\rho \to e''[e'/x]}\} : \varphi$

□

Lemma 1.1 (Substitution of linear variables on case alternatives preserves typing)**.** *If* $\Gamma; \Delta, x{:}_1\sigma \vdash_{alt} \rho \to e :^z_{\Delta_s} \sigma \Longrightarrow \varphi$ *and* $\Gamma; \Delta' \vdash e' : \sigma$ *and* $\Delta_s \subseteq \Delta, x$ *then* $\Gamma\,[\Delta'/x]\,; \Delta, \Delta' \vdash_{alt} \rho \to e[e'/x] :^z_{\Delta_s[\Delta'/x]} \sigma \Longrightarrow \varphi$

Proof. By structural induction on the *alt* judgment.

Case: *AltN*

(1) $\Gamma; \Delta' \vdash e' : \sigma$
(2) $\Gamma; \Delta, x{:}_1\sigma \vdash_{alt} K\ \overline{x{:}_\omega\sigma}, \overline{y_i{:}_1\sigma_i}^n\ \to e :^z_{\Delta_s} \sigma' \Longrightarrow \varphi$
(3) $n > 0$ by inv.
(4) $\overline{\Delta_i} = \overline{\Delta_s \# K_j}^n$ by inv.
(5) $\overline{\Delta_i \neq \cdot}$
(6) $\Gamma, \overline{x{:}_\omega\sigma}, \overline{y_i{:}_{\Delta_i}\sigma_i}; \Delta, x{:}_1\sigma \vdash e : \varphi$ by inv.
(7) $\Gamma\,[\Delta'/x]\,, \overline{x{:}_\omega\sigma}, \overline{y_i{:}_{\Delta_i[\Delta'/x]}\sigma_i}; \Delta, \Delta' \vdash e[e'/x] : \varphi$ by i.h.
(8) $\overline{\Delta_i[\Delta'/x] = \Delta_s[\Delta'/x] \# K_j}^n$ by (4) and cong.
(8) $\Gamma\,[\Delta'/x]\,; \Delta, \Delta' \vdash_{alt} \rho \to e[e'/x] :^z_{\Delta_s[\Delta'/x]} \sigma' \Longrightarrow \varphi$

Case: *Alt*0 This is one of the most interesting proof cases, and particularly hard to prove.

- The first insight is to divide the proof into two subcases, accounting for when the scrutinee (and hence Δ_s) contains the linear resource and when it does not.
- The second insight is to recall that Δ and Δ' are disjoint to be able to prove the subcase in which x does not occur in the scrutinee

- The third insight is to *create* linear resources seemingly out of nowhere *under a substitution that removes them.* We see this happen in the case where x occurs in the scrutinee, for both the linear and affine contexts (see (5,6)). We must also see that we can swap x for Δ' if neither can occur (see (7)).

(1) $\Gamma; \Delta' \vdash e' : \sigma$
Subcase x occurs in scrutinee
(2) $\Gamma; \Delta, x{:}_1\sigma \vdash_{alt} K\ \overline{x{:}_\omega\sigma}\ \to e :^z_{\Delta_s, x:_1\sigma} \sigma' \Longrightarrow \varphi$
(2.5) $\Gamma\left[\cdot/\Delta_s, x\right]_z, \overline{x{:}_\omega\sigma}; (\Delta, x{:}_1\sigma)\left[\cdot/\Delta_s, x\right] \vdash e : \varphi$ by inv.
(3) $\Gamma\left[\cdot/\Delta_s, x\right]_z, \overline{x{:}_\omega\sigma}; \Delta\left[\cdot/\Delta_s\right] \vdash e : \varphi$
(4) $e[e'/x] = e$ since x cannot occur in e (erased from cx)
(5) $\Delta[\cdot/\Delta_s] = (\Delta, \Delta')[\cdot/\Delta_s, \Delta']$ by cong. of subst.
(6) $\Gamma[\cdot/\Delta_s, x]_z[\Delta'/x] = \Gamma[\Delta'/x][\cdot/\Delta_s, \Delta']_z$ by cong. of subst. and more
(7) $\forall x, \Delta, \Delta', \Gamma : x \notin \Delta \wedge \Delta' \not\subset \Delta \wedge \Gamma; \Delta \vdash e : \sigma \Longrightarrow \Gamma[\Delta'/x]; \Delta \vdash e : \sigma$ by Weaken and variables in Γ cannot occur in e if they mention x nor if they mention Δ'
(8) $\Gamma\left[\Delta'/x\right]\left[\cdot/\Delta_s, \Delta'\right]_z, \overline{x{:}_\omega\sigma}; (\Delta, \Delta')\left[\cdot/\Delta_s, \Delta'\right] \vdash e[e'x] : \varphi$ by (4,5,6,7) and x and Δ' are erased from ctx
(9) $\Gamma\left[\Delta'/x\right]; \Delta, \Delta' \vdash_{alt} K\ \overline{x{:}_\omega\sigma}\ \to e[e'/x] :^z_{\Delta_s, \Delta'} \sigma' \Rightarrow \varphi$ by $Alt0$
Subcase x does not occur in scrutinee
(2) $\Gamma; \Delta, x{:}_1\sigma \vdash_{alt} K\ \overline{x{:}_\omega\sigma}\ \to e :^z_{\Delta_s} \sigma' \Longrightarrow \varphi$
(3) $\Gamma\left[\cdot/\Delta_s\right]_z, \overline{x{:}_\omega\sigma}; \Delta\left[\cdot/\Delta_s\right], x{:}_1\sigma \vdash e : \varphi$ by x does not occur in Δ_s and inv.
(4) $\Gamma\left[\Delta'/x\right]\left[\cdot/\Delta_s\right]_z, \overline{x{:}_\omega\sigma}; \Delta\left[\cdot/\Delta_s\right], \Delta' \vdash e[e'/x] : \varphi$ by i.h. and x does not occur in Δ_s
(5) $\Gamma\left[\Delta'/x\right]\left[\cdot/\Delta_s\right]_z, \overline{x{:}_\omega\sigma}; (\Delta, \Delta')\left[\cdot/\Delta_s\right] \vdash e[e'/x] : \varphi$ by Δ and Δ' being disjoint by hypothesis, and Δ_s being a subset of Δ
(6) $\Delta_s[\Delta'/x] = \Delta_s$ by x does not occur in Δ_s
(7) $\Gamma\left[\Delta'/x\right]; \Delta, \Delta' \vdash_{alt} K\ \overline{x{:}_\omega\sigma}\ \to e[e'/x] :^z_{\Delta_s[\Delta'/x]} \sigma' \Rightarrow \varphi$

Case: $Alt\_$ (trivial induction)

(1) $\Gamma; \Delta' \vdash e' : \sigma$
(2) $\Gamma; \Delta, x{:}_1\sigma \vdash_{alt} \_\ \to e :^z_{\Delta_s} \sigma' \Longrightarrow \varphi$
(3) $\Gamma; \Delta, x{:}_1\sigma \vdash e : \varphi$
(4) $\Gamma\left[\Delta'/x\right]; \Delta, \Delta' \vdash e[e'/x] : \varphi$
(5) $\Gamma\left[\Delta'/x\right]; \Delta, \Delta' \vdash_{alt} \_\ \to e[e'/x] :^z_{\Delta_s, \Delta'} \sigma' \Rightarrow \varphi$

□

Lemma 2 (Substitution of unrestricted variables preserves typing)**.** If $\Gamma, x{:}_\omega\sigma; \Delta \vdash e : \varphi$ and $\Gamma; \cdot \vdash e' : \sigma$ then $\Gamma, \Delta \vdash e[e'/x] : \varphi$.

