# Nax theory

Ki Yung Ahn Tim Sheard Marcelo P. Fiore Andrew M. Pitts

Portland State University*
Portland, Oergon, USA
kya@cs.pdx.edu sheard@cs.pdx.edu

University of Cambridge†
Cambridge, UK
{Marcelo.Fiore,Andrew.Pitts}@cl.cam.ac.uk

This is a sentence in the abstract. This is another sentence in the abstract. This is yet another sentence in the abstract. This is the final sentence in the abstract.

## 1 Introduction

### 1.1 Need for a unified system for both programming and reasoning

Few will argue with the statement that we need better tools for reasoning about programs, yet there is little widespread agreement about how such tools should be built. One promising approach is to exploit the Curry-Howard isomorphism that states there is an isomorphism between two kinds of systems in widespread use. The first kind of system includes typed programming languages (e.g., ML, Haskell) , where programs are assigned types, and the second kind of system includes logical reasoning systems (or, proof assistants, e.g., Coq, Agda) where proofs prove propositions. The Curry-Howard isomorphism states the structure encoding the relationships *Program :: Type* and *Proof :: Proposition* is identical in both systems. It seems reasonable that since both systems have the typed lambda calculi as their core, that unified system would be developed. Such a system would have the benefits of both, and the additional symbiosis of providing a natural substrate for reasoning about programs. While there has been much work in this area, few would agree that we have arrived. The problem is hard because the two kinds of systems were designed for different purposes, and the features that support these purposes often clash – being crucial in one system but anathema in the other. Examples include non-termination and effects to model real world systems (in programming systems) v.s. totality and purity to ensure soundness (in reasoning systems).

### 1.2 Naive approaches towards a unified system

At first glance, the design strategy for such a unified system may seem obvious: either (1) extend a proof assistant with general recursion and effects, or, (2) extend a functional language with dependent types. In either case, be careful to track where the undesirable features creep from one part of the system to the other. The absence of such a unified system tells us that how to do this is perhaps not obvious. Termination checking, and the ensuing tracking are, of course, both challenging issues in their own right, but are only part of the problem. Neither (1) nor (2) will lead to a successful design, even if we had good strategies for termination checking and tracking. Why is this so? It is because dependently typed languages do not subsume all the other desired properties of functional programming languages. There are other issues in play.

*This paper is based upon work supported by the National Science Foundation under Grant No. 0613969.
†Another thanks here if needed

Firstly, dependently typed languages, designed for logical reasoning, usually do not support *all the recursive datatypes* that are commonly used in functional programs. For example, most dependently typed proof assistants will reject a straightforward datatype definition for Higher-Order Abstract Syntax (HOAS). For example, in Haskell we may write:

```
data HOAS = Lam (HOAS -> HOAS) | App HOAS HOAS
```

But in Coq, this would not be admitted as a legal datatype, because of the use of `HOAS` in a contravariant position in the type of `Lam`. In short, there is a mismatch between types allowed in proof assistants and functional languages. This is why (1) fails to be a promising approach. Approach (1) can only supply partial support for the kinds of data definition in common use in functional programming systems.

Secondly, dependently typed languages, in general, lack both *type erasure* and *type inference*. A dependently typed language designed for programming, even without considering logical consistency, would be certainly more expressive than a functional language based on Hindley-Milner type reconstruction. However, some good features we enjoy in functional languages are lost when we move to such a system. One feature is the conciseness of Hindley-Milner type reconstruction. Programmers need supply only the most minimal amount of type information when programming. Another feature we lose is *type erasure*. In functional languages, types are irrelevant once type checking is done. So, they need not persist for computation at runtime. In dependently typed languages, types can be indexed by terms as well as types. Furthermore, dependently typed languages usually do not distinguish between term applications, which are usually computationally relevant, and type application, which are usually computationally irrelevant. Thus, type erasure becomes very difficult. In a dependently typed language, it is unclear whether, in the application $f\ 3$, the argument 3 will be used for computation or used only for type checking. For these two reasons, we don't believe (2) is a promising approach either.

These two issues are not only counter productive for functional programmers, but also become obstacles for efficient implementation and separate compilation. So, we believe that rather than blend one existing system towards the other, it may be useful to start the design process from scratch, of course, all the while keeping in mind not only these issues, but also all the valuable lessons learned from previous systems. Design goals

- Type inference and type reconstruction wherever possible. Keep type annotations light weight and minimal (minimal might be hard to tie down precisely).
- Use dependent types to state and ensure properties of programs. Our strategy is to start with indexed types and move to full dependency in future work.
- Clearly separate what parts of the program are irrelevant at run time and use erasure to build efficient implementations.
- Let the mathematics and theory guide the development.

## 1.3 Nax as a starting point

We have designed and implemented a prototype of Nax, which is a strongly normalizing functional language supporting the following features (which are all illustrated in §2):

**Two level datatypes.** Recursive dataypes are introduced in two stages. First a non-recursive *structure* is introduced which abstracts over where recursive sub-components will appear. Then a *fix-point* is taken to define the recursive types (§2.1). To minimize the extra notation necessary to program in this manner an extensive *macro-facility* is provided. The most common macro forms can be automatically derived. This is illustrated in §2.3.

**Indexed types with static term indices.** A type constructor is applied to arguments. Arguments are either parameters or indices. A datatype is polymorphic over its parameters (in the sense that parametricity theorems hold over parameters). Parameters are always types. Indexed arguments can be either types or terms. An index usually encodes a static property about the shape or form of a value with that type. We use different kinding rules to separate term indices from type indices. For instance a length indexed list, `x`, might have type (`List Int 2`). The `Int` is a parameter, indicating the list contains integers, but the `2` is an index indicating that the list, `x`, has exactly two elements. Types are static in Nax. Types are only used for type checking and are computationally irrelevant, even though some parts of a type might include terms. In other words, Nax supports *type erasure*,

**Recursive types of unrestricted polarity but restricted elimination.** It is well known that unrestricted recursive types enable diverging computation even without any recursion at the term level. To design a normalizing language that supports recursive types, we must make a design choice that limits the use of recursive types. There are two possible design choices. We may restrict the formation of recursive types (i.e., type definition) or we may restrict the elimination of recursive types (i.e., pattern matching). In Nax, we make the latter design choice, so that we can define *all the recursive datatypes* available in modern functional languages.

**Mendler style iteration and recursion combinators.** Any useful normalizing language should support principled recursion operators that guarantee normalization. Such operators should be easy to use, and expressive over datatypes with both parameters and indices. Mendler style combinators meet both requirements. So, we adopt them in Nax.

**Type inference (reconstruction) from minimal annotation.** When we extend the Hindley-Milner type system with indexed data types, we no longer have type inference for completely unannotated terms. For example, this restriction shows up in languages which support GADTs, which support a kind of type indexing. Although complete type inference is not possible, partial type inference (reconstruction of missing type information) is still possible when sufficient type annotations are provided. Nax's systematic partition of type parameters from type indices provides a mechanism where it is possible to decide exactly where additional type annotations are needed, and to enforce that the programmer supply such annotations. This system faithfully extends the Hindley-Milner type inference (i.e., no additional annotations are needed for the programs that are already inferable by Hindley-Milner).

## 2 Nax by Example

We introduce programming in our implementation of Nax by providing examples. An example usually consists of several parts.

- Introducing data definitions to describe the data of interest. Recursive data is introduced in two stages. We must be careful to separate parameters from indices when using indices to describe static properties of data.
- Introduce macros, either by explicit definition, or by automatic fixpoint derivation to limit the amount of explicit notation that must be supplied by the programmer.
- Write a series of definitions that describe how the data is to be manipulated. Deconstruction of recursive data can only be performed with Mendler-style combinators to ensure strong normalization.

## 2.1 Two-level types

Non recursive datatypes are introduced by the **data** declaration. The data declaration can include arguments. The kind and separation of arguments into parameters and a indices is inferred. For example, the three non-recursive data types, *Bool*, *Either*, and *Maybe*, familiar to many functional programmers, are introduced by declaring the kind of the type, and the type of each of the constructors. This is similar to the way GADTs are introduced in Haskell.

| **data** $Bool : *$ **where** | **data** $Either : * \to * \to *$ **where** | **data** $Maybe : * \to *$ **where** |
|---|---|---|
| $False : Bool$ | $Left : a \to Either\ a\ b$ | $Nothing : Maybe\ a$ |
| $True\ : Bool$ | $Right : b \to Either\ a\ b$ | $Just : a \to Maybe\ a$ |

Note the kind information ($Bool : *$) declares *Bool* to be a type, ($Either : * \to * \to *$) declares *Either* to be a type constructor with two type arguments, and ($Maybe : * \to *$) declares *Maybe* to be a type constructor with one type argument.

To introduce a recursive type, we first introduce a non recursive datatype that uses a parameter where the usual recursive components occur. By design, normal parameters of the introduced type are written first ($a$ in $L$ below) and the type argument to stand for the recursive component is written last (the $r$ of $N$, and the $r$ of $L$ below).

| -- The fixpoint of $N$ will<br>-- be the natural numbers.<br>**data** $N : * \to *$ **where** | -- The fixpoint of $(L\ a)$ will<br>-- be the polymorphic lists<br>**data** $L : * \to * \to *$ **where** |
|---|---|
| $Zero : N\ r$ | $Nil\ \ : L\ a\ r$ |
| $Succ : r \to N\ r$ | $Cons : a \to r \to L\ a\ r$ |

A recursive type can be defined as the fixpoint of a (perhaps partially applied) non-recursive type constructor. Thus the traditional natural numbers are typed by $\mu^{[*]}\ N$ and the traditional lists with components of type $a$ are typed by $\mu^{[*]}\ (L\ a)$. Note that the recursive type operator $\mu^{[\kappa]}$ is itself specialized with a kind argument inside square brackets ($[\kappa]$). The recursive type $(\mu^{[\kappa]}\ f)$ is well kinded only if the operand $f$ has kind $\kappa \to \kappa$, in which case the recursive type $(\mu^{[k]}\ f)$ has kind $\kappa$. Since both $N$ and $(L\ a)$ have kind $* \to *$, the recursive types $\mu^{[*]}\ N$ and $\mu^{[*]}\ (L\ a)$ have kind $*$. That is, they are both types, not type constructors.

## 2.2 Creating values

Values of a particular data type are created by use of constructor functions. For example *True* and *False* are nullary constructors (or, constants) of type *Bool*. $(Left\ 4)$ is a value of type $(Either\ Int\ a)$. Values of recursive types (i.e., those values with types such as $(\mu^{[k]}\ f)$ are formed by using the special $\mathsf{In}^{[\kappa]}$ constructor expression. Thus *Nil* has type $L\ a$ and $(\mathsf{In}^{[*]}\ Nil)$ has type $(\mu^{[*]}\ (L\ a))$. In general, applying the operator $\mathsf{In}^{[k]}$ injects a term of type $f\ (\mu^{[k]}\ f)$ to the recursive type $(\mu^{[k]}\ f)$. Thus a list of *Bool* could be created using the term $(\mathsf{In}^{[*]}\ (Cons\ True\ (\mathsf{In}^{[*]}\ (Cons\ False\ (\mathsf{In}^{[*]}\ Nil)))))$. A general rule of thumb, is to apply $\mathsf{In}^{[k]}$ to terms of non-recursive type to get terms of recursive type. Writing programs using two level types, and recursive injections has definite benefits, but it surely makes programs rather annoying to write. Thus, we have provided Nax with a simple but powerful synonym (macro) facility.

## 2.3 Synonyms, constructor functions, and fixpoint derivation

We may codify that some type is the fixpoint of another, once and for all, by introducing a type synonym (macro).