Proof. By structural induction on the first derivation.

Case: ΛI

(1) $\Gamma, x{:}_\omega\sigma; \Delta \vdash \Lambda p.\ e : \forall p.\ \varphi$
(2) $\Gamma; \cdot \vdash e' : \sigma$

(3) $\Gamma, x{:}_{\omega}\sigma, p; \Delta \vdash e : \varphi$ by inversion on ΛI
(4) $p \notin \Gamma$ by inversion on ΛI
(5) $\Gamma, p; \Delta \vdash e[e'/x] : \varphi$ by induction hypothesis by (2,3)
(6) $\Gamma; \Delta \vdash \Lambda p.\ e[e'/x] : \forall p.\ \varphi$ by ΛI (4,5)
(7) $(\Lambda p.\ e)[e'/x] = (\Lambda p.\ e[e'/x])$ by def. of substitution

Case: ΛE

(1) $\Gamma, x{:}_{\omega}\sigma; \Delta \vdash e\ \pi : \varphi[\pi/p]$
(2) $\Gamma; \cdot \vdash e' : \sigma$
(3) $\Gamma, x{:}_{\omega}\sigma; \Delta \vdash e : \forall p.\ \varphi$ by inversion on ΛE
(4) $\Gamma \vdash_{mult} \pi$ by inversion on ΛE
(5) $\Gamma; \Delta \vdash e[e'/x] \forall p.\ \varphi$ by induction hypothesis by (2,3)
(6) $\Gamma; \Delta \vdash e[e'/x]\ \pi : \varphi[\pi/p]$ by ΛE (4,5)
(7) $(e\ \pi)[e'/x] = e[e'/x]\ \pi$ by def. of substitution

Case: λI_1

(1) $\Gamma, x{:}_{\omega}\sigma; \Delta \vdash \lambda y{:}_1\sigma'.\ e : \sigma' \to_1 \varphi$
(2) $\Gamma; \cdot \vdash e' : \sigma$
(3) $\Gamma, x{:}_{\omega}\sigma; \Delta, y{:}_1\sigma' \vdash e : \varphi$ by inversion on λI_1
(4) $\Gamma; \Delta, y{:}_1\sigma' \vdash e[e'/x] : \varphi$ by induction hypothesis (2,3)
(5) $\Gamma; \Delta \vdash \lambda y{:}_1\sigma'.\ e[e'/x] : \sigma' \to_1 \varphi$ by λI_1
(6) $(\lambda y{:}_{\pi}\sigma'.\ e)[e'/x] = (\lambda y{:}_{\pi}\sigma'.\ e[e'/x])$ by def. of subst.

Case: λI_{ω}

(1) $\Gamma, x{:}_{\omega}\sigma; \Delta \vdash \lambda y{:}_{\omega}\sigma'.\ e : \sigma' \to_{\omega} \varphi$
(2) $\Gamma; \cdot \vdash e' : \sigma$
(3) $\Gamma, x{:}_{\omega}\sigma, y{:}_{\omega}\sigma'; \Delta \vdash e : \varphi$ by inversion on λI_{ω}
(4) $\Gamma, y{:}_{\omega}\sigma'; \Delta, \vdash e[e'/x] : \varphi$ by induction hypothesis (2,3)
(5) $\Gamma; \Delta \vdash \lambda y{:}_{\omega}\sigma'.\ e[e'/x] : \sigma' \to_{\omega} \varphi$ by λI_{ω}
(6) $(\lambda y{:}_{\pi}\sigma'.\ e)[e'/x] = (\lambda y{:}_{\pi}\sigma'.\ e[e'/x])$ by def. of subst.

Case: Var_{ω}

(1) $\Gamma, x{:}_{\omega}; \cdot\sigma \vdash x : \sigma$
(2) $\Gamma; \cdot \vdash e' : \sigma$
(4) $x[e'/x] = e'$ by def. of substitution
(5) $\Gamma; \cdot \vdash e' : \sigma$ by (2)

Case: Var_{ω}

(1) $\Gamma, x{:}_{\omega}\sigma; \cdot \vdash y : \varphi$
(2) $\Gamma; \cdot \vdash e' : \sigma$
(3) $y[e'/x] = y$ by def. of substitution
(4) $\Gamma; \cdot \vdash y : \varphi$ by inversion on $Weaken_{\omega}$ (1)

Case: Var_1

(1) Impossible. The context in Var_1 is empty.

Case: Var_{Δ}

(1) Impossible. The context in Var_{Δ} only contains linear variables.

Case: *Split*

Trivial induction

Case: $\lambda E_{1,p}$

(1) $\Gamma, x{:}_{\omega}\sigma; \Delta, \Delta' \vdash e\ e'' : \varphi$
(2) $\Gamma; \cdot \vdash e' : \sigma$
(3) $\Gamma, x{:}_{\omega}\sigma; \Delta \vdash e : \sigma' \to_{1,p} \varphi$ by inversion on $\lambda E_{1,p}$
(4) $\Gamma, x{:}_{\omega}\sigma; \Delta' \vdash e'' : \sigma'$ by inversion on $\lambda E_{1,p}$
(5) $\Gamma; \Delta \vdash e[e'/x] : \sigma' \to_{1,p} \varphi$ by induction hypothesis (2,3)
(6) $\Gamma; \Delta' \vdash e''[e'/x] : \sigma'$ by induction hypothesis (2,4)
(7) $\Gamma; \Delta, \Delta' \vdash e[e'/x]\ e''[e'/x] : \varphi$ by $\lambda E_{1,p}$ (5,6)
(8) $(e\ e'')[e'/x] = (e[e'/x]\ e''[e'/x])$ by def. of subst.

Case: λE_{ω}

(1) $\Gamma, x{:}_{\omega}\sigma; \Delta \vdash e\ e'' : \varphi$
(2) $\Gamma; \cdot \vdash e' : \sigma$
(3) $\Gamma, x{:}_{\omega}\sigma; \Delta \vdash e : \sigma' \to_{\omega} \varphi$ by inversion on λE_{ω}
(4) $\Gamma, x{:}_{\omega}\sigma; \cdot \vdash e'' : \sigma'$ by inversion on λE_{ω}
(5) $\Gamma; \Delta \vdash e[e'/x] : \sigma' \to_{1} \varphi$ by induction hypothesis (2,3)
(6) $\Gamma; \cdot \vdash e''[e'/x] : \sigma'$ by induction hypothesis (2,4)
(7) $\Gamma; \Delta \vdash e[e'/x]\ e''[e'/x] : \varphi$ by λE_{ω} (5,6)
(8) $(e\ e'')[e'/x] = (e[e'/x]\ e''[e'/x])$ by def. of subst.

Case: *Let*

(1) $\Gamma, x{:}_{\omega}\sigma; \Delta, \Delta' \vdash \mathbf{let}\ y{:}_{\Delta}\sigma' = e\ \mathbf{in}\ e'' : \varphi$
(2) $\Gamma; \cdot \vdash e' : \sigma$
(3) $\Gamma, x{:}_{\omega}\sigma, y{:}_{\Delta}\sigma'; \Delta, \Delta' \vdash e''\varphi$ by inversion on *Let*
(4) $\Gamma, x{:}_{\omega}\sigma; \Delta \vdash e : \sigma'$ by inversion on *Let*
(5) $\Gamma, y{:}_{\Delta}\sigma'; \Delta \vdash e''[e'/x] : \varphi$ by induction hypothesis (2,3)
(6) $\Gamma; \Delta \vdash e[e'/x] : \sigma'$ by induction hypothesis (2,4)
(7) $\Gamma; \Delta, \Delta' \vdash \mathbf{let}\ y{:}_{\Delta}\sigma' = e[e'/x]\ \mathbf{in}\ e''[e'/x]$ by *Let* (5,6)
(8) $(\mathbf{let}\ y{:}_{\Delta}\sigma' = e\ \mathbf{in}\ e'')[e'/x] = (\mathbf{let}\ y{:}_{\Delta}\sigma' = e[e'/x]\ \mathbf{in}\ e''[e'/x])$

Case: *LetRec*

(1) $\Gamma, x{:}_\omega\sigma; \Delta, \Delta' \vdash \textbf{let rec } \overline{y{:}_\Delta\sigma' = e} \textbf{ in } e'' : \varphi$
(2) $\Gamma'; \cdot \vdash e' : \sigma$
(3) $\Gamma, x{:}_\omega\sigma, \overline{y{:}_\Delta\sigma'}; \Delta, \Delta' \vdash e'' : \varphi$ by inversion on *LetRec*
(4) $\Gamma, x{:}_\omega\sigma, \overline{y{:}_\Delta\sigma'}; \Delta \vdash e : \sigma'$ by inversion on *LetRec*
(5) $\Gamma, \overline{y{:}_\Delta\sigma'}; \Delta, \Delta' \vdash e''[e'/x] : \varphi$ by induction hypothesis (2,3)
(6) $\Gamma, \overline{y{:}_\Delta\sigma'}; \Delta \vdash e[e'/x] : \sigma'$ by induction hypothesis (2,4)
(7) $\Gamma; \Delta, \Delta' \vdash \textbf{let rec } \overline{y{:}_\Delta\sigma' = e[e'/x]} \textbf{ in } e''[e'/x] : \varphi$ by *LetRec* (5,6)
(8) $(\textbf{let rec } \overline{y{:}_\Delta\sigma' = e} \textbf{ in } e'')[e'/x] = (\textbf{let rec } \overline{y{:}_\Delta\sigma' = e[e'/x]} \textbf{ in } e''[e'/x])$

Case: *CaseWHNF*

(1) $\Gamma; \cdot \vdash e' : \sigma$
(2) $\Gamma, x{:}_\omega\sigma; \Delta, \Delta' \vdash \textbf{case } e \textbf{ of } z{:}_\Delta\sigma' \ \{\overline{\rho \to e''}\} : \varphi$
(3) $\Gamma, x{:}_\omega\sigma; \Delta \vdash e : \sigma$
(4) $\Gamma; \Delta \vdash e[e'/x] : \sigma'$ by i.h.
(5) e is in WHNF
(6) $\overline{\Gamma, x{:}_\omega\sigma, z{:}_\Delta\sigma'; \Delta, \Delta' \vdash \rho \to e'' :_\Delta \sigma' \Rightarrow \varphi}$
(7) $\overline{\Gamma, z{:}_\Delta\sigma'; \Delta, \Delta' \vdash \rho \to e''[e'/x] :_\Delta \sigma' \Rightarrow \varphi}$ by unr. subst. on alts lemma
(8) $\Gamma; \Delta, \Delta' \vdash \textbf{case } e[e'/x] \textbf{ of } z{:}_\Delta\sigma' \ \{\overline{\rho \to e''[e'/x]}\} : \varphi$

Case: *CaseNotWHNF*

(1) $\Gamma; \cdot \vdash e' : \sigma$
(2) $\Gamma, x{:}_\omega\sigma; \Delta, \Delta' \vdash \textbf{case } e \textbf{ of } z{:}_{[\Delta]}\sigma' \ \{\overline{\rho \to e''}\} : \varphi$
(3) $\Gamma, x{:}_\omega\sigma; \Delta \vdash e : \sigma$
(4) $\Gamma; \Delta \vdash e[e'/x] : \sigma'$ by i.h.
(5) e is definitely not in WHNF
(6) $\overline{\Gamma, x{:}_\omega\sigma, z{:}_{[\Delta]}\sigma'; [\Delta], \Delta' \vdash \rho \to e'' :_{[\Delta]} \sigma' \Rightarrow \varphi}$
(6) $\overline{\Gamma, z{:}_{[\Delta]}\sigma'; [\Delta], \Delta' \vdash \rho \to e''[e'/x] :_{[\Delta]} \sigma' \Rightarrow \varphi}$ by unr. subst. on alts lemma
(8) $\Gamma; \Delta, \Delta' \vdash \textbf{case } e[e'/x] \textbf{ of } z{:}_{[\Delta]}\sigma' \ \{\overline{\rho \to e''[e'/x]}\} : \varphi$

□

Lemma 2.1 (Substitution of unrestricted variables on case alternatives preserves typing)**.** *If* $\Gamma, x{:}_\omega\sigma; \Delta \vdash_{alt} \rho \to e :^z_{\Delta_s} \sigma' \Rightarrow \varphi$ *and* $\Gamma; \Delta \vdash e' : \sigma$ *and then* $\Gamma; \Delta \vdash_{alt} \rho \to e[e'/x] :^z_{\Delta_s} \sigma' \Rightarrow \varphi$

Proof. By structural induction on the *alt* judgment.

Case: *AltN* (trivial induction)

(1) $\Gamma; \cdot \vdash e : \sigma$
(2) $\Gamma, x{:}_\omega\sigma; \Delta \vdash_{alt} K \ \overline{x{:}_\omega\sigma}, \overline{y_i{:}_1\sigma_i}^n \ \to e :^z_{\Delta_s} \sigma' \Rightarrow \varphi$
(3) $\Gamma, x{:}_\omega\sigma, \overline{x{:}_\omega\sigma}, \overline{y_i{:}_{\Delta_i}\sigma_i}; \Delta \vdash e : \varphi$
(4) $\Gamma, \overline{x{:}_\omega\sigma}, \overline{y_i{:}_{\Delta_i}\sigma_i}; \Delta \vdash e[e'/x] : \varphi$ by i.h.
(5) $\Gamma; \Delta \vdash_{alt} K \ \overline{x{:}_\omega\sigma}, \overline{y_i{:}_1\sigma_i}^n \ \to e[e'/x] :^z_{\Delta_s} \sigma' \Rightarrow \varphi$ by *AltN*

Case: $Alt0$

(1) $\Gamma; \cdot \vdash e' : \sigma$
(2) $\Gamma, x{:}_\omega\sigma; \Delta \vdash_{alt} K\ \overline{x{:}_\omega\sigma}\ \to e :^z_{\Delta_s} \sigma' \Rightarrow \varphi$
(3) $\Gamma[\cdot/\Delta_s]_z, x{:}_\omega\sigma, \overline{x{:}_\omega\sigma}; \Delta[\cdot/\Delta_s] \vdash e : \varphi$ by inv.
(4) $\Gamma[\cdot/\Delta_s]_z, \overline{x{:}_\omega\sigma}; \Delta[\cdot/\Delta_s] \vdash e[e'/x] : \varphi$ by i.h.
(5) $\Gamma; \Delta \vdash_{alt} K\ \overline{x{:}_\omega\sigma}\ \to e :^z_{\Delta_s} \sigma' \Rightarrow \varphi$ by $Alt0$