**synonym** $Nat = \mu^{[*]}\ N$
**synonym** $List\ a = \mu^{[*]}\ (L\ a)$

In a similar manner we can introduce constructor functions that create recursive values without explicit mention of $\mathsf{In}^{\cdot}$ at their call sites (potentially many), but only at their site of definition (exactly once).

$$\begin{aligned} zero &= \mathsf{In}^{[*]}\ Zero \\ succ\ n &= \mathsf{In}^{[*]}\ (Succ\ n) \\ nil &= \mathsf{In}^{[*]}\ Nil \\ cons\ x\ xs &= \mathsf{In}^{[*]}\ (Cons\ x\ xs) \end{aligned}$$

This is such a common occurrence that recursive synonyms and recursive constructor functions can be automatically derived. With automatic synonym and constructor derivation using Nax is both concise and simple. The clause "**deriving fixpoint** *List*" (below right) causes the **synonym** for *List* to be automatically defined. It also defines the constructor functions *nil* and *cons*. By convention, the constructor functions are named by dropping the initial upper-case letter in the name of the non-recursive constructors to lower-case. To illustrate, we provide side-by-side comparisons of Haskell and two different uses of Nax.

| *Haskell* | *Nax with synonyms* | *Nax with derivation* |
|---|---|---|
| **data** *List a* | **data** $L : * \to * \to *$ **where** | **data** $L : * \to * \to * \to *$ **where** |
| $= Nil$ | $Nil : L\ a\ r$ | $Nil : L\ a\ r$ |
| $\mid\ Cons\ a\ (List\ a)$ | $Cons : a \to r \to L\ a\ r$ | $Cons : a \to r \to L\ a\ r$ |
| | **synonym** $List\ a = \mu^{[*]}\ (L\ a)$ | **deriving fixpoint** *List* |
| | $nil = \mathsf{In}^{[*]}\ Nil$ | |
| | $cons\ x\ xs = \mathsf{In}^{[*]}\ (Cons\ x\ xs)$ | |
| $x = Cons\ 3\ (Cons\ 2\ Nil)$ | $x = cons\ 3\ (cons\ 2\ nil)$ | $x = cons\ 3\ (cons\ 2\ nil)$ |

## 2.4 Mendler combinators for non-indexed types

There are no restrictions on what kind of datatypes can be defined in Nax. There are also no restrictions on the creation of values. Values are created using constructor functions, and the recursive injection ($\mathsf{In}^{[k]}$). To ensure strong normalization, analysis of constructed values has some restrictions. Values of non-recursive types can be freely analysed using pattern matching. Values of recursive types must be analysed using one of the Mendler-style combinators. By design, we limit pattern matching to values of non-recursive types, by *not* providing any mechanism to match against the recursive injection ($\mathsf{In}^{[k]}$).

To illustrate simple pattern matching over non-recursive types, we give a Nax multi-clause definition for the $\neg$ function over the (non-recursive) *Bool* type, and a function that strips off the *Just* constructor over the (non-recursive) *Maybe* type using a case expression.

$$\begin{aligned} \neg\ True &= False \\ \neg\ False &= True \end{aligned} \qquad \left| \qquad \begin{aligned} unJust0\ x = \mathbf{case}^{\{\}}\ x\ \mathbf{of}\ Just\ x &\to x \\ Nothing &\to 0 \end{aligned} \right.$$

Analysis of recursive data is performed with Mendler-style combinators. In our implementation we provide 5 Mendler style combinators: $\mathsf{MIt}^{\cdot}$ (fold or catamorphism or iteration), $\mathsf{MPr}^{\cdot}$ (primitive recursion), $\mathsf{Mcvlt}^{\cdot}$ (courses of values iteration), and *McvPr* (courses of values primitive recursion), and $\mathsf{Msflt}^{\cdot}$ (fold or catamorphism or iteration for recursive types with negative occurrences). A Mendler-style combinator appears similar to a case expression. It contains patterns, and the variables in the patterns are

scoped over a term, that is executed if that pattern matches. It differs from a case expression in that it also introduces additional names (or variables) into scope. These variables play a role similar in nature to the operations of an abstract datatype, and provide additional functionality over what can be done using just case analysis.

For a visual example, compare the **case** expression to the $\mathsf{MIt}^{\cdot}$ expression. In the **case**, each *clause* following the **of** indicates a possible match of the scrutinee $x$. In the $\mathsf{MIt}^{\cdot}$, each *equation* following the **with**, binds the variable $f$, and matches the pattern to a value related to the scrutinee $x$.

$$\begin{array}{l} \textbf{case}^{\{\}}\ x\ \textbf{of}\ \mathit{Nil} \quad \to e_1 \\ \qquad\qquad\ \mathit{Cons}\ x\ xs \to e_2 \end{array} \qquad \Big| \qquad \begin{array}{l} \mathsf{MIt}^{\{\}}\ x\ \textbf{with}\ f\ \ (\mathit{Cons}\ x\ xs) = e_1 \\ \qquad\qquad\qquad\quad\ f\ \ \mathit{Nil} \quad\quad = e_2 \end{array}$$

The number and type of the additional variables depends upon which family of Mendler combinators is used to analyze the scrutinee. Each equation specifies (a potential) computation in an abstract datatype depending on whether the pattern matches. For the $\mathsf{MIt}^{\cdot}$ combinator (above) the abstract datatype has the following form. The scrutinee, $x$ is a value of some recursive type $(\mu^{[*]}\ T)$ for a non-recursive type constructor $T$. In each clause, the pattern has type $(T\ r)$, for some abstract type $r$. The additional variable introduced ($f$) is an operator over the abstract type, $r$, that can safely manipulate only abstract values of type $r$.

Different Mendler style combinators are implemented by different abstract types. Each abstraction safely describes a class of provably terminating computations over a recursive type. The number (and type) of abstract operations differs from one family of Mendler combinators to another. We give descriptions of three families of Mendler combinators, their abstractions, and the types of the operators within the abstraction, below. In each description, the type *ans* represents the result type, when the Mendler combinator is fully applied.

$$\begin{array}{l} \mathsf{MIt}^{\{\}}\ x\ \textbf{with} \\ \quad f\ \ p_i = e_i \\ \\ x\ : \mu^{[*]}\ T \\ f\ : r \to \mathit{ans} \\ \\ p_i : T\ r \\ e_i : \mathit{ans} \\ \\ \mathsf{MIt}^{\{\psi\}}\ \varphi\ (\mathsf{In}^{[*]}\ x) \\ \quad = \varphi\ (\mathsf{MIt}^{\{\psi\}}\ \varphi)\ x \end{array} \qquad \Big| \qquad \begin{array}{l} \mathsf{MPr}^{\{\}}\ x\ \textbf{with} \\ \quad f\ \ \mathit{cast}\ \ p_i = e_i \\ \\ x\ : \mu^{[*]}\ T \\ f\ : r \to \mathit{ans} \\ \mathit{cast} : r \to \mu^{[*]}\ T \\ p_i : T\ r \\ e_i : \mathit{ans} \\ \\ \mathsf{MPr}^{\{\psi\}}\ \varphi\ (\mathsf{In}^{[*]}\ x) \\ \quad = \varphi\ (\mathsf{MPr}^{\{\psi\}}\ \varphi)\ (\mathsf{In}^{[*]})\ x \end{array} \qquad \Big| \qquad \begin{array}{l} \mathsf{McvIt}^{\{\}}\ x\ \textbf{with} \\ \quad f\ \ \mathit{project}\ \ p_i = e_i \\ \\ x\ \ \ : \mu^{[*]}\ T \\ f\ \ \ : r \to \mathit{ans} \\ \mathit{project} : r \to T\ r \\ p_i\ \ \ : T\ r \\ e_i\ \ \ : \mathit{ans} \\ \\ \mathsf{McvIt}^{\{\psi\}}\ \varphi\ (\mathsf{In}^{[*]}\ x) \\ \quad = \varphi\ (\mathsf{McvIt}^{\{\psi\}}\ \varphi)\ \mathit{out}\ x \\ \quad \textbf{where}\ \mathit{out}\ (\mathsf{In}^{[*]}\ x) = x \end{array}$$

A Mendler-style combinator implements a (provably terminating) recursive function applied to the scrutinee. The abstract type and its operations ensure termination. Note that every operation above includes an abstract operator, $f : r \to \mathit{ans}$. This operation represents a recursive call in the function defined by the Mendler-style combinator. Other operations, such as *cast* and *project*, support additional functionality within the abstraction in which they are defined ($\mathsf{MPr}^{\cdot}$ and $\mathsf{McvIt}^{\cdot}$ respectively). The equations at the bottom of each section provide an operational understanding of how the operator works. These can be safely ignored until after we see some examples of how a Mendler-style combinator works in practice.

$$\mathit{length}\ y \quad = \mathsf{MIt}^{\{\}}\ y \quad \textbf{with}\ \mathit{len}\ \mathit{Nil} \qquad = \mathit{zero}$$

$$
\begin{array}{lll}
 & & \mathit{len}\ (\mathit{Cons}\ x\ xs) = (\mathit{succ}\ \mathit{zero}) + \mathit{len}\ xs \\
\mathit{tail}\ x = \mathsf{MPr}^{\{\}}\ x & \textbf{with} & \mathit{tl}\ \mathit{cast}\ \mathit{Nil} = \mathit{nil} \\
 & & \mathit{tl}\ \mathit{cast}\ (\mathit{Cons}\ y\ ys) = \mathit{cast}\ ys \\
\mathit{factorial}\ x = \mathsf{MPr}^{\{\}}\ x & \textbf{with} & \mathit{fact}\ \mathit{cast}\ \mathit{Zero} = \mathit{succ}\ \mathit{zero} \\
 & & \mathit{fact}\ \mathit{cast}\ (\mathit{Succ}\ n) = \mathit{times}\ (\mathit{succ}\ (\mathit{cast}\ n))\ (\mathit{fact}\ n) \\
\mathit{fibonacci}\ x = \mathsf{Mcvlt}^{\{\}}\ x & \textbf{with} & \mathit{fib}\ \mathit{out}\ \mathit{Zero} = \mathit{succ}\ \mathit{zero} \\
 & & \mathit{fib}\ \mathit{out}\ (\mathit{Succ}\ n) = \textbf{case}^{\{\}}\ (\mathit{out}\ n)\ \textbf{of} \\
 & & \qquad \mathit{Zero} \to \mathit{succ}\ \mathit{zero} \\
 & & \qquad \mathit{Succ}\ m \to \mathit{fib}\ n + \mathit{fib}\ m
\end{array}
$$

The *length* function uses the simplest kind of recursion where each recursive call is an application to a direct subcomponent of the input. Operationally, *length* works as follows. The scrutinee, $y$, has type $(\mu^{[*]}\ (L\ a))$, and has the form $(\mathsf{In}^{[*]}\ x)$. The type of $y$ implies that $x$ must have the form *Nil* or $(\mathit{Cons}\ x\ xs)$. The $\mathsf{Mlt}^{\cdot}$ strips off the $\mathsf{In}^{[*]}$ and matches $x$ against the *Nil* and $(\mathit{Cons}\ x\ xs)$ patterns. If the *Nil* pattern matches, then 0 is returned. If the $(\mathit{Cons}\ x\ xs)$ pattern matches, $x$ and $xs$ are bound. The abstract type mechanism gives the pattern $(\mathit{Cons}\ x\ xs)$ the type $(L\ a\ r)$, so $(x : a)$ and $(xs : r)$ for some abstract type $r$. The abstract operation, $(\mathit{len} : r \to \mathit{Int})$, can safely be applied to $xs$, obtaining the length of the tail of the original list. This value is incremented, and then returned. The $\mathsf{Mlt}^{\cdot}$ abstraction provides a safe way to allow the user to make recursive calls, *len*, but the abstract type, $r$, limits its use to direct subcomponents, so termination is guaranteed.

Some recursive functions need direct access, not only to the direct subcomponents, but also the original input as well. The Mendler-style combinator $\mathsf{MPr}^{\cdot}$ provides a safe, yet abstract mechanism, to support this. The Mendler $\mathsf{MPr}^{\cdot}$ abstraction provides two abstract operations. The recursive caller with type $(r \to \mathit{ans})$ and a casting function with type $(r \to \mu^{[k]}\ T)$. The casting operation allows the user to recover the original type from the abstract type $r$, but since the recursive caller only works on the abstract type $r$, the user cannot make a recursive call on one of these cast values. The functions *factorial* (over the natural numbers) and *tail* (over lists) are both defined using $\mathsf{MPr}^{\cdot}$.

Note how in *factorial* the original input is recovered (in constant time) by taking the successor of casting the abstract predecessor, $n$. In the *tail* function, the abstract tail, $ys$, is cast to get the answer, and the recursive caller is not even used.

Some recursive functions need direct access, not only to the direct subcomponents, but even deeper subcomponents. The Mendler-style combinator $\mathsf{Mcvlt}^{\cdot}$ provides a safe, yet abstract mechanism, to support this. The function *fibonacci* is a classic example of this kind of recursion. The Mendler $\mathsf{Mcvlt}^{\cdot}$ provides two abstract operations. The recursive caller with type $(r \to \mathit{ans})$ and a projection function with type $(r \to T\ r)$. The projection allows the programmer to observe the hidden $T$ structure inside a value of the abstract type $r$. In the *fibonacci* function above, we name the projection *out*. It is used to observe if the abstract predecessor, $n$, of the input, $x$, is either zero, or the successor of the second predecessor, $m$, of $x$. Note how recursive calls are made on the direct predecessor, $n$, and the second predecessor, $m$.

Mendler observed well, did Mendler? –KYA that each operator can be defined by the equation at the bottom of its figure. Each operation can be given a naive type involving $(\mu^{[*]}\ T)$, but if we instead give it a more abstract type, abstracting values of type $(\mu^{[*]}\ T)$ into some unknown abstract type $r$, one can safely guarantee a certain pattern of use that insures termination. Informally, if the operation works for some unknown type $r$ it will certainly also work for the actual type $(\mu^{[*]}\ T)$, but because it cannot assume that $r$ has any particular structure, the user is forced to use the abstract operations in carefully proscribed ways.