Case: $Alt_\_$ (trivial induction)

(1) $\Gamma; \cdot \vdash e : \sigma$
(2) $\Gamma, x{:}_\omega\sigma; \Delta \vdash_{alt\ \_} \to e :_{\Delta_s} \sigma' \Rightarrow \varphi$
(3) $\Gamma, x{:}_\omega\sigma; \Delta \vdash e : \varphi$
(4) $\Gamma; \Delta \vdash e[e'/x] : \varphi$ by i.h.
(5) $\Gamma; \Delta \vdash_{alt\ \_} \to e[e'/x] :^z_{\Delta_s} \sigma' \Rightarrow \varphi$ by $Alt_\_$

□

Lemma 3 (Substitution of variables with usage environments preserves typing)**.** *If* $\Gamma, x{:}_\Delta\sigma; \Delta, \Delta' \vdash e : \varphi$ *and* $\Gamma; \Delta \vdash e' : \sigma$ *then* $\Gamma; \Delta, \Delta' \vdash e[e'/x] : \varphi$

Proof. By structural induction on the first derivation.

Case: ΛI

(1) $\Gamma, x{:}_\Delta\sigma; \Delta, \Delta' \vdash \Lambda p.\ e : \forall p.\ \varphi$
(2) $\Gamma; \Delta \vdash e' : \sigma$
(3) $\Gamma, p, x{:}_\Delta\sigma; \Delta, \Delta' \vdash e : \varphi$ by inversion on ΛI
(4) $\Gamma, p; \Delta, \Delta' \vdash e[e'/x]$ by induction hypothesis (2,3)
(5) $\Gamma; \Delta, \Delta' \vdash \Lambda p.\ e[e'/x] : \forall p.\ \varphi$ by ΛI
(6) $(\Lambda p.\ e)[e'/x] = (\Lambda p.\ e[e'/x])$ by def. of subst.
(7) $\Gamma; \Delta, \Delta' \vdash (\Lambda p.\ e)[e'/x] : \forall p.\ \varphi$ by (5,6)

Case: ΛE

(1) $\Gamma, x{:}_\Delta\sigma; \Delta, \Delta' \vdash e\ \pi : \varphi$
(2) $\Gamma; \Delta \vdash e' : \sigma$
(3) $\Gamma, x{:}_\Delta\sigma; \Delta, \Delta' \vdash e : \forall p.\ \varphi$ by inversion on ΛE
(4) $\Gamma \vdash_{mult} \pi$ by inversion on ΛE
(5) $\Gamma; \Delta, \Delta' \vdash e[e'/x] : \forall p.\ \varphi$ by induction hypothesis (2,3)
(6) $\Gamma; \Delta, \Delta' \vdash e[e'/x]\ \pi : \varphi$ by ΛE
(7) $(e\ \pi)[e'/x] = (e[e'/x]\ \pi)$ by def. of subst.
(6) $\Gamma; \Delta, \Delta' \vdash (e\ \pi)[e'/x] : \varphi$ by (5,6)

Case: λI_1

(1) $\Gamma, x{:}_{\Delta}\sigma; \Delta, \Delta' \vdash \lambda y{:}_1\sigma'.\ e : \sigma' \to_1 \varphi$
(2) $\Gamma; \Delta \vdash e' : \sigma$
(3) $\Gamma, x{:}_{\Delta}\sigma; \Delta, y{:}_1\sigma', \Delta' \vdash e : \varphi$ by inversion on λI
(4) $\Gamma; \Delta, y{:}_1\sigma', \Delta' \vdash e[e'/x] : \varphi$ by induction hypothesis (2,3)
(5) $\Gamma; \Delta, \Delta' \vdash \lambda y{:}_1\sigma'.\ e[e'/x] : \sigma' \to_1 \varphi$ by λI
(6) $(\lambda y{:}_1\sigma'.\ e[e'/x]) = (\lambda y{:}_1\sigma'.\ e)[e'/x]$ by def. of subst.
(7) $\Gamma; \Delta, \Delta' \vdash \lambda(y{:}_1\sigma'.\ e)[e'/x] : \sigma' \to_1 \varphi$ by (4,5)

Case: λI_ω

(1) $\Gamma, x{:}_{\Delta}\sigma; \Delta, \Delta' \vdash \lambda y{:}_\omega\sigma'.\ e : \sigma' \to_\omega \varphi$
(2) $\Gamma; \Delta \vdash e' : \sigma$
(3) $\Gamma, x{:}_{\Delta}\sigma, y{:}_\omega\sigma'; \Delta, \Delta' \vdash e : \varphi$ by inversion on λI
(4) $\Gamma, y{:}_\omega\sigma'; \Delta, \Delta' \vdash e[e'/x] : \varphi$ by induction hypothesis (2,3)
(5) $\Gamma; \Delta, \Delta' \vdash \lambda y{:}_\omega\sigma'.\ e[e'/x] : \sigma' \to_\omega \varphi$ by λI
(6) $(\lambda y{:}_\omega\sigma'.\ e[e'/x]) = (\lambda y{:}_\omega\sigma'.\ e)[e'/x]$ by def. of subst.
(7) $\Gamma; \Delta, \Delta' \vdash \lambda(y{:}_\omega\sigma'.\ e)[e'/x] : \sigma' \to_\omega \varphi$ by (4,5)

Case: Var_ω

(1) $\Gamma, y{:}_\omega\sigma', x{:}_{.}\sigma; \cdot \vdash y : \sigma'$
(2) $\Gamma; \cdot \vdash e' : \sigma$
(3) $y[e'/x] = y$
(4) $\Gamma, y{:}_\omega\sigma'; \cdot \vdash y : \sigma'$ by (1) and $Weaken_\Delta$

Case: Var_1

(1) $\Gamma, x{:}_{y:_1\sigma}\sigma; y{:}_1\sigma \vdash y : \sigma$
(2) $\Gamma; y{:}_1\sigma \vdash e' : \sigma$
(3) $y[e'/x] = y$
(4) $\Gamma, x{:}_{y:_1\sigma}\sigma; y{:}_1\sigma \vdash y : \sigma$ by 1
(5) $\Gamma; y{:}_1\sigma \vdash y : \sigma$ by $Weaken_\Delta$

Case: Var_Δ

(1) $\Gamma, x{:}_{\Delta}\sigma; \Delta \vdash y : \sigma$
(2) $\Gamma'; \Delta \vdash e' : \sigma$
(3) $x[e'/x] = e'$
(4) $\Gamma'; \Delta \vdash e' : \sigma$ by (2)

Case: *Split*

Trivial induction

Case: $\lambda E_{1,p}$

(1) $\Gamma, x{:}_{\Delta}\sigma; \Delta, \Delta', \Delta'' \vdash e\ e'' : \varphi$
(2) $\Gamma; \Delta \vdash e' : \sigma$
Subcase Δ occurs in e
(3) $\Gamma, x{:}_{\Delta}\sigma; \Delta, \Delta' \vdash e : \sigma' \to_{1,p} \varphi$
(4) $\Gamma, x{:}_{\Delta}\sigma; \Delta'' \vdash e'' : \sigma'$
(5) $\Gamma; \Delta'' \vdash e'' : \sigma'$ by $Weaken_{\Delta}$
(6) $\Gamma; \Delta, \Delta' \vdash e[e'/x] : \sigma' \to_{1,p} \varphi$ by i.h.
(7) $\Gamma; \Delta, \Delta', \Delta'' \vdash e[e'/x]\ e'' : \varphi$ by $(\lambda E_{1,p})$
(8) $(e[e'/x]\ e'') = (e\ e'')[e'/x]$ since x cannot occur in e''
Subcase Δ occurs in e''
(3) $\Gamma, x{:}_{\Delta}\sigma; \Delta' \vdash e : \sigma' \to_{1,p} \varphi$
(4) $\Gamma; \Delta' \vdash e : \sigma' \to_{1,p} \varphi$ by $Weaken_{\Delta}$
(5) $\Gamma, x{:}_{\Delta}\sigma; \Delta, \Delta'' \vdash e'' : \sigma'$
(6) $\Gamma; \Delta, \Delta'' \vdash e''[e'/x] : \sigma'$ by i.h.
(7) $\Gamma; \Delta, \Delta', \Delta'' \vdash (e\ e''[e'/x]) : \varphi$ by $(\lambda E_{1,p})$
(8) $e\ e''[e'/x] = (e\ e'')[e'/x]$ since x does not occur in e
Subcase Δ is split between e and e''
x cannot occur in either, so the substitution is trivial, and x can be weakened.

Case: λE_{ω}

(1) $\Gamma, x{:}_{\Delta}\sigma; \Delta, \Delta' \vdash e\ e'' : \varphi$
(2) $\Gamma; \Delta \vdash e' : \sigma$
(3) Δ cannot occur in e''
(4) $\Gamma, x{:}_{\Delta}\sigma; \Delta, \Delta' \vdash e : \sigma' \to_{\omega} \varphi$ by inv. on λE_{ω}
(5) $\Gamma; \cdot \vdash e'' : \sigma'$ by inv. on λE_{ω}
(6) $\Gamma; \Delta, \Delta' \vdash e[e'/x] : \sigma' \to_{\omega} \varphi$ by induction hypothesis (2,4)
(7) $\Gamma; \Delta, \Delta' \vdash e[e'/x]\ e'' : \varphi$ by λE_{ω} (5,6)
(8) $e[e'/x]\ e'' = (e\ e'')[e'/x]$ x does not occur in e'' by (3)

Case: *Let*

(1) $\Gamma; \Delta \vdash e' : \sigma$
Subcase Δ occurs in e
(2) $\Gamma, x{:}_{\Delta}\sigma; \Delta, \Delta', \Delta'' \vdash \mathbf{let}\ y{:}_{\Delta,\Delta'}\sigma' = e\ \mathbf{in}\ e'' : \varphi$
(3) $\Gamma, x{:}_{\Delta}\sigma; \Delta, \Delta' \vdash e : \sigma'$ by inversion on (let)
(4) $\Gamma, x{:}_{\Delta}\sigma, y{:}_{\Delta,\Delta'}\sigma'; \Delta, \Delta', \Delta'' \vdash e'' : \varphi$ by inversion on (let)
(5) $\Gamma, y{:}_{\Delta,\Delta'}\sigma'; \Delta, \Delta', \Delta'' \vdash e'' : \varphi$ by $Weaken_{\Delta}$ (admissible)
(6) $\Gamma; \Delta, \Delta' \vdash e[e'/x] : \sigma'$ by induction hypothesis (1,3)
(7) $\Gamma; \Delta, \Delta', \Delta'' \vdash \mathbf{let}\ y{:}_{\Delta,\Delta'}\sigma' = e[e'/x]\ \mathbf{in}\ e'' : \varphi$ by (let) (5,6)
(8) $\mathbf{let}\ y{:}_{\Delta,\Delta'}\sigma' = e[e'/x]\ \mathbf{in}\ e'' = (\mathbf{let}\ y{:}_{\Delta,\Delta'}\sigma' = e\ \mathbf{in}\ e'')[e'/x]$
since x cannot occur in e''
Subcase Δ occurs in e''
(2) $\Gamma, x{:}_{\Delta}\sigma; \Delta, \Delta', \Delta'' \vdash \mathbf{let}\ y{:}_{\Delta'}\sigma' = e\ \mathbf{in}\ e'' : \varphi$
(3) $\Gamma, x{:}_{\Delta}\sigma; \Delta' \vdash e : \sigma'$ by inversion on (let)
(4) $\Gamma; \Delta' \vdash e : \sigma'$ by $Weaken_{\Delta}$
(5) $\Gamma, x{:}_{\Delta}\sigma, y{:}_{\Delta'}\sigma'; \Delta, \Delta', \Delta'' \vdash e'' : \varphi$ by inversion on (let)
(6) $\Gamma, y{:}_{\Delta'}\sigma'; \Delta, \Delta', \Delta'' \vdash e''[e'/x] : \varphi$ by i.h. (1,5)
(7) $\Gamma; \Delta, \Delta', \Delta'' \vdash \mathbf{let}\ y{:}_{\Delta'}\sigma' = e\ \mathbf{in}\ e''[e'/x] : \varphi$ by (let)

(8) $\mathbf{let}\ y{:}_{\Delta'}\sigma' = e\ \mathbf{in}\ e''[e'/x] = (\mathbf{let}\ y{:}_{\Delta'}\sigma' = e\ \mathbf{in}\ e'')[e'/x]$
since x cannot occur in e

Subcase Δ is split between e and e''
x cannot occur in either, so the substitution is trivial, and x can be weakened.