## 2.5 Types with static indices

Recall that a type can have both parameters and indices, and that indices can be either types or terms. We define three types below each with one or more indices. Each example defines a non-recursive type, and then uses derivation to define synonyms for its fix point and recursive constructor functions. By convention, in each example, the argument that abstracts the recursive components is called *r*. By design, arguments appearing before *r* are understood to be parameters, and arguments appearing after *r* are understood to be indices. To define a recursive type with indices, it is necessary to give the argument, *r*, a higher-order kind. That is, *r* should take indices as well, since it abstracts over a recursive type which takes indices.

**data** $Nest : (* \to *) \to * \to *$ **where**
  $Tip \quad : a \to Nest\ r\ a$
  $Fork \quad : r\ (a,a) \to Nest\ r\ a$
    **deriving fixpoint** *PowerTree*

**data** $V : * \to (Nat \to *) \to Nat \to *$ **where**
  $Vnil \quad : V\ a\ r\ \{\text{`}zero\}$
  $Vcons : a \to r\ \{n\} \to V\ a\ r\ \{\text{`}succ\ n\}$
    **deriving fixpoint** *Vector*

**data** $Tag = E \mid O$

**data** $P : (Tag \to Nat \to *) \to Tag \to Nat \to *$ **where**
  $Base \quad : P\ r\ \{E\}\ \{\text{`}zero\}$
  $StepO : r\ \{O\}\ \{i\} \to P\ r\ \{E\}\ \{\text{`}succ\ i\}$
  $StepE : r\ \{E\}\ \{i\} \to P\ r\ \{O\}\ \{\text{`}succ\ i\}$
    **deriving fixpoint** *Proof*

Note, to distinguish type indices from term indices (and to make parsing unambiguous), we enclose term indices in braces ($\{...\}$). We also backquote (‘) variables in terms that we expect to be bound in the current environment. Un-backquoted variables are taken to be universally quantified. By backquoting *succ*, we indicate that we want terms, which are applications of the successor function, but not some universally quantified function variable[1]. For non-recursive types without parameters, the kind of the fixpoint is the same as the kind of the recursive argument *r*. If the non-recursive type has parameters, the kind of the fixpoint will be composed of the parameters $\to$ the kind of the recursive argument *r*. For example, study the kinds of the fixpoints for the non-recursive types declared above in the table below.

| non-recursive type | *Nest* | *V* | *P* |
|---|---|---|---|
| recursive type | *PowerTree* | *Vector* | *Proof* |
| kind of *T* | $* \to *$ | $* \to Nat \to *$ | $Tag \to Nat \to *$ |
| kind of *r* | $* \to *$ | $Nat \to *$ | $Tag \to Nat \to *$ |
| number of parameters | 0 | 1 | 0 |
| number of indices | 1 (type) | 1 (term) | 2 (term,term) |

Recall, indices are used to track static properties about values with those types. A well formed (*PowerTree x*) contains a balanced set of parenthesized binary tuples of elements. The index, *x*, describes what kind

[1] In the design of Nax we had a choice. Either, explicitly declare each universally quantified variable, or explicitly mark those variables not universally quantified. Since quantification is much more common than referring to variables already in scope, the choice was easy.

of values are nested in the parentheses. The invariant is that the number of items nested is always an exact power of 2. A (*Vector a* $\{n\}$) is a list of elements of type $a$, with length exactly equal to $n$, and a (*Proof* $\{E\}$ $\{n\}$) witnesses that the natural number $n$ is even, and a (*Proof* $\{O\}$ $\{m\}$) witnesses that the natural number $m$ is odd. Some example value with these types are given below.

$$
\begin{aligned}
&\mathit{tree1} : \mathit{PowerTree\ Int} = \mathit{tip}\ 3 \\
&\mathit{tree2} : \mathit{PowerTree\ Int} = \mathit{fork}\ (\mathit{tip}\ (2,5)) \\
&\mathit{tree3} : \mathit{PowerTree\ Int} = \mathit{fork}\ (\mathit{fork}\ (\mathit{tip}\ ((4,7),(0,2)))) \\
&\mathit{v2} : \mathit{Vector\ Int}\ \{\mathit{succ}\ (\mathit{succ}\ \mathit{zero})\} = (\mathit{vcons}\ 3\ (\mathit{vcons}\ 5\ \mathit{vnil})) \\
&\mathit{p1} : P\ \{O\}\ \{\mathit{succ}\ \mathit{zero}\} \quad\quad = \mathit{stepE}\ \mathit{base} \\
&\mathit{p2} : P\ \{E\}\ \{\mathit{succ}\ (\mathit{succ}\ \mathit{zero})\} = \mathit{stepO}\ (\mathit{stepE}\ \mathit{base})
\end{aligned}
$$

Note that in the types of the terms above, the indices in braces ($\{...\}$) are ordinary terms (not types). In these example we use natural numbers (e.g., *succ* (*succ zero*)) and elements ($E$ and $O$) of the two-valued type *Tag*. It is interesting to note that sometimes the terms are of recursive types (e.g., *Nat* which is a synonym for $\mu^{[*]}\ N$), and some are non-recursive types (e.g., *Tag*).

## 2.6 Mendler-style combinators for indexed types

Mendler-style combinators generalize naturally to indexed types. The key observation that makes this generalization possible is that the types of the operations within abstraction have to be generalized to deal with the type indices in a consistent manner. How this is done is best first explained by example, and then later abstracted to its full general form.

Recall, a value of type (*PowerTree Int*) is a nested, parenthesized what does parenthesized mean? –KYA, set of integers, where the number of integers is an exact power of 2. Consider a function that adds up all those integers. One wants a function of type (*PowerTree Int* $\to$ *Int*). One strategy to writing this function is to write a more general function of type (*PowerTree a* $\to (a \to \mathit{Int}) \to \mathit{Int}$). In Nax, we can do this as follows:

$$
\begin{aligned}
&\mathit{genericSum}\ t = \mathsf{MIt}^{\{a.\,(a\to \mathit{Int})\to \mathit{Int}\}}\ t\ \textbf{with} \\
&\qquad\qquad \mathit{sum}\ (\mathit{Tip}\ x) \quad = \lambda f \to f\ x \\
&\qquad\qquad \mathit{sum}\ (\mathit{Fork}\ x) = \lambda f \to \mathit{sum}\ x\ (\lambda(a,b) \to f\ a + f\ b) \\
&\mathit{sumTree}\ t = \mathit{genericSum}\ t\ (\lambda x \to x)
\end{aligned}
$$

In general, the type of the result of a function over an indexed type, can depend upon what the index is. Thus, a Mendler-style combinator over a value with an indexed type, must be type-specialized to that value's index. Different values of the same general type, will have different indices. After all, the role of an index is to witness an invariant about the value, and different values might have different invariants. Capturing this variation is the role of the clause $\{a\,.\,(a \to \mathit{Int}) \to \mathit{Int}\}$ following the keyword $\mathsf{MIt}^{\cdot}$. We call such a clause, an *index transformer*. In the same way that the type of the result depends upon the index, the type of the different components of the abstract datatype implementing the Mendler-style combinator also depend upon the index. In fact, everything depends upon the index in a uniform way. The index transformer captures this uniformity. One cannot abstract over the index transformer in Nax. Each Mendler-style combinator, over an indexed type, must be supplied with a concrete clause (inside the braces) that describe how the results depend upon the index. To see how the transformer is used,

study the types of the terms in the following paragraph. Can you see the relation between the types and the transformer?

The scrutinee $t$ has type (*PowerTree a*) which is a synonym for $((\mu^{[*\to *]}\ Nest)\ a)$. The recursive caller *sum* has type $(\forall\, a\,.\, r\ a \to (a \to Int) \to Int)$, for some abstract type constructor $r$. Recall $r$ has an index, so it must be a type constructor, not a type. The patterns (*Tip x*) and (*Fork x*) have type (*Nest r a*) and the right hand sides of the equations: $(\lambda f \to f\ x)$ and $(\lambda f \to sum\ x\ (\lambda(a,b) \to f\ a + f\ b))$, have type $((a \to Int) \to Int)$. Note that the dependency of $((a \to Int) \to Int)$ on the index $a$, appears in both the result type, and the type of the recursive caller. If we think of an index transformer, like $\{a\,.\,(a \to Int) \to Int\}$, as a function: $\psi\ a = (a \to Int) \to Int$, we can succinctly describe the types of the abstract operations in the MIt· Mendler abstraction. In the table below, we put the general case on the left, and terms from the *genericSum* example, that illustrate the general case, on the right.

$\mathsf{MIt}^{\{\psi\}}\ x$ **with**
$f\ p_i = e_i$

| | | | |
|---|---|---|---|
| $\psi : \kappa \to *$ | $\{a\,.\,(a \to Int) \to Int\}$ | : | $* \to *$ |
| $T : (\kappa \to *) \to \kappa \to *$ | $Nest$ | : | $(* \to *) \to * \to *$ |
| $x : (\mu^{[\kappa \to *]}\ T)\ a$ | $t$ | : | $(\mu^{[* \to *]}\ Nest)\ a$ |
| $f : \forall\ (a : \kappa)\,.\, r\ a \to \psi\ a$ | $sum$ | : | $\forall\ (a : *)\,.\, r\ a \to (a \to Int) \to Int$ |
| $p_i : T\ r\ a$ | $Fork\ x$ | : | $Nest\ r\ a$ |
| $e_i : \psi\ a$ | $\lambda f \to f\ x$ | : | $(a \to Int) \to Int$ |

The same scheme for MIt· generalizes to type constructors with term indices, and with multiple indices. To illustrate this we give the generic schemes for type constructors with 2 or 3 indices. In the table the variables $\kappa_1$, $\kappa_2$, and $\kappa_3$, stand for arbitrary kinds (either kinds for types, like $*$, or kinds for terms, like *Nat* or *Tag*).

| | |
|---|---|
| $T : (\kappa_1 \to \kappa_2 \to *) \to (\kappa_1 \to \kappa_2 \to *)$ | $T : (\kappa_1 \to \kappa_2 \to \kappa_3 \to *) \to (\kappa_1 \to \kappa_2 \to \kappa_3 \to^*)$ |
| $\psi : \kappa_1 \to \kappa_2 \to *$ | $\psi : \kappa_1 \to \kappa_2 \to \kappa_3 \to *$ |
| $x : (\mu^{[\kappa_1 \to \kappa_2 \to *]}\ T)\ a\ b$ | $x : (\mu^{[\kappa_1 \to \kappa_2 \to \kappa_3 \to *]}\ T)\ a\ b\ c$ |
| $f : \forall\ (a : \kappa_1)\ (b : \kappa_2)\,.\, r\ a\ b \to \psi\ a\ b$ | $f : \forall\ (a : \kappa_1)\ (b : \kappa_2)\ (c : \kappa_3)\,.\, r\ a\ b\ c \to \psi\ a\ b\ c$ |
| $p_i : T\ r\ a\ b$ | $p_i : T\ r\ a\ b\ c$ |
| $e_i : \psi\ a\ b$ | $e_i : \psi\ a\ b\ c$ |

The simplest form of index transformation, is where the transformation is a constant function. This is the case of the function that computes the integer length of a natural-number, length-indexed, list (what we called a *Vector*). Independent of the length the result is an integer. Such a function has type: $Vector\ a\ \{n\} \to Int$. We can write this as follows:

$$vlen\ x = \mathsf{MIt}^{\{\{i\}.Int\}}\ x\ \textbf{with}\ \begin{array}{ll} len\ Vnil & = 0 \\ len\ (Vcons\ x\ xs) & = 1 + len\ xs \end{array}$$

Let's study an example with a more interesting index transformation. A term with type $(Proof\ \{E\}\ \{n\})$, which is synonymous with the type $(\mu^{[Tag \to Nat \to *]}\ P\ \{E\}\ \{n\})$, witnesses that the term $n$ is even. Can we transform such a term into a proof that $n+1$ is odd? We can generalize this by writing a function which has both of the types below:
$Proof\ \{E\}\ \{n\} \to Proof\ \{O\}\ \{\text{`}succ\ n\}$, and
$Proof\ \{O\}\ \{n\} \to Proof\ \{E\}\ \{\text{`}succ\ n\}$.