Case: LetRec

(1) $\Gamma; \Delta \vdash e' : \sigma$
Subcase Δ occurs in $\overline{e_i}$
(2) $\Gamma, x{:}_{\Delta}\sigma; \Delta, \Delta', \Delta'' \vdash \mathbf{let\ rec}\ \overline{y_i{:}_{\Delta,\Delta'}\sigma'_i = e_i}\ \mathbf{in}\ e'' : \varphi$
(3) $\Gamma, x{:}_{\Delta}\sigma, \overline{y_i{:}_{\Delta,\Delta'}\sigma'_i}; \Delta, \Delta', \Delta'' \vdash e'' : \varphi$ by inversion on (let)
(4) $\overline{\Gamma, y_i{:}_{\Delta,\Delta'}\sigma'_i; \Delta, \Delta', \Delta'' \vdash e'' : \varphi}$ by $Weaken_{\Delta}$
(5) $\overline{\Gamma, x{:}_{\Delta}\sigma, y_i{:}_{\Delta,\Delta'}\sigma'_i; \Delta, \Delta' \vdash e_i : \sigma'_i}$ by inversion on (let)
(6) $\overline{\Gamma, y_i{:}_{\Delta,\Delta'}\sigma'_i; \Delta, \Delta' \vdash e_i[e'/x] : \sigma'_i}$ by induction hypothesis (1,5)
(7) $e''[e'/x] = e''$ since x cannot occur in e''
(8) $\Gamma; \Delta, \Delta', \Delta''\mathbf{let\ rec}\ \overline{y_i{:}_{\Delta,\Delta'}\sigma'_i = e_i[e'/x]}\ \mathbf{in}\ e'' : \varphi$ by (let) (4,6)
Subcase Δ occurs in e''
(2) $\Gamma, x{:}_{\Delta}\sigma; \Delta, \Delta', \Delta'' \vdash \mathbf{let\ rec}\ \overline{y_i{:}_{\Delta'}\sigma'_i = e_i}\ \mathbf{in}\ e'' : \varphi$
(3) $\overline{\Gamma, x{:}_{\Delta}\sigma, y_i{:}_{\Delta'}\sigma'_i; \Delta' \vdash e_i : \sigma'_i}$ by inversion on (let)
(4) $\overline{\Gamma, y_i{:}_{\Delta'}\sigma'_i; \Delta' \vdash e_i : \sigma'_i}$ by $Weaken_{\Delta}$
(6) $\Gamma, x{:}_{\Delta}\sigma, \overline{y_i{:}_{\Delta'}\sigma'_i}; \Delta, \Delta', \Delta'' \vdash e'' : \varphi$ by inversion on (let)
(7) $\Gamma, \overline{y_i{:}_{\Delta'}\sigma'_i}; \Delta, \Delta', \Delta'' \vdash e''[e'/x] : \varphi$ by i.h. (1,6)
(8) $\overline{e_i[e'/x] = e_i}$ since x cannot occur in $\overline{e_i}$
(9) $\Gamma; \Delta, \Delta', \Delta'' \vdash \mathbf{let\ rec}\ \overline{y_i{:}_{\Delta'}\sigma'_i = e_i}\ \mathbf{in}\ e''[e'/x] : \varphi$ by (let)
Subcase Δ is split between e and e''
x cannot occur in either, so the substitution is trivial, and x can be weakened.

Case: CaseWHNF

(1) $\Gamma; \Delta \vdash e' : \sigma$
Subcase Δ occurs in e
(2) $\Gamma, x{:}_{\Delta}\sigma; \Delta, \Delta', \Delta'' \vdash \mathbf{case}\ e\ \mathbf{of}\ z{:}_{\Delta,\Delta'}\sigma'\ \{\overline{\rho \to e''}\} : \varphi$
(3) e is in WHNF
(4) $\Gamma, x{:}_{\Delta}\sigma; \Delta, \Delta' \vdash e : \sigma'$
(5) $\overline{\Gamma, x{:}_{\Delta}\sigma, z{:}_{\Delta,\Delta'}\sigma'; \Delta, \Delta', \Delta'' \vdash_{alt} \rho \to e'' :^{z}_{\Delta,\Delta'}: \sigma' \Rightarrow \varphi}$
(6) $\Gamma; \Delta, \Delta' \vdash e[e'/x] : \sigma'$ by i.h.
(7) $\overline{\Gamma, z{:}_{\Delta,\Delta'}\sigma'; \Delta, \Delta', \Delta'' \vdash_{alt} \rho \to e''[e'/x] :^{z}_{\Delta,\Delta'} \sigma' \Rightarrow \varphi}$ by subst. of Δ vars on case alts
(8) $\Gamma; \Delta, \Delta', \Delta'' \vdash \mathbf{case}\ e[e'/x]\ \mathbf{of}\ z{:}_{\Delta,\Delta'}\sigma'\ \{\overline{\rho \to e''[e'/x]}\} : \varphi$ by $CaseWHNF$
Subcase Δ does not occurs in e
(2) $\Gamma, x{:}_{\Delta}\sigma; \Delta, \Delta', \Delta'' \vdash \mathbf{case}\ e\ \mathbf{of}\ z{:}_{\Delta'}\sigma'\ \{\overline{\rho \to e''}\} : \varphi$
(3) e is in WHNF
(4) $\Gamma, x{:}_{\Delta}\sigma; \Delta' \vdash e : \sigma'$
(5) $\Gamma; \Delta' \vdash e : \sigma'$ by (admissible) $Weaken_{\Delta}$
(6) $e[e'/x] = e$ by x cannot occur in e
(7) $\overline{\Gamma, x{:}_{\Delta}\sigma, z{:}_{\Delta'}\sigma'; \Delta, \Delta', \Delta'' \vdash_{alt} \rho \to e'' :^{z}_{\Delta'}: \sigma' \Rightarrow \varphi}$
(8) $\overline{\Gamma, z{:}_{\Delta'}\sigma'; \Delta, \Delta', \Delta'' \vdash_{alt} \rho \to e''[e'/x] :^{z}_{\Delta'} \sigma' \Rightarrow \varphi}$ by subst. of Δ vars on case alts
(9) $\Gamma; \Delta, \Delta', \Delta'' \vdash \mathbf{case}\ e[e'/x]\ \mathbf{of}\ z{:}_{\Delta'}\sigma'\ \{\overline{\rho \to e''[e'/x]}\} : \varphi$ by $CaseWHNF$
Subcase Δ is partially used in e

This is like the subcase above, but consider Δ'
to contain some of part of Δ and Δ to refer to the other part only.

Case: CaseNotWHNF

(1) $\Gamma; \Delta \vdash e' : \sigma$
Subcase Δ occurs in e
(2) $\Gamma, x{:}_{\Delta}\sigma; \Delta, \Delta', \Delta'' \vdash \mathbf{case}\ e\ \mathbf{of}\ z{:}_{[\Delta,\Delta']}\sigma'\ \{\overline{\rho \to e''}\}$
(3) $\Gamma, x{:}_{\Delta}\sigma; \Delta, \Delta' \vdash e : \sigma'$ by inv.
(4) $\Gamma; \Delta, \Delta' \vdash e[e'/x] : \sigma'$ by i.h.
(5) $\overline{\Gamma, x{:}_{\Delta}\sigma, z{:}_{[\Delta,\Delta']}\sigma'; [\Delta, \Delta'], \Delta'' \vdash_{alt} \rho \to e'' :^{z}_{[\Delta,\Delta']} \sigma' \Rightarrow \varphi}$ by inv.
(6) $e''[e'/x] = e$ by x cannot occur in $\overline{e''}$ since Δ is not available (only $[\Delta]$)
(7) $\overline{\Gamma, z{:}_{[\Delta,\Delta']}\sigma'; [\Delta, \Delta'], \Delta'' \vdash_{alt} \rho \to e'' :^{z}_{[\Delta,\Delta']} \sigma' \Rightarrow \varphi}$ by (admissible) $Weaken_{\Delta}$
(8) $\Gamma; \Delta, \Delta', \Delta'' \vdash \mathbf{case}\ e[e'/x]\ \mathbf{of}\ z{:}_{[\Delta,\Delta']}\sigma'\ \{\overline{\rho \to e''}\}$ by $CaseNotWHNF$
Subcase Δ does not occur in e
(2) $\Gamma, x{:}_{\Delta}\sigma; \Delta, \Delta', \Delta'' \vdash \mathbf{case}\ e\ \mathbf{of}\ z{:}_{[\Delta']}\sigma'\ \{\overline{\rho \to e''}\}$
(3) $\Gamma, x{:}_{\Delta}\sigma; \Delta' \vdash e : \sigma'$ by inv.
(4) $\Gamma; \Delta' \vdash e : \sigma'$ by weaken
(5) $e[e'/x] = e$ by x cannot occur in e
(5) $\overline{\Gamma, x{:}_{\Delta}\sigma, z{:}_{[\Delta']}\sigma'; \Delta, [\Delta'], \Delta'' \vdash_{alt} \rho \to e'' :^{z}_{[\Delta']} \sigma' \Rightarrow \varphi}$ by inv.
(7) $\overline{\Gamma, z{:}_{[\Delta']}\sigma'; \Delta, [\Delta'], \Delta'' \vdash_{alt} \rho \to e''[e'/x] :^{z}_{[\Delta']} \sigma' \Rightarrow \varphi}$
by subst. of Δ-vars in case alternatives
(8) $\Gamma; \Delta, \Delta', \Delta'' \vdash \mathbf{case}\ e\ \mathbf{of}\ z{:}_{[\Delta,\Delta']}\sigma'\ \{\overline{\rho \to e''[e'/x]}\}$ by $CaseNotWHNF$
Subcase Δ is partially used in e
This is like the subcase above, but consider Δ'
to contain some of part of Δ and Δ to refer to the other part only.