We can capture this dependency by defining the term-level function *flip*, and using an $\mathsf{MIt}^{\cdot}$ with the index transformer: $\{\{t\}\,\{i\}\,.\,Proof\,\{\text{`}flip\,t\}\,\{\text{`}succ\,i\}\}$.

$$
\begin{array}{l}
flip\ E = O \\
flip\ O = E \\
flop\ x = \mathsf{MIt}^{\{\{t\}\,\{i\}.\,Proof\,\{\text{`}flip\,t\}\,\{\text{`}succ\,i\}\}}\ x\ \textbf{with} \\
\qquad\begin{array}{ll}
f\ Base & = stepE\ base \\
f\ (StepO\ p) & = stepE\ (f\ p) \\
f\ (StepE\ p) & = stepO\ (f\ p)
\end{array}
\end{array}
$$

For our last term-indexed example, every length-indexed list has a length, which is either even or odd. We can witness this fact by writing a function with type: $Vector\ a\ \{n\} \to Either\ (Even\ \{n\})\ (Odd\ \{n\})$. Here, *Even* and *Odd* are synonyms for particular kinds of *Proof*. To write this function, we need the index transformation: $\{\{n\}\,.\,Either\ (Even\ \{n\})\ (Odd\ \{n\})\}$.

$$
\begin{array}{l}
\textbf{synonym}\ Even\ \{x\} = Proof\ \{E\}\ \{x\} \\
\textbf{synonym}\ Odd\ \ \{x\} = Proof\ \{O\}\ \{x\} \\
proveEvenOrOdd\ x = \mathsf{MIt}^{\{\{n\}.\,Either\ (Even\ \{n\})\ (Odd\ \{n\})\}}\ x\ \textbf{with} \\
\qquad\begin{array}{ll}
prEOO\ Vnil & = Left\ base \\
prEOO\ (Vcons\ x\ xs) & = \textbf{case}^{\{\}}\ prEOO\ xs\ \textbf{of} \\
 & \qquad\begin{array}{ll}
Left\ p & \to Right\ (stepE\ p) \\
Right\ p & \to Left\ (stepO\ p)
\end{array}
\end{array}
\end{array}
$$

## 2.7 Recursive types of unrestricted polarity but restricted elimination

In Nax, programmers can define recursive data structures with both positive and negative polarity. The classic example is a datatype encoding the syntax of $\lambda$-calculus, which uses higher-order abstract syntax (HOAS). Terms in the $\lambda$-calculus are either variables, applications, or abstractions. In a HOAS representation, one uses Nax functions to encode abstractions. We give a two level description for recursive $\lambda$-calculus *Term*s, by taking the fixpoint of the non-recursive *Lam* datatype.

$$
\begin{array}{l}
\textbf{data}\ Lam : * \to * \to *\ \textbf{where} \\
\quad App :: r \to r \to Lam\ r \\
\quad Abs :: (r \to r) \to Lam\ r \\
\qquad \textbf{deriving fixpoint}\ Term \\
apply = abs\ (\lambda f \to abs\ (\lambda x \to app\ f\ x))
\end{array}
$$

Note that we don't need to include a constructor for variables, as variables are represented by Nax variables, bound by Nax functions. For example the lambda term: $(\lambda f.\lambda x.f\ x)$ is encoded by the Nax term *apply* above.

Note also, the recursive constructor: $abs : (Term \to Term) \to Term$, introduced by the **deriving fixpoint** clause, has a negative occurrence of the type *Term*. In a language with unrestricted analysis, such a type could lead to non-terminating computations. The Mendler $\mathsf{MIt}^{\cdot}$ and $\mathsf{MPr}^{\cdot}$ operators limit the analysis of such types in a manner that precludes non-terminating computations. The Mendler-style combinator,

$\mathsf{Mcvlt}^{\cdot}$, is too expressive to exclude non-terminating computations, and must be restricted to recursive datatypes with no negative occurrences.

Even though $\mathsf{Mlt}^{\cdot}$ and $\mathsf{MPr}^{\cdot}$ allow us to safely operate on values of type *Term*, they are not expressive enough to write many interesting functions. Fortunately, there is a more expressive Mendler style operation that is safe over recursive types with negative operations. We call this operator $\mathsf{Msflt}^{\cdot}$. This operator is based upon an interesting programming trick, first described by Sheard and Fegaras [], hence the "sf" in the name $\mathsf{Msflt}^{\cdot}$. The abstraction supported by $\mathsf{Msflt}^{\cdot}$ is as follows:

$$\begin{array}{l|l} \mathsf{Msflt}^{\{\}}\ x\ \textbf{with} & x \ : \mu^{[*]}\ T \\ \quad f\ inv\ p_i = e_i & f \ : r \to ans \\ & inv : ans \to r \\ & p_i \ : T\ r \\ & e_i \ : ans \end{array}$$

To use $\mathsf{Msflt}^{\cdot}$ the inverse allows one to cast an answer into an abstract value. To see how this works, study the function that turns a *Term* into a string. The strategy is to write an auxiliary function, *showHelp* that takes an extra integer argument. Every time we encounter a lambda abstraction, we create a new variable, x*n* (see the function *new*), where *n* is the current value of the integer variable. When we make a recursive call, we increment the integer. In the comments (the rest of a line after -- ), we give the type of a few terms, including the abstract operations *sh* and *inv*.

```
                                  -- cat : List String → String
                                  -- new : Int → String
new n = cat ["x", show n]
                                  -- showHelp : Term → (Int → String)
                                  -- sh : r → (Int → String)
                                  -- inv : (Int → String) → r
                                  -- (λn → new m) : Int → String
showHelp x =
  Msflt{} x with
    sh inv (App x y) = λm → cat ["(", sh x m, " ", sh y m, ")"]
    sh inv (Abs f)   = λm → cat ["(fn ", new m, " => ", sh (f (inv (λn → new m))) (m+1), ")"]
showTerm x = showHelp x 0
showTerm apply : List Char = "(fn x0 => (fn x1 => (x0 x1)))"
```

The final line of the example above illustrates applying *showTerm* to *apply*. Recall that $apply = abs\ (\lambda f \to abs\ (\lambda x \to app\ f\ x))$, which is the HOAS representation of the $\lambda$-calculus term $(\lambda f.\lambda x.f\ x)$.

## 2.8 Lessons from Nax

Nax is our first attempt to build a strongly normalizing, sound and consistent logic, based upon Mendler style iteration. We would like to emphasize the lessons we learned along the way.

- Writing types as the fixed point of a non-recursive type constructor is quite expressive. It supports a wide variety of types including the regular types (*Nat* and *List*), nested types (*PowerTree*), GADTs (*Vector*), and mutually recursive types (*Even* and *Odd*).
- Two-level types, while expressive, are a pain to program with (all those $\mu^{[\kappa]}$ and $\mathsf{In}^{[\kappa]}$ annotations), so a strong synonym or macro facility is necessary. With syntactic support, one hardly even notices.

- The use of term-indexed types allows programmers to write types that act as logical relations, and form the basis for reasoning about programs. Formalizing this is a large part of a sequel to this paper.
- Using Mendler-style combinators is expressive, and with syntactic support (the **with** equations of the Mendler operations), is easy to use. In fact Nax programs are often no more complicated than their Haskell counterparts.
- Type inference is an important feature of a programming language. We hope you noticed, that apart from index transformers, no type information is supplied in any of the Nax examples. The Nax compiler reconstructs all type information.
- Index transformers are the minimal information needed to extend Hindley-Milner type inference over GADTs. One can always predict where they are needed, and the compiler can enforce that the programmer supplies them. They are never needed for non-indexed types. Nax faithfully extends Hindley-Milner type inference.

The next few chapters formalize the theory behind Nax. We want Nax to be a sound and consistent logic. In the future we want Nax programs to include both a logical fragment, and a non-logical (or programatic) fragment, and we want the type system to separate the two. Our approach to formalizing the logical Nax, is to embed each feature of Nax into a lower level language known to be strongly normalizing. Our approach of distinguishing type and term indices is unique, and requires the extension of some previous work on normalizing calculi. It is the subject of the sequel.

# 3 System $\mathsf{F}_i$

System $\mathsf{F}_i$ is a higher-order polymorphic lambda calculus with term indices. In other words, System $\mathsf{F}_i$ is an extension of System $\mathsf{F}_\omega$ by term indices. The complete syntax and rules of $\mathsf{F}_i$ are described in Figure 1 and Figure 2. The syntax and rules highlighted by grey boxes are the extensions new to $\mathsf{F}_i$, which are not originally part of $\mathsf{F}_\omega$. That is, the system we obtain by excluding all the grey boxes from Figure 1 and Figure 2 is a version of $\mathsf{F}_\omega$. In particular, it is a version of $\mathsf{F}_\omega$ with Curry style terms and typing contexts separated into two zones (i.e., type level and term level). Terms are Curry style. That is, term level abstractions are unannotated ($\lambda x.t$), and type generalization ($\forall I$) and type instantiation ($\forall E$) are implicit at term level. Types remain Church style as usual. That is, type level abstractions are annotated by kinds ($\lambda X^\kappa.F$). Typing contexts are separated into type level contexts ($\Delta$) and term level contexts ($\Gamma$). We expect readers to be familiar to $\mathsf{F}_\omega$ and focus on describing new constructs of $\mathsf{F}_i$, which are in grey boxes.

## 3.1 The constructs new to $\mathsf{F}_i$

**Typing contexts** Typing contexts are split into two zones: type level contexts ($\Delta$) for type level bindings and term level contexts ($\Gamma$) for term level bindings. We have a new form of index variable bindings ($i^A$) that can appear in type level contexts in addition to type variable bindings ($X^\kappa$). There is only one form of term level binding ($x : A$) that can appear in term level contexts.

A type level context $\Delta$ is well-formed when it is either empty, extended by a type variable binding $X^\kappa$ whose kind $\kappa$ is well-sorted under $\Delta$, or extended by an index binding $i^A$ whose type $A$ is well-kinded under the empty type level context. Similarly to the well-sorted rule ($Ri$) for indexed arrow kinds, we

**Syntax:**

$$\begin{array}{lrcl}
\text{Kinds} & \kappa & ::= & * \mid \kappa \to \kappa \mid A \to \kappa \\
\text{Type Constructors} & A,B,F,G & ::= & X \mid \lambda X^{\kappa}.F \mid \lambda i^{A}.F \mid F\,G \mid F\,\{s\} \mid A \to B \mid \forall X^{\kappa}.B \mid \forall i^{A}.B \\
\text{Terms} & r,s,t & ::= & x \mid i \mid \lambda x.t \mid r\ s \\
\text{Typing Contexts} & \Delta & ::= & \cdot \mid \Delta, X^{\kappa} \mid \Delta, i^{A} \\
 & \Gamma & ::= & \cdot \mid \Gamma, x : A
\end{array}$$

**Well-formed typing contexts:**

$$\boxed{\vdash \Delta} \qquad \frac{}{\vdash \cdot} \qquad \frac{\vdash \Delta \quad \Delta \vdash \kappa : \square}{\vdash \Delta, X^{\kappa}} \left(X \notin \mathsf{dom}(\Delta)\right) \qquad \frac{\vdash \Delta \quad \cdot \vdash A : *}{\vdash \Delta, i^{A}} \left(i \notin \mathsf{dom}(\Delta)\right)$$

$$\boxed{\Delta \vdash \Gamma} \qquad \frac{\vdash \Delta}{\Delta \vdash \cdot} \qquad \frac{\Delta \vdash \Gamma \quad \Delta \vdash A : *}{\Delta \vdash \Gamma, x : A} \left(x \notin \mathsf{dom}(\Gamma)\right)$$

**Sorting:** $\boxed{\vdash \kappa : \square}$

$$(A)\ \frac{}{\vdash * : \square} \qquad (R)\ \frac{\vdash \kappa : \square \quad \vdash \kappa' : \square}{\vdash \kappa \to \kappa' : \square} \qquad (Ri)\ \frac{\cdot \vdash A : * \quad \vdash \kappa : \square}{\vdash A \to \kappa : \square}$$

**Kinding:** $\boxed{\Delta \vdash F : \kappa}$

$$(Var)\ \frac{X^{\kappa} \in \Delta \quad \vdash \Delta}{\Delta \vdash X : \kappa} \qquad (Conv)\ \frac{\Delta \vdash A : \kappa \quad \Delta \vdash \kappa = \kappa' : \square}{\Delta \vdash A : \kappa'}$$

$$(\lambda)\ \frac{\Delta, X^{\kappa} \vdash F : \kappa'}{\Delta \vdash \lambda X^{\kappa}.F : \kappa \to \kappa'} \qquad (@)\ \frac{\Delta \vdash F : \kappa \to \kappa' \quad \Delta \vdash G : \kappa}{\Delta \vdash F\,G : \kappa'}$$

$$(\lambda i)\ \frac{\Delta, i^{A} \vdash F : \kappa}{\Delta \vdash \lambda i^{A}.F : A \to \kappa} \qquad (@i)\ \frac{\Delta \vdash F : A \to \kappa \quad \Delta; \cdot \vdash s : A}{\Delta \vdash F\,\{s\} : \kappa}$$

$$(\to)\ \frac{\Delta \vdash A : * \quad \Delta \vdash B : *}{\Delta \vdash A \to B : *} \qquad (\forall)\ \frac{\Delta, X^{\kappa} \vdash B : *}{\Delta \vdash \forall X^{\kappa}.B : *} \qquad (\forall i)\ \frac{\Delta, i^{A} \vdash B : *}{\Delta \vdash \forall i^{A}.B : *}$$

**Typing:** $\boxed{\Delta; \Gamma \vdash t : A}$

$$(:)\ \frac{x : A \in \Gamma \quad \Delta \vdash \Gamma}{\Delta; \Gamma \vdash x : A} \qquad (:i)\ \frac{i^{A} \in \Delta \quad \Delta \vdash \Gamma}{\Delta; \Gamma \vdash i : A} \qquad (=)\ \frac{\Delta; \Gamma \vdash t : A \quad \Delta \vdash A = B : *}{\Delta; \Gamma \vdash t : B}$$

$$(\to I)\ \frac{\Delta; \Gamma, x : A \vdash t : B}{\Delta; \Gamma \vdash \lambda x.t : A \to B} \qquad (\to E)\ \frac{\Delta; \Gamma \vdash r : A \to B \quad \Delta; \Gamma \vdash s : A}{\Delta; \Gamma \vdash r\ s : B}$$

$$(\forall I)\ \frac{\Delta, X^{\kappa}; \Gamma \vdash t : B}{\Delta; \Gamma \vdash t : \forall X^{\kappa}.B} \qquad (\forall E)\ \frac{\Delta; \Gamma \vdash t : \forall X^{\kappa}.B \quad \Delta \vdash G : \kappa}{\Delta; \Gamma \vdash t : [G/X]B}$$

$$(\forall Ii)\ \frac{\Delta, i^{A}; \Gamma \vdash t : B}{\Delta; \Gamma \vdash t : \forall i^{A}.B} \left(i \notin \mathrm{FV}(t)\right) \qquad (\forall Ei)\ \frac{\Delta; \Gamma \vdash t : \forall i^{A}.B \quad \Delta; \cdot \vdash s : A}{\Delta; \Gamma \vdash t : [s/x]B}$$

Figure 1: Syntax and Typing rules of $\mathsf{F}_i$

**Kind equality:** $\boxed{\vdash \kappa = \kappa' : \Box}$

$$\frac{}{\vdash * = * : \Box} \qquad \frac{\vdash \kappa_1 = \kappa_1' : \Box \quad \vdash \kappa_2 = \kappa_2' : \Box}{\vdash \kappa_1 \to \kappa_2 = \kappa_1' \to \kappa_2' : \Box} \qquad \frac{\cdot \vdash A = A' : * \quad \vdash \kappa = \kappa' : \Box}{\vdash A \to \kappa = A' \to \kappa' : \Box}$$

$$\frac{\vdash \kappa = \kappa' : \Box}{\vdash \kappa' = \kappa : \Box} \qquad \frac{\vdash \kappa = \kappa' : \Box \quad \vdash \kappa' = \kappa'' : \Box}{\vdash \kappa = \kappa'' : \Box}$$

**Type constructor equality:** $\boxed{\Delta \vdash F = F' : \kappa}$

$$\frac{\Delta \vdash X : \kappa}{\Delta \vdash X = X : \kappa} \qquad \frac{\Delta, X^\kappa \vdash F : \kappa \quad \Delta \vdash G : \kappa}{\Delta \vdash (\lambda X^\kappa.F)\, G = [G/X]F : \kappa'} \qquad \frac{\Delta, i^A \vdash F : \kappa \quad \Delta; \cdot \vdash s : A}{\Delta \vdash (\lambda i^A.F)\,\{s\} = [s/x]F : \kappa}$$

$$\frac{\Delta, X^\kappa \vdash F = F' : \kappa'}{\Delta \vdash \lambda X^\kappa.F = \lambda X^\kappa.F' : \kappa \to \kappa'} \qquad \frac{\Delta \vdash F = F' : \kappa \to \kappa' \quad \Delta \vdash G = G' : \kappa}{\Delta \vdash F\, G = F'\, G' : \kappa'}$$

$$\frac{\Delta, i^A \vdash F = F' : \kappa}{\Delta \vdash \lambda i^A.F = \lambda i^A.F' : A \to \kappa} \qquad \frac{\Delta \vdash F = F' : A \to \kappa \quad \Delta; \cdot \vdash s = s' : A}{\Delta \vdash F\,\{s\} = F'\,\{s'\} : \kappa}$$

$$\frac{\Delta \vdash A = A' : * \quad \Delta \vdash B = B' : *}{\Delta \vdash A \to B = A' \to B' : *} \qquad \frac{\Delta, X^\kappa \vdash B = B' : *}{\Delta \vdash \forall X^\kappa.B = \forall X^\kappa.B' : *} \qquad \frac{\Delta, i^A \vdash B = B' : *}{\Delta \vdash \forall i^A.B = \forall i^A.B' : *}$$

$$\frac{\Delta \vdash F = F' : \kappa}{\Delta \vdash F' = F : \kappa} \qquad \frac{\Delta \vdash F = F' : \kappa \quad \Delta \vdash F' = F'' : \kappa}{\Delta \vdash F = F'' : \kappa}$$

**Term equality:** $\boxed{\Delta; \Gamma \vdash t = t' : A}$

$$\frac{\Delta; \Gamma \vdash x : A}{\Delta; \Gamma \vdash x = x : A} \qquad \frac{\Delta; \Gamma, x : A \vdash t : B \quad \Delta; \Gamma \vdash s : A}{\Delta; \Gamma \vdash (\lambda x.t)s = [s/x]t : B}$$

$$\frac{\Delta; \Gamma \vdash r = r' : A \to B \quad \Delta; \Gamma \vdash s = s' : A}{\Delta; \Gamma \vdash r\, s = r'\, s' : B}$$

$$\frac{\Delta; \Gamma \vdash t = t' : A}{\Delta; \Gamma \vdash t' = t : A} \qquad \frac{\Delta; \Gamma \vdash t = t' : A \quad \Delta; \Gamma \vdash t' = t'' : A}{\Delta; \Gamma \vdash t = t'' : A}$$

**Reduction:** $\boxed{t \rightsquigarrow t'}$

$$\frac{}{(\lambda x.t)\, s \rightsquigarrow [s/x]t} \qquad \frac{t \rightsquigarrow t'}{\lambda x.t \rightsquigarrow \lambda x.t'} \qquad \frac{r \rightsquigarrow r'}{r\, s \rightsquigarrow r'\, s} \qquad \frac{s \rightsquigarrow s'}{r\, s \rightsquigarrow r\, s'}$$

Figure 2: Equality rules and Reduction rules for $\mathsf{F}_i$

require $A$ of $i^A$ to be well-kinded in the empty type level context $(\cdot)$, since no bindings are introduced at kind level in $\mathsf{F}_i$.

A term level context $\Gamma$ is well-formed under a type level contexts $\Delta$ when it is either empty or extended by a term variable binding $x : A$ whose type $A$ is well-kinded under $\Delta$.

**Kinds and their sorting rules** We extend the kind syntax of $\mathsf{F}_\omega$ by indexed arrow kinds of the form $A \to \kappa$. The formation of indexed arrow kinds is governed by the sorting rule $(Ri)$. The rule $(Ri)$ specifies that an indexed arrow kind $A \to \kappa$ is well-sorted when $A$ is well-kinded under the empty type level context $(\cdot)$ and $\kappa$ is well-sorted. We avoid dependent kinds (i.e., kinds depending on type level or value level bindings) by requiring $\cdot \vdash A$. The type $A$ appearing in the index arrow kind $A \to \kappa$ must be well-kinded under the empty type level context $(\cdot)$, since no bindings are introduced at kind level in $\mathsf{F}_i$.

**Type constructors and their kinding rules** We extend the type constructor syntax by three constructs, and extend the kinding rules accordingly for these new constructs.

$\lambda i^A.F$ is the type level abstraction over an index (or, index abstraction). Index abstractions introduce indexed arrow kinds by the kinding rule $(\lambda i)$. Note, we have a new form of binding $i^A$ in the kinding rule $(\lambda i)$. We will explain what this binding means when we discuss contexts.

$F\,\{s\}$ is the type level index application. In contrast to the ordinary type level application $(F\,G)$ whose argument being applied is a type constructor $(G)$, the argument of the index application $(F\,\{s\})$ is a term $(s)$. We use the curly bracket notation around the index argument to emphasize the distinction from ordinary type arguments and also to emphasize that $s$ is an index term, which is erasable. Index applications eliminate indexed arrow kinds by the kinding rule $(@i)$. Note, we type check the index term $(s)$ under the current type level context paired with the empty term level context $(\Delta; \cdot)$ since we do not want the index term $(s)$ to depend on any term level bindings.

$\forall i^A.B$ is an index polymorphic type. The formation of indexed polymorphic types is governed by the kinding rule $\forall i$, which is very similar to the formation rule $(\forall)$ for ordinary polymorphic types.

In addition to the rules $(\lambda i)$, $(@i)$, and $(\forall i)$, we need a conversion rule $(Conv)$ at kind level. This is because the new extension to the kind syntax $A \to \kappa$ involves types. Since kind syntax involves types, we need more than simple structural equality over kinds. The equality over kinds is the usual structural equality extended by type equality when comparing indexed arrow kinds (see Figure 2).

**Terms and their typing rules** The term syntax is extended by index variables ($i$), since terms used as indices may have index variables as well as term variables (e.g., $\lambda i^A.F\{(\lambda x.x\ i)\,(\lambda x.x)\}$). The term variables $(x)$ are introduced from term level abstractions $(\lambda x.t)$. The index variables $(i)$ are introduced from index abstraction $(\lambda i^A.F)$ and index polymorphic types $(\forall i^A.B)$. However, the distinction between $x$ and $i$ is in fact only a convention for the convenience of readability. An equivalent but more succinct description of the system would be possible by having only $x$ for both term and index variables instead of having two kinds of variables $x$ and $i$.

Since $\mathsf{F}_i$ has index polymorphic types $(\forall i^A.B)$, we need typing rules for index polymorphism: $(\forall Ii)$ for index generalization and $(\forall Ei)$ for index instantiation.

The index generalization rule $(\forall Ii)$ is similar to the type generalization rule $(\forall I)$, except the additional side condition $\big(i \notin \mathrm{FV}(t)\big)$. This side condition prevents terms from accessing the type level index variables introduced by index polymorphism. Otherwise, without this side condition, $\forall$-binder would be no longer behave as polymorphism but powerful enough to behave as dependent functions, which are

usually denoted by the Π-binder in dependent type theories. The side condition on generalization rules for polymorphism is fairly standard in dependently typed languages supporting distinctions between polymorphism (or, erasable arguments) and dependent functions (e.g., IPTS[TODO cite Nathans' thesis], ICC[TODO cite]). The rule ($\forall I$) for ordinary type generalization rule does not need a side condition because type variables cannot appear in the syntax of terms.

The index instantiation rule ($\forall Ei$) is similar to the type instantiation rule ($\forall Ei$), except that we type check the index term $s$ to be instantiated for $i$ in the current type level context paired with the empty term level context $(\Delta;\cdot)$ rather than the current term level context. Since index terms are at type level, they should not depend on term level bindings.

In addition to the rules ($\forall Ii$) and ($\forall Ei$) for index polymorphism, we need an additional variable rule $(:i)$ to be able to access the index variables already in scope. Terms ($s$) used at type level in index applications ($F\{s\}$) should be able to access index variables already in scope. For example, $\lambda i^A.F\{i\}$ should be well-kinded under a context where $F$ is well-kinded, justified by the following derivation:

$$(\lambda i)\ \frac{(@i)\ \dfrac{\Delta, i^A \vdash F : A \to \kappa \qquad (:i)\ \dfrac{i^A \in \Delta, i^A \qquad \Delta \vdash \cdot}{\Delta, i^A; \cdot \vdash i : A}}{\Delta, i^A \vdash F\{i\} : \kappa}}{\Delta \vdash \lambda i^A.F\{i\} : \kappa}$$

## 3.2 Metatheory?

**Proposition 1** (well-formed type level context ensures well-sorted kinding judgement)**.**

$$\frac{\vdash \Delta \qquad \Delta \vdash F : \kappa}{\vdash \kappa : \Box}$$

*Proof.* Mutual induction on the derivation on the kinding judgement and the typing judgement since proof of this proposition and the next proposition depends on each other, but I'm a little bit confusing what exactly I need to induct on. –KYA

case (*Var*) Trivial by the second well-formedness rule of Δ.

case (*Conv*) By induction and a helper lemma that kind equality rules ensure that both sides of equality are well-sorted. This lemma should be straightforward to prove, but this lemma also is needs mutual induction with the lemma that type equality rules ensure that both sides of equality are well-kinded.

case ($\lambda$) By induction and the second well-formedness rule of Δ

case (@) By induction.

case ($\lambda i$) By induction and the third well-formedness rule of Δ.

case ($@i$) By induction provided that we can prove the next proposition that well-formed term level context ensures well-kinded typing judgement.

case ($\to$) Trivial since $\vdash * : \Box$.

case ($\forall$) Trivial since $\vdash * : \Box$.

case ($\forall i$) Trivial since $\vdash * : \Box$.