□

Lemma 3.1 (Substitution of Δ-bound variables on case alternatives preserves typing)**.** *If* $\Gamma, x{:}_{\Delta}\sigma; \Delta, \Delta' \vdash_{alt} \rho \to e :^{z}_{\Delta_s} \sigma' \Rightarrow \varphi$ *and* $\Gamma; \Delta \vdash e' : \sigma$ *and* $\Delta_s \subseteq (\Delta, \Delta')$ *then* $\Gamma; \Delta, \Delta' \vdash_{alt} \rho \to e[e'/x] :^{z}_{\Delta_s} \sigma' \Rightarrow \varphi$

Proof. By structural induction on the *alt* judgment.

Case: $AltN$ (trivial induction)

(1) $\Gamma; \Delta \vdash e' : \sigma$
(2) $\Gamma, x{:}_{\Delta}\sigma; \Delta, \Delta' \vdash_{alt} K\ \overline{x{:}_{\omega}\sigma}, \overline{y_i{:}_1\sigma_i}^{n} \to e :^{z}_{\Delta_s} \sigma' \Rightarrow \varphi$
(3) $n > 0$ by inv.
(4) $\overline{\Delta_i} = \overline{\Delta_s \# K_j}$ by inv.
(5) $\Gamma, x{:}_{\Delta}\sigma, \overline{x{:}_{\omega}\sigma}, \overline{y_i{:}_{\Delta_i}\sigma_i}; \Delta, \Delta' \vdash e : \varphi$ by inv.
(6) $\Gamma, \overline{x{:}_{\omega}\sigma}, \overline{y_i{:}_{\Delta_i}\sigma_i}; \Delta, \Delta' \vdash e[e'/x] : \varphi$ by i.h.
(7) $\Gamma; \Delta, \Delta' \vdash_{alt} K\ \overline{x{:}_{\omega}\sigma}, \overline{y_i{:}_1\sigma_i}^{n} \to e[e'/x] :^{z}_{\Delta_s} \sigma' \Rightarrow \varphi$ by $AltN$

Case: $Alt0$

(1) $\Gamma; \Delta \vdash e' : \sigma$
Subcase Δ occurs in scrutinee
(2) $\Gamma, x{:}_{\Delta}\sigma; \Delta, \Delta', \Delta'' \vdash_{alt} K\ \overline{x{:}_1\sigma}\ \to e :^{z}_{\Delta,\Delta'} \sigma' \Rightarrow \varphi$
(3) $(\Gamma, x{:}_{\Delta}\sigma)[\cdot/\Delta, \Delta']_z; (\Delta, \Delta', \Delta'')[\cdot/\Delta, \Delta'] \vdash e : \varphi$
(4) $\Gamma[\cdot/\Delta, \Delta']_z, x{:}_{\Delta}\sigma; \Delta'' \vdash e : \varphi$
by def. of $[]_z$ subst. and [] subst.
(5) $\Gamma[\cdot/\Delta, \Delta']_z, x{:}_{\Delta}\sigma; \Delta'' \vdash e[e'/x] : \varphi$
by x cannot occur in e by Δ not available
(6) $\Gamma[\cdot/\Delta, \Delta']_z; \Delta'' \vdash e[e'/x] : \varphi$
by (admissible) $Weaken_{\Delta}$
(7) $\cdot = (\Delta, \Delta')[\cdot/\Delta, \Delta']$
(8) $\Gamma[\cdot/\Delta, \Delta']_z; (\Delta, \Delta', \Delta'')[\cdot/\Delta, \Delta'] \vdash e[e'/x] : \varphi$
by (6,7)
(9) $\Gamma; \Delta, \Delta', \Delta'' \vdash_{alt} e[e'/x] :^{z}_{\Delta,\Delta'} \sigma' \Rightarrow \varphi$
Subcase Δ does not occur in the scrutinee
(2) $\Gamma, x{:}_{\Delta}\sigma; \Delta, \Delta', \Delta'' \vdash_{alt} K\ \overline{x{:}_1\sigma}\ \to e :^{z}_{\Delta'} \sigma' \Rightarrow \varphi$
(3) $(\Gamma, x{:}_{\Delta}\sigma)[\cdot/\Delta']_z; (\Delta, \Delta', \Delta'')[\cdot/\Delta'] \vdash e : \varphi$
(4) $\Gamma[\cdot/\Delta']_z, x{:}_{\Delta}\sigma; \Delta, \Delta'' \vdash e : \varphi$
by def. of $[]_z$ subst. and [] subst.
(5) $\Gamma[\cdot/\Delta']_z; \Delta, \Delta'' \vdash e[e'/x] : \varphi$ by Δ-subst. lemma
(6) $\cdot = \Delta'[\cdot/\Delta']$
(7) $\Gamma[\cdot/\Delta']_z; (\Delta, \Delta', \Delta'')[\cdot/\Delta'] \vdash e[e'/x] : \varphi$ by (5,6)
(8) $\Gamma; \Delta, \Delta', \Delta'' \vdash_{alt} \vdash e[e'/x] :^{z}_{\Delta'} \sigma' \Rightarrow \varphi$ by $Alt0$
Subcase Δ is partially used in the scrutinee
This is like the subcase above, but consider Δ'
to contain some of part of Δ and Δ to refer to the other part only.

Case: $Alt_{\_}$ (trivial induction)

(1) $\Gamma; \Delta \vdash e' : \sigma$
(2) $\Gamma, x{:}_{\Delta}\sigma; \Delta, \Delta' \vdash_{alt} \_\ \to e :^{z}_{\Delta_s} \sigma' \Rightarrow \varphi$
(3) $\Gamma, x{:}_{\Delta}\sigma; \Delta, \Delta' \vdash e : \varphi$ by inv.
(4) $\Gamma; \Delta, \Delta' \vdash e[e'/x]] : \varphi$ by i.h.
(5) $\Gamma; \Delta, \Delta' \vdash_{alt} \_\ \to e[e'/x] :^{z}_{\Delta_s} \sigma' \Rightarrow \varphi$ by $Alt_{\_}$

□

TODO! Substitution of proof-irrelevant linear variables preserves typing. The term always remains the same because x cannot occur in any term, however, all variables that refer to x in their usage environment must now refer the usage env. of the substitee (e.g. $[x] => [\Delta]$). This seems trivial to see correct, since all occurrences are in environments, so we get some equivalence similar to the one we need for the proof of Alt0.