□

**Proposition 2** (well-formed term level context ensures well-kinded typing judgement)**.**

$$\frac{\Delta \vdash \Gamma \qquad \Delta;\Gamma \vdash t : A}{\Delta \vdash A : *}$$

*Proof.* The same induction principle as the previous proposition since the proof of these propositions are mutually recursive.

case (:) Trivial by the second well-formedness rule of $\Gamma$.

case (: $i$) Trivial by the third the well-formedness rule of $\Delta$.

case (=) By induction and a helper lemma that type equality rules ensure that both sides of equality are well-kinded. This lemma should be straightforward to prove, but mutually inductive proof with the lemma on kind equality rules, which we used in the proof of the previous proposition.

case ($\to I$) By induction and well-formedness of $\Gamma$.

case ($\to E$) By induction.

case ($\forall I$) By induction and well-formedness of $\Delta$.

case ($\forall E$) TODO some sort of substitution lemma?

case ($\forall Ii$) By induction and well-formedness of $\Delta$.

case ($\forall Ei$) TODO some sort of substitution lemma?

□

After going through the proof sketch for the two propositions above, I relaized that the rules for $\mathsf{F}_i$ needs more well-typeness and well-kindness conditions (e.g., in ($\forall I$) and ($\forall Ii$)), unlike $\mathsf{F}_\omega$. We need some adjustment on the $\mathsf{F}_i$ rules. –KYA

**Proposition 3** (anti-dependency on arrow kinds)**.**

$$\frac{\vdash \Delta, X^\kappa \qquad \Delta, X^\kappa \vdash F : \kappa'}{X \notin \mathrm{FV}(\kappa')}$$

**Proposition 4** (anti-dependency on indexed arrow kinds)**.**

$$\frac{\vdash \Delta, i^A \qquad \Delta, i^A \vdash F : \kappa}{i \notin \mathrm{FV}(\kappa)}$$

**Proposition 5** (anti-dependency on arrow types)**.**

$$\frac{\Delta \vdash \Gamma, x : A \qquad \Delta;\Gamma, x : A \vdash t : B}{x \notin \mathrm{FV}(B)}$$

*Remark* 1. Our system is more strong??? than anti-dependency on arrow types TODO

**Definition 1** (index erasure)**.**

$\boxed{\kappa^\circ}$ $\quad *^\circ = * \quad (\kappa \to \kappa')^\circ = \kappa^\circ \to \kappa^\circ \quad (A \to \kappa)^\circ = \kappa$

$\boxed{F^\circ}$ $\quad X^\circ = X \quad (\lambda X^\kappa.F)^\circ = \lambda X^{\kappa^\circ}.F^\circ \quad (\lambda i^A.F)^\circ = F^\circ \quad (F\ G)^\circ = F^\circ\ G^\circ \quad (F\ \{s\})^\circ = F^\circ$
$(A \to B)^\circ = A^\circ \to B^\circ \quad (\forall X^\kappa.B)^\circ = \forall X^{\kappa^\circ}.B^\circ \quad (\forall i^A.B)^\circ = B^\circ$

$\boxed{\Delta^\circ}$ $\quad \cdot^\circ = \cdot \quad (\Delta, X^\kappa)^\circ = \Delta^\circ, X^{\kappa^\circ} \quad (\Delta, i^A)^\circ = \Delta^\circ$

$\boxed{\Gamma^\circ}$ $\quad \cdot^\circ = \cdot \quad (\Gamma, x : A)^\circ = \Gamma^\circ, x : A^\circ$

**Lemma 1** (index erasure on well-formed type level contexts)**.** *If* $\vdash \Delta$ *then* $\vdash \Delta^\circ$.
**Lemma 2** (index erasure on well-formed term level contexts)**.** *If* $\Delta \vdash \Gamma$ *then* $\Delta^\circ \vdash \Gamma^\circ$.
**Lemma 3** (index erasure on well-sorted kinds)**.** *If* $\vdash \Delta$ *and* $\Delta \vdash \kappa : \Box$ *then* $\Delta^\circ \vdash \kappa^\circ : \Box$.
**Lemma 4** (index erasure on well-kinded type constructors)**.** *If* $\vdash \Delta$ *and* $\Delta \vdash F : \kappa$ *then* $\Delta^\circ \vdash F^\circ : \kappa^\circ$.
**Theorem 1** (index erasure on well-typed terms)**.** *If* $\Delta \vdash \Gamma$ *and* $\Delta;\Gamma \vdash t : A$ *then* $\Delta^\circ;\Gamma^\circ \vdash t : A^\circ$.

# 4 Nax

## 4.1 Language definition

The Nax language definition is described in Figure 3 and Figure 4. Figure 3 illustrates syntax, reduction rules, and well-formedness conditions for typing contexts. Figure 4 illustrates sorting, kinding, and typing rules.

**Typing contexts** The typing context of Nax is separated into three zones. In addition to the two zones of $\mathsf{F}_i$(the type level context $\Delta$ and the term level context $\Gamma$), we have top level contexts ($\Sigma$). The top level contexts can contain three kinds of bindings: type constructor bindings ($T : \kappa$), data constructor bindings ($C : \sigma$), and top level variable bindings ($`x : \sigma$). These bindings are introduced from declarations ($D$). Type constructor bindings ($T : \kappa$) and data constructor bindings ($C : \sigma$) are introduced from datatype declarations (**data** $T : \ldots$ **where** $\ldots$). Top level variable bindings ($`x : \sigma$) are introduced from top level definitions ($`x = t$). The rules for well-formed contexts in Nax are similar to those rules in $\mathsf{F}_i$.

**Kinds and their sorting rules** The kind syntax of Nax is exactly the same as the kind syntax of $\mathsf{F}_i$. The sorting rules are the same as $\mathsf{F}_i$ except we judge the sorts of kinds under the top level context ($\Sigma$).

**Type constructors and their kinding rules** The syntax for type constructors of Nax is similar to $\mathsf{F}_i$, but different from $\mathsf{F}_i$ in two aspects.

Firstly, polymorphic types are separate out as type schemes ($\sigma$) in Nax since the type system of Nax is in flavour of Hindley-Milner to support type inference (or, reconstruction).

Secondly, there are no type level abstractions and index abstractions in Nax. Instead of defining type constructors expecting type arguments by abstraction and index abstraction at type level, Nax supports datatype declarations (**data** $T : \kappa$ **where** $\ldots$) and recursive type operators ($\mu^\kappa$) as language constructs.

Intuitively, the kinding rule for the recursive type operator should be $\Sigma \vdash \mu^\kappa : (\kappa \to \kappa) \to \kappa$. However, we restrict the recursive type operator ($\mu^\kappa$) only to be applied to datatypes ($T\,\overline{\tau}$). This restriction is evident in both the type constructor syntax in Figure 3 and the kinding rule ($\mu$) in Figure 4. What this restriction really excludes are nested applications of recursive type operators. For instance, $\mu^\kappa(\mu^{\kappa\to\kappa}F)$ where $F : (\kappa \to \kappa) \to \kappa \to \kappa$ is not allowed although it would be well-kinded under the less restrictive kinding rule ($\Sigma \vdash \mu^\kappa : (\kappa \to \kappa) \to \kappa$). Motivation behind this restriction is type inference. In order to infer a type for a Mendler style iterator, we need to restrict the form of its body since the body must be polymorphic over the indices (see (MIt) rule). In general, we do not want polymorphic types to be first class since we want type inference. One simple design choice is to allow case branches ($\varphi$) to have polymorphic types, or type schemes, and annotate case branches with index transformers ($\varphi^\psi$). For the exact same reason (i.e., type inference), we restrict the body of the Mendler style iterators be case terms (i.e., ($\mathsf{MIt}\ x.\varphi^\psi$) instead of ($\mathsf{MIt}\ x.t$)).

**Syntax:**

| | |
|---|---|
| Kinds | $\kappa ::= * \mid \kappa \to \kappa \mid A \to \kappa$ |
| Type Constructors | $F,G,A,B ::= X \mid T \mid \mu^{\kappa}(T\,\overline{\tau}) \mid F\ G \mid F\,\{s\} \mid A \to B$ |
| Type Schemes | $\sigma ::= A \mid \forall X.\sigma \mid \forall i.\sigma$ |
| Terms | $r,s,t ::= x \mid `x \mid i \mid \lambda x.t \mid r\ s \mid \mathbf{let}\ x = s\ \mathbf{in}\ t \mid \varphi^{\psi} \mid \mathsf{MIt}\ x.\varphi^{\psi} \mid \mathsf{In}^{\kappa}$ |
| Program | $Prog ::= \overline{D};t$ |
| Declarations | $D ::= \mathbf{data}\ T : \overline{K} \to * \ \mathbf{where}\ \overline{C : \overline{A} \to T\,\overline{\tau}} \ \mid\ `x = t$ |
| List of Declarations | $\overline{D} ::= \cdot \mid D,\overline{D}$ |
| Kind Arguments | $K ::= \kappa \mid A$ |
| Type Arguments | $\tau ::= G \mid \{s\}$ |
| Type Argument Variables | $\iota ::= X \mid i$ |
| Index Transformers | $\psi ::= \cdot \mid \overline{\iota}.B$ |
| Case Branches | $\varphi ::= \overline{C\,\overline{x} \to t}$ |
| Contexts | $\Sigma ::= \cdot \mid \Sigma, T : \kappa \mid \Sigma, C : \sigma \mid \Sigma, `x : \sigma$ |
| | $\Delta ::= \cdot \mid \Delta, X^{\kappa} \mid \Delta, i^{\sigma}$ |
| | $\Gamma ::= \cdot \mid \Gamma, x : \sigma$ |

**Well-formed contexts:**

$$\boxed{\vdash \Sigma} \quad \frac{}{\vdash \cdot} \qquad \frac{\vdash \Sigma \qquad \Sigma \vdash \kappa : \square}{\vdash \Sigma, T : \kappa}\,\big(T \notin \mathsf{dom}(\Sigma)\big)$$

$$\frac{\vdash \Sigma \qquad \Sigma;\cdot \vdash \sigma : *}{\vdash \Sigma, C : \sigma}\,\big(C \notin \mathsf{dom}(\Sigma)\big) \qquad \frac{\vdash \Sigma \qquad \Sigma;\cdot \vdash \sigma : *}{\vdash \Sigma, `x : \sigma}\,\big(`x \notin \mathsf{dom}(\Sigma)\big)$$

$$\boxed{\Sigma \vdash \Delta} \quad \frac{\vdash \Sigma}{\Sigma \vdash \cdot} \qquad \frac{\Sigma \vdash \Delta \qquad \Sigma \vdash \kappa : \square}{\Sigma \vdash \Delta, X^{\kappa}}\,\big(X \notin \mathsf{dom}(\Delta)\big) \qquad \frac{\Sigma \vdash \Delta \qquad \Sigma;\cdot \vdash \sigma : *}{\Sigma \vdash \Delta, i^{\sigma}}\,\big(i \notin \mathsf{dom}(\Delta)\big)$$

$$\boxed{\Sigma;\Delta \vdash \Gamma} \quad \frac{\Sigma \vdash \Delta}{\Sigma;\Delta \vdash \cdot} \qquad \frac{\Sigma;\Delta \vdash \Gamma \qquad \Sigma;\Delta \vdash A : *}{\Sigma;\Delta \vdash \Gamma, x : A}\,\big(x \notin \mathsf{dom}(\Gamma)\big)$$

**Reduction:** $\boxed{t \rightsquigarrow t'}$

$$\frac{}{(\lambda x.t)\,s \rightsquigarrow [s/x]t} \qquad \frac{}{\mathbf{let}\ x = s\ \mathbf{in}\ t \rightsquigarrow [s/x]t}$$

$$\frac{C\,\overline{x} \to t \in \varphi}{\varphi^{\psi}(C\,\overline{t}) \rightsquigarrow [\overline{t}/\overline{x}]t} \qquad \frac{}{\mathsf{MIt}\ x.\varphi^{\psi}\ (\mathsf{In}^{\kappa}t) \rightsquigarrow [\mathsf{MIt}\ x.\varphi^{\psi}/x]\varphi^{\psi}\ t} \qquad \frac{`x = t \in \overline{D}}{`x \rightsquigarrow t}$$

$$\frac{t \rightsquigarrow t'}{\lambda x.t \rightsquigarrow \lambda x.t'} \qquad \frac{r \rightsquigarrow r'}{r\ s \rightsquigarrow r'\ s} \qquad \frac{s \rightsquigarrow s'}{r\ s \rightsquigarrow r\ s'} \qquad \frac{t_i \rightsquigarrow t_i'}{C\ t_1 \cdots t_i \cdots t_n \rightsquigarrow C\ t_1 \cdots t_i' \cdots t_n}$$

$$\frac{s \rightsquigarrow s'}{\mathbf{let}\ x = s\ \mathbf{in}\ t \rightsquigarrow \mathbf{let}\ x = s'\ \mathbf{in}\ t} \qquad \frac{t \rightsquigarrow t'}{\mathbf{let}\ x = s\ \mathbf{in}\ t \rightsquigarrow \mathbf{let}\ x = s\ \mathbf{in}\ t'} \qquad \frac{\varphi^{\psi} \rightsquigarrow \varphi'^{\psi}}{\mathsf{MIt}\ x.\varphi^{\psi} \rightsquigarrow \mathsf{MIt}\ x.\varphi'^{\psi}}$$

$$\frac{t_i \rightsquigarrow t_i'}{(C_1\,\overline{x_1} \to t_1;\cdots;C_i\,\overline{x_i} \to t_i;\cdots;C_n\,\overline{x_n} \to t_n)^{\psi} \ \rightsquigarrow\ (C_1\,\overline{x_1} \to t_1;\cdots;C_i\,\overline{x_i} \to t_i';\cdots;C_n\,\overline{x_n} \to t_n)^{\psi}}$$

Figure 3: Syntax and Reduction rules of Nax

**Sorting:**

$$\boxed{\Sigma \vdash \kappa : \Box} \quad (A)\frac{}{\Sigma \vdash * : \Box} \quad (R)\frac{\Sigma \vdash \kappa : \Box \quad \Sigma \vdash \kappa' : \Box}{\Sigma \vdash \kappa \to \kappa' : \Box} \quad (Ri)\frac{\Sigma;\cdot \vdash A : * \quad \Sigma \vdash \kappa : \Box}{\Sigma \vdash A \to \kappa : \Box}$$

**Kinding:** $\boxed{\Sigma;\Delta \vdash \sigma : \kappa}$ $(\forall)\dfrac{\Sigma;\Delta, X^{\kappa} \vdash \sigma : *}{\Sigma;\Delta \vdash \forall X.\sigma : *}$ $(\forall i)\dfrac{\Sigma;\Delta, i^{A} \vdash \sigma : *}{\Sigma;\Delta \vdash \forall i.\sigma : *}$

$$\boxed{\Sigma;\Delta \vdash F : \kappa} \quad (Var)\frac{X^{\kappa} \in \Delta \quad \Sigma \vdash \Delta}{\Sigma;\Delta \vdash X : \kappa} \quad (TCon)\frac{T : \kappa \in \Sigma \quad \Sigma \vdash \Delta}{\Sigma;\Delta \vdash T : \kappa} \quad (\mu)\frac{\Sigma;\Delta \vdash T\,\overline{\tau} : \kappa \to \kappa}{\Sigma;\Delta \vdash \mu^{\kappa}(T\,\overline{\tau}) : \kappa}$$

$$(@)\frac{\Sigma;\Delta \vdash F : \kappa \to \kappa' \quad \Sigma;\Delta \vdash G : \kappa}{\Sigma;\Delta \vdash F\,G : \kappa'} \quad (@i)\frac{\Sigma;\Delta \vdash F : A \to \kappa \quad \Sigma;\Delta;\cdot \vdash s : A}{\Sigma;\Delta \vdash F\,\{s\} : \kappa}$$

$$(\to)\frac{\Sigma;\Delta \vdash A : * \quad \Sigma;\Delta \vdash B : *}{\Sigma;\Delta \vdash A \to B : *} \quad (Conv)\frac{\Sigma;\Delta \vdash A : \kappa \quad \Sigma \vdash \kappa = \kappa' : \Box}{\Sigma;\Delta \vdash A : \kappa'}$$

**Typing:**

$$\boxed{\Sigma \vdash Prog : A} \quad (\cdot;t)\frac{\Sigma;\cdot;\cdot \vdash t : A}{\Sigma \vdash \cdot;t : A} \quad (D)\frac{\Sigma \vdash D \Rrightarrow \Sigma' \quad \Sigma' \vdash \overline{D};\, t : A}{\Sigma \vdash D, \overline{D};\, t : A}$$

$$\boxed{\Sigma;\Delta;\Gamma \vdash t : A} \quad (=)\frac{\Sigma;\Delta;\Gamma \vdash t : A \quad \Sigma;\Delta \vdash A = B : *}{\Sigma;\Delta;\Gamma \vdash t : B}$$

$$(:)\frac{x : \sigma \in \Gamma \quad \Sigma;\Delta \vdash A \prec \sigma \quad \Sigma;\Delta \vdash \Gamma}{\Sigma;\Delta;\Gamma \vdash x : A} \quad (:i)\frac{i^{\sigma} \in \Delta \quad \Sigma;\Delta \vdash A \prec \sigma \quad \Sigma;\Delta \vdash \Gamma}{\Sigma;\Delta;\Gamma \vdash i : A}$$

$$(:C)\frac{C : \sigma \in \Sigma \quad \Sigma;\Delta \vdash A \prec \sigma \quad \Sigma;\Delta \vdash \Gamma}{\Sigma;\Delta;\Gamma \vdash C : A} \quad (:\,`)\frac{`x : \sigma \in \Sigma \quad \Sigma;\Delta \vdash A \prec \sigma \quad \Sigma;\Delta \vdash \Gamma}{\Sigma;\Delta;\Gamma \vdash `x : A}$$

$$(\to I)\frac{\Sigma;\Delta;\Gamma, x : A \vdash t : B}{\Sigma;\Delta;\Gamma \vdash \lambda x.t : A \to B} \qquad (\to E)\frac{\Sigma;\Delta;\Gamma \vdash r : A \to B \quad \Sigma;\Delta;\Gamma \vdash s : A}{\Sigma;\Delta;\Gamma \vdash r\,s : B}$$

$$(\text{let})\frac{\Sigma;\Delta,\overline{\iota^{K}};\Gamma \vdash s : A \quad \Sigma;\Delta;\Gamma, x : \forall\overline{\iota}.A \vdash t : B}{\Sigma;\Delta;\Gamma \vdash \textbf{let}\ x = s\ \textbf{in}\ t : B}\ \begin{pmatrix}\overline{\iota} \cap \mathrm{FV}(s) = \emptyset \\ \overline{\iota} \cap \mathrm{FV}(\Gamma) = \emptyset\end{pmatrix} \quad (\text{case})\frac{\Sigma;\Delta;\Gamma \vdash^{\psi} \varphi : \forall\overline{\iota}.F\,\overline{\iota} \to \psi(\overline{\iota})}{\Sigma;\Delta;\Gamma \vdash \varphi^{\psi} : F\ \overline{\tau} \to \psi(\overline{\tau})}$$

$$(\text{MIt})\frac{\Sigma;\Delta, X^{\kappa};\Gamma, x : \forall\overline{\iota'}.X\overline{\iota'} \to \psi(\overline{\iota'}) \vdash^{\psi} \varphi : \forall\overline{\iota}.F\,X\,\overline{\iota} \to \psi(\overline{\iota})}{\Sigma;\Delta;\Gamma \vdash \mathsf{MIt}\ x.\varphi^{\psi} : \mu^{\kappa}F\ \overline{\tau} \to \psi(\overline{\tau})}\big(X \notin \mathrm{FV}(\Gamma)\big)$$

$$(\text{In})\frac{}{\Sigma;\Delta;\Gamma \vdash \mathsf{In}^{\kappa} : F(\mu^{\kappa}F)\,\overline{\tau} \to \mu^{\kappa}F\ \overline{\tau}}$$

$$\boxed{\Sigma;\Delta;\Gamma \vdash^{\psi} \varphi : \sigma} \quad \frac{\Sigma|_T = \overline{C_k : \sigma_k}^{\,k=1..n} \qquad \overline{\Sigma;\Delta \vdash \overline{A} \to T\,\overline{\tau}\,\overline{\tau}_k \prec \sigma_k \quad \Sigma;\Delta;\Gamma, \overline{x : A} \vdash t : \psi(\overline{\tau}_k)}^{\,k=1..n}}{\Sigma;\Delta;\Gamma \vdash^{\psi} \overline{C_k\,\overline{x} \to t}^{\,k=1..n} : \forall\overline{\iota}.T\,\overline{\tau}\,\overline{\iota} \to \psi(\overline{\iota})}$$

**Extending the Global Context:** $\boxed{\Sigma \vdash D \Rrightarrow \Sigma'}$

$$(\Sigma, T)\frac{\overline{\Sigma, T : \kappa;\ \overline{\iota^{K}} \vdash \overline{A} \to T\,\overline{\tau} : *}}{\Sigma \vdash \textbf{data}\ T : \kappa\ \textbf{where}\ \overline{C : \overline{A} \to T\,\overline{\tau}} \ \Rrightarrow\ \Sigma, T : \kappa, \overline{C : \forall\overline{\iota}.\overline{A} \to T\,\overline{\tau}}}$$

$$(\Sigma, `x)\frac{\Sigma;\overline{\iota^{K}};\cdot \vdash t : A}{\Sigma \vdash `x = t \Rrightarrow \Sigma, `x : \forall\overline{\iota}.A}\big(\overline{\iota} \cap \mathrm{FV}(t) = \emptyset\big)$$

Figure 4: Typing rules of Nax

**Terms and their typing rules** The term syntax of Nax has six additional term constructs than $\mathsf{F}_i$: data constructors ($C$), top level variables ($`x$), polymorphic let bindings (**let** $x = s$ **in** $t$), eliminators for datatypes ($\varphi^{\psi}$), Mendler style iterators ($\mathsf{Mlt}\, x.\varphi^{\psi}$), and constructors for recursive types ($\mathsf{In}^{\kappa}$). Typing rules for them are provided in Figure 4.

The typing rules (: $C$) and (: ‘) are for data constructors ($C$) and top level variables ($`x$) bound in the top level context ($\Sigma$). Data constructors ($C$) are introduced from datatype declarations (**data** $T : \kappa$ **where** ...) by the rule ($\Sigma, T$), and top level variables ($`x$) are introduced from top level definitions ($`x = t$) by the rule ($\Sigma, `x$). The typing rules (: $C$) and (: ‘) behave similar to the rule (:) for the variables and the rule (: $i$) for index variables. All these four rules (:), (: $i$), (: $C$), and (: ‘) for identifiers look up a certain context (one of the three zones $\Sigma$, $\Delta$, and $\Gamma$). Since the Nax type system is in flavour of Hindley-Milner, identifiers are bound to type schemes ($\sigma$) and the typing rules for the identifiers instantiate type schemes to types ($A$). Note, a type instantiation ($\Sigma; \Delta \vdash A \prec \sigma$) is a judgement under the top level context ($\Sigma$) and the type level context ($\Delta$), since the instantiated type needs to be well-kinded under $\Sigma$ and $\Delta$.

Polymorphic let bindings in Nax are just the usual polymorphic bindings of Hindley-Milner type system for generalizing types of local definitions into type schemes. In Nax, we generalize over term indices as well as types. The typing rule for let bindings is the (let) rule.

Eliminators for datatypes ($\varphi^{\psi}$), or case-terms, are case branches ($\varphi$) annotated by index transformers ($\psi$). For non-indexed types, case-terms are the usual single level pattern matching expressions in functional languages. For example, a Nax case-term applied to non-indexed typed term ($\varphi^{\cdot}\ s$) corresponds to a Haskell case-expression over that term (**case** $s$ **of** $\{\varphi\}$). Note, we give trivial index transformer annotation (i.e., $\psi = \cdot$) for non-indexed types (e.g., booleans, natural numbers) since there are no indices to worry about. For indexed types, the indexed transformer annotations proivide useful information for type reconstruction. For example, consider the following datatype declaration:

$$\begin{aligned}\textbf{data}\ \texttt{Judgement} : \texttt{Bool} \to * \ \textbf{where}\ \ & \texttt{TJ} : \texttt{Formula} \to \texttt{Judgement}\ \{\texttt{True}\};\\ & \texttt{FJ} : \texttt{Formula} \to \texttt{Judgement}\ \{\texttt{False}\}\end{aligned}$$

The datatype `Judgement` is index by boolean terms (e.g., `True` and `False` of type `Bool`). The data constructor `TJ` contains a formula expected to be true and the data constructor `FJ` contains a formula expected to be false. We can define a function, which produces an inverted judgement by negating the formula contained in a given judgement, as follows[2]:

$$\begin{pmatrix}\texttt{TJ}\ x \to \texttt{FJ}(\mathit{neg}\ x);\\ \texttt{FJ}\ x \to \texttt{TJ}(\mathit{neg}\ x)\end{pmatrix}^{i.\,\texttt{Judgement}\ \{`\mathit{not}\ i\}}$$

where *neg* is a function that produces negated formula and ‘*not* is a top level function that negates booleans.