Lemma 4 (Substitution of proof-irrelevant linear variables preserves typing)**.** *If* $\Gamma; \Delta, [x{:}_1\sigma] \vdash [: \delta]e\varphi$ *and* $\Gamma; \Delta' \vdash [: \delta']e'\sigma$ *then* $\Gamma; \Delta, [\Delta'] \vdash [: \delta\,[\Delta'/x]\,, \delta']e\varphi$

TODO: Multiplicity substitution preserves typing lemma

TODO: Canonical forms lemma

TODO: Corollary of Δ-var subst. for $\overline{\Delta}$

TODO: Constructor app typing: If $\Gamma, \Delta \vdash K\ \overline{e}$ and $K{:}\overline{\sigma \to \pi}\ T\ \overline{p} \in \Gamma$ and Γ has no linear vars then $\overline{\Gamma, \Delta_i \vdash e_i : \sigma_i}$

4.2 How reverse binder swap interacts with linearity

- We can have a rule ($CaseVar$) to type cases of variables that still get used in its body
- And type the reverse-binder-swap + the float-out that simon mentioned.
- However, if we beta-reduce an expression that uses the case-var rule and does use x in the case-alternatives, then we effectively duplicate resources.
- This looks like a real bug, not a type system limitation. (The soundness proof for the language that had $CaseVar$ uncovered it)
- c.f. examples in call-notes (28-07 mainly)
- Great, we become uniform in that variables are considered not in WHNF
- This might, however, be actually OK in Core - the occurrence analysis that determines whether beta-reduction can or cannot be call-by-name is different from the linear type-checker (which is an unfortunate non-uniformity – our system can likely see much more things as being linear, but can't support reverse-binder-swap AND call-by-name-beta-reduction)

4.3 The K-Vars Arrangement Dilemma

Consider the reduction of case expressions for a known pattern,

$$\textbf{case}\ K\ \overline{e}\ \textbf{of}\ z{:}_{\Delta}\sigma'\{\ldots, K\ \overline{x{:}_{\pi}\sigma} \to e'\} \longrightarrow e'\overline{[e/x]}[K\ \overline{e}/z]$$

and the typing rule for $CaseWHNF$ and the alternatives $AltN$:

$$\frac{\text{e is in } \mathit{WHNF} \qquad \Gamma;\Delta \vdash e : \sigma \qquad \overline{\Gamma, z{:}_{\Delta}\sigma;\Delta,\Delta' \vdash_{alt} \rho \to e' :^{z}_{\Delta} \sigma \Longrightarrow \varphi}}{\Gamma;\Delta,\Delta' \vdash \textbf{case}\ e\ \textbf{of}\ z{:}_{\Delta}\sigma\ \{\overline{\rho \to e'}\} : \varphi}\ (\textsc{CaseWHNF})$$

$$\frac{\Gamma, \overline{x{:}_{\omega}\sigma}, \overline{y_i{:}_{\Delta_s \# K_i}\sigma_i}^{n};\Delta \vdash e : \varphi \qquad n > 0 \qquad K : \overline{\sigma_i \to_{\pi}}\sigma \in \Gamma}{\Gamma;\Delta \vdash_{alt} K\ \overline{x{:}_{\omega}\sigma}, \overline{y_i{:}_{1}\sigma_i}^{n} \to e :^{z}_{\Delta_s} \sigma \Longrightarrow \varphi}\ (\textsc{AltN})$$

When we add the constructor-bound variables to the context, we make them Δ-bound and assign a tag to each of the variables in their usage environment (which is the usage env. of the scrutinee, modulo the tags).

The tags work great to ensure all the linear variables in the pattern are used exactly once. In contrast, if we used simply fractions to fragment the usage environment we could e.g. use two times the same pattern variable to use all the resources. Tags are able to encode the idea that each pattern positional-variable must be consumed once, even if they're pattern-matched on multiple times, for example:

```
f x y =
  case (x, y) of
    (a, b) → case (x, y) of
      (n, p) → (a, p)
```

is well-typed because we split x, y into $x\#(,)1, x\#(,)2, y\#(,)1, y\#(,)2$, and give to the pattern variables usage environments $\Delta_a = x\#(,)1, y\#(,)1$, $\Delta_b = x\#(,)2, y\#(,)2$, $\Delta_n = x\#(,)1, y\#(,)1$, $\Delta_p = x\#(,)2, y\#(,)2$. (Really, we first assign the usage environments, and are forced to Split the resources in order to use the pattern variables).

However, this interacts badly with our substitution lemma for Δ-vars: If $\Gamma; \Delta \vdash e' : \sigma$ and $\Gamma, x{:}_\Delta\sigma; \Delta, \Delta' \vdash e : \varphi$ then $\Gamma; \Delta, \Delta' \vdash e[e'/x] : \varphi$. We'll want to substitute an expression for each pattern-variable (see above reduction), but we'll have expressions using different resources for each pattern while simultaneously have each pattern variable use a fragment of all the resources used in the scrutinee. This doesn't allow us to use the Δ-substitution lemma. An example makes this clear:

```
f x y =
  case K x y of
    K a {x # K1, y # K1} b {x # K2, y # K2} → (a, b)
```

We want to substitute $[x/a]$ and $[y/b]$, however, a doesn't have u.e. $= x$ and b doesn't have u.e. equal to y.

How can we keep the fragmented usage environments that can simply encode mutual exclusion between using the scrutinee resources (in CaseWHNF), the case binder, or *all* the pattern variables exactly once; while allowing this substitution to happen.

I think the solution is to **allow rearraging the usage environments**. Even better, don't specify how tagged resources are distributed amongst the usage environments, as long as all linear pat-vars are assigned at least one resource, and that all resources are split on that constructor!

With this generalization in place, we are able to rather write the above example as

```
f x y =
  case K x y of
    K a {x # K1, x # K2} b {y # K1, y # K2} → (a, b)
```

for which it is now obvious we can split x and y and have them match the usage environment as the pattern variable they are substituting!

That makes the new *AltN* rule

$$\text{(AltN)}\quad \frac{\Gamma, \overline{x{:}_\omega\sigma}, \overline{y_i{:}_{\Delta_i}\sigma_i}; \Delta \vdash e : \varphi \qquad \overline{\Delta_i} = \overline{\Delta_s \# K_j}^n \qquad \overline{\Delta_i \neq \cdot} \qquad n > 0 \qquad K : \overline{\sigma_i \to_\pi} \sigma \in \Gamma}{\Gamma; \Delta \vdash_{alt} K\ \overline{x{:}_\omega\sigma}, \overline{y_i{:}_1\sigma_i}^n \to e :^z_{\Delta_s} \sigma \Longrightarrow \varphi}$$

where $\overline{\Delta_i}$ is any (non-empty) combination of K-fragmented resources from Δ_s.

This almost works, were it not for the fact we might want to substitute the pattern variable by an expression that doesn't use resources, despite the pattern-variable being linear.

In the case alternative, we must treat all linear variables equally in a way that ensures if one of them is used then all of them are used exactly once. Splitting resources equally amongst the variable works, but requires rearranging s.t. the substitution environment matches the variable environment. By allowing the var environment to be any (non-empty) arrangement a-priori we facilitate the substitution.

Regarding the arragement being necessarily non-empty: perhaps when substituting we can identify these variables and say something special about them in the proof, like what? Perhaps the posterior rearrangement really is the best idea?