Note that the index transformer ($i.\,\texttt{Judgement}\ \{`\mathit{not}\ i\}$) captures the idea that the resulting inverted judgement has opposite expectations from the given judgement. The types of such case-terms involving indexed types can also be inferred when we annotate the case-terms with appropriate index transformers. Reduction rules for case-terms (Figure 3) are standard.

Mendler style iterators ($\mathsf{Mlt}\, x.\varphi^{\psi}$) are eliminators for recursive types. A case-term expects a datatype argument (of type $T\,\overline{\tau}$). A Mendler style iterator expects a recursive type argument (of type $\mu^{\kappa}(T\,\overline{\tau})$). Intuitively, Mendler style iterators open up the recursive type ($\mu^{\kappa}(T\,\overline{\tau})$) and case branch over its base datatype structure (of type $T\,\overline{\tau}$). This intuition is captured by the reduction rule for Mendler style iterators (Figure 3): $\mathsf{Mlt}\, x.\varphi^{\psi}\ (\mathsf{In}^{\kappa} t) \rightsquigarrow [\mathsf{Mlt}\, x.\varphi^{\psi}/x]\varphi^{\psi}\ t$. Note that a Mendler style iterator ($\mathsf{Mlt}\, x.\varphi^{\psi}$) applied to a term of recursive type ($\mathsf{In}^{\kappa} t$) constructed by the $\mathsf{In}^{\kappa}$ constructor reduces to a case-term

[2] case branches are laid out in multiple lines for better readability

($[\mathsf{MIt}\, x.\varphi^{\psi}/x]\varphi^{\psi}$) applied to the base structure ($t$) contained in the $\mathsf{In}^{\kappa}$ constructor. The variable ($x$) bound by $\mathsf{MIt}$ is a label for the recursive call. Note that the case-term ($[\mathsf{MIt}\, x.\varphi^{\psi}/x]\varphi^{\psi}$) appearing in the reduction rule substitutes $x$ with the Mendler style iterator itself. However, unlike the fixpoint operator for unrestricted general recursion, Mendler style iterators are guaranteed to normalize because of their carefully designed typing rule (MIt) due to Mendler.

The constructors for recursive types ($\mathsf{In}^{\kappa}$) are standard (see rule (In) in Figure 4). The kind annotation $\kappa$ on the $\mathsf{In}^{\kappa}$ constructor aids kind inference. If we were to simulate the recursive type operator $\mu^{\kappa}$ and its constructor $\mathsf{In}^{\kappa}$ in a functional language like Haskell (with GADT and kind annotation extensions), we would simulate them by the following recursive datatype:

$$\textbf{data}\ \mu^{\kappa} : (\kappa \to \kappa) \to \kappa\ \textbf{where}\ \mathsf{In}^{\kappa} : X(\mu^{\kappa} X)\overline{\iota} \to \mu^{\kappa} X\, \overline{\iota}$$

However, such a simulation of $\mu^{\kappa}$ by a recursive datatype cannot guarantee normalization of the language, since unlimited elimination of $\mathsf{In}^{\kappa}$ via case branches is already powerful enough to encode non-terminating computation even without using any recursion at term level. Thus, Nax provides $\mu^{\kappa}$ and $\mathsf{In}^{\kappa}$ as primitive language constructs, and only allow elimination of $\mathsf{In}^{\kappa}$ via Mendler style iteration.

**Nax programs and their typing rules** A Nax program $(\overline{D};t)$ is a list of declarations $(\overline{D})$ followed by a term $(t)$. A declaration can be either a datatype declaration (**data** $T : \kappa$ **where** $\ldots$) or a top level definition ($`x = t$). The list of declarations $(\overline{D})$ are processed by the rules $(\Sigma, T)$ and $(\Sigma, `x)$ before type checking the term $(t)$. The kinding and typing information from the datatype declarations and the top level definitions preceding the term are captured into the top level context $(\Sigma)$ according to the rules $(\Sigma, T)$ and $(\Sigma, `x)$. The top level context extended by these rules are used for type checking the term following the list of declarations. Therefore, the sorting, kinding, and typing rules of Nax (Figure 4) involves $\Sigma$ in addtion to $\Delta$ and $\Gamma$, while the corresponding rule of $\mathsf{F}_i$ (Figure 1) involves $\Delta$ and $\Gamma$ only.

**Reduction rules** Reduction rules are defined in Figure 3. First five rules are the redex rules that makes an actual reduction step on redexes. A redex is be one of the following: a lambda term applied to an argument, a let binding, a case term applied to a constructor term, a Mendler style iterator applied to an $\mathsf{In}^{\kappa}$-constructed term, and a top level variable.

Note, the reduction rule for $`x$ mentions $\overline{D}$). Although we illustrate the reduction as a relation on terms ($t \rightsquigarrow t'$), we implicitly assume that there exists some fixed list of declarations $(\overline{D})$ for the reduction relation $(\rightsquigarrow)$. In order to make a reduction step for top level variables, we need to know the top level definition for $`x$, which should be contained in $\overline{D}$. Since the list of declarations are given by the input program $(\overline{D};t)$ to type check, it is non-ambiguous which $\overline{D}$ to use for reducing $`x$. In case when it is ambiguous, we could use a notation like $t \overset{\overline{D}}{\rightsquigarrow} t'$ to make it more precise.

The other rules, following the top level variable reduction rule ($`x \rightsquigarrow t$), are context rules to make a reduction step for the terms whose redexes appear inside their subterms.

**Equality over types and kinds** TODO

## 4.2 Syntax-directed type system

The kinding and typing rules of Nax illustrated in Figure 4 is not syntax directed since the conversion rules (*Conv*) and $(=)$ are not syntax directed. These conversion rules can apply to anywhere regardless of the syntactic category of terms and types.

We can easily adapt the system to be syntax directed by embedding the conversion rules into application-like rules (e.g., $(@i)$, $(\to E)$). We need to prove that the syntax directed system are equivalent to the standard system modulo conversion –KYA Among the kinding rules, the only place where conversion is truly necessary is in the index application rule $(@i)$. We can define the syntax directed application rule $(@i)_s$ as follows:

$$(@i)_s \frac{\Sigma;\Delta \vdash_s F : A \to \kappa \qquad \Sigma;\Delta;\cdot \vdash_s s : A' \qquad \Sigma;\cdot \vdash_s A = A' : *}{\Sigma;\Delta \vdash_s F\,\{s\} : \kappa}$$

Among the typing rules, we need to embed conversion into the $(\to E)$ rule and probably the rules (let) and (MIt), and the branch checking rule as well??? TODO

### 4.3 Type inference (or, reconstruction)

**Kinding:** $\boxed{\Sigma;\Delta \vdash \sigma \rhd \kappa}$

$$(\forall) \frac{X \leftarrow \mathit{frvar} \quad \Sigma;\Delta, X^\kappa \vdash \sigma \rhd *}{\Sigma;\Delta \vdash \forall X.\sigma \rhd *} \qquad (\forall i) \frac{i \leftarrow \mathit{frvar} \quad \Sigma;\Delta, i^A \vdash \sigma \rhd *}{\Sigma;\Delta \vdash \forall i.\sigma \rhd *}$$

$\boxed{\Sigma;\Delta \vdash F \rhd \kappa}$

$$(\mathit{Var}) \frac{X^\kappa \in \Delta \qquad \Sigma \vdash \Delta}{\Sigma;\Delta \vdash X \rhd \kappa} \qquad (\mathit{TCon}) \frac{T : \kappa \in \Sigma \qquad \Sigma \vdash \Delta}{\Sigma;\Delta \vdash T \rhd \kappa} \qquad (\mu) \frac{\Sigma;\Delta \vdash T\,\overline{\tau} : \kappa \to \kappa}{\Sigma;\Delta \vdash \mu^\kappa (T\,\overline{\tau}) : \kappa}$$

$$(@) \frac{\Sigma;\Delta \vdash F : \kappa \to \kappa' \qquad \Sigma;\Delta \vdash G : \kappa}{\Sigma;\Delta \vdash F\,G : \kappa'} \qquad (@i) \frac{\Sigma;\Delta \vdash F : A \to \kappa \qquad \Sigma;\Delta;\cdot \vdash s : A}{\Sigma;\Delta \vdash F\,\{s\} : \kappa}$$

$$(\to) \frac{\Sigma;\Delta \vdash A : * \qquad \Sigma;\Delta \vdash B : *}{\Sigma;\Delta \vdash A \to B : *}$$

**Typing:** $\boxed{\Sigma;\Delta;\Gamma \vdash t \rhd A}$

$$(:) \frac{x : \sigma \in \Gamma \quad A \leftarrow \mathit{inst}(\sigma)}{\Sigma;\Delta;\Gamma \vdash x \rhd A} \qquad (:i) \frac{i^\sigma \in \Delta \quad A \leftarrow \mathit{inst}(\sigma)}{\Sigma;\Delta;\Gamma \vdash i \rhd A} \qquad (:C) \frac{C : \sigma \in \Sigma \quad A \leftarrow \mathit{inst}(\sigma)}{\Sigma;\Delta;\Gamma \vdash C \rhd A} \qquad (:\text{`}) \frac{\text{`}x : \sigma \in \Sigma \quad A \leftarrow \mathit{inst}(\sigma)}{\Sigma;\Delta;\Gamma \vdash \text{`}x \rhd A}$$

$$(\to I) \frac{A \leftarrow \mathit{fresh} \quad \Sigma;\Delta;\Gamma, x : A \vdash t \rhd B}{\Sigma;\Delta;\Gamma \vdash \lambda x.t \rhd A \to B} \qquad (\to E) \frac{\Sigma;\Delta;\Gamma \vdash r \rhd A' \qquad \Sigma;\Delta;\Gamma \vdash s \rhd A \quad B \leftarrow \mathit{fresh} \qquad \mathit{unify}(A', A \to B)}{\Sigma;\Delta;\Gamma \vdash r\,s \rhd B}$$

$$(\mathrm{let}) \frac{\Sigma;\Delta;\Gamma \vdash s \rhd A \qquad \sigma \leftarrow \mathit{gen}(A) \quad \Sigma;\Delta;\Gamma, x : \sigma \vdash t \rhd B}{\Sigma;\Delta;\Gamma \vdash \mathbf{let}\ x = s\ \mathbf{in}\ t \rhd B} \qquad (\mathrm{In}) \frac{F \leftarrow \mathit{fresh} \qquad \overline{\tau} \leftarrow \mathit{fresh}^{|\kappa|}}{\Sigma;\Delta;\Gamma \vdash \mathsf{In}^\kappa \rhd F(\mu^\kappa F)\,\overline{\tau} \to \mu^\kappa F\,\overline{\tau}}$$

$$(\mathrm{case}) \frac{\Sigma;\Delta;\Gamma \vdash^\psi \varphi \rhd \sigma \quad A \leftarrow \mathit{inst}(\sigma)}{\Sigma;\Delta;\Gamma \vdash \varphi^\psi \rhd A} \qquad (\mathrm{MIt}) \frac{\begin{array}{c}\overline{K} \leftarrow \mathit{fresh}^{|\psi|} \qquad X \leftarrow \mathit{frvar} \qquad \kappa = \overline{K} \to * \qquad \overline{\imath'} \leftarrow \mathit{frvar}^{|\psi|} \\ \Sigma;\Delta, X^\kappa;\Gamma, x : \forall \overline{\imath'}.X\overline{\imath'} \to \psi(\overline{\imath'}) \vdash^\psi \varphi \rhd \sigma \qquad A \leftarrow \mathit{inst}(\sigma) \\ \overline{\tau} \leftarrow \mathit{fresh}^{|\psi|} \qquad F \leftarrow \mathit{fresh} \qquad \mathit{unify}(A,\ F\,X\,\overline{\tau} \to \psi(\overline{\tau}))\end{array}}{\Sigma;\Delta;\Gamma \vdash \mathsf{Mlt}\,x.\varphi^\psi : \mu^\kappa F\ \overline{\tau} \to \psi(\overline{\tau})}$$

$\boxed{\Sigma;\Delta;\Gamma \vdash^\psi \varphi \rhd \sigma}$

$$\frac{\Sigma|_T = \overline{C_k : \sigma_k}^{\,k=1..n} \qquad \Sigma;\cdot \vdash T \rhd \kappa \qquad \overline{\tau} \leftarrow \mathit{fresh}^{|\kappa|-|\psi|} \qquad \overline{\mathit{InferBranch}}^{\,k=1..n} \qquad \overline{\imath} \leftarrow \mathit{fresh}^{|\psi|}}{\Sigma;\Delta;\Gamma \vdash^\psi \overline{C_k\,\overline{x} \to t}^{\,k=1..n} \rhd \forall \overline{\imath}.T\,\overline{\tau}\,\overline{\imath} \to \psi(\overline{\imath})}$$

$$\text{where} \quad \mathit{InferBranch} \stackrel{\text{def}}{=} \overline{\tau}_k \leftarrow \mathit{fresh}^{|\psi|} \qquad B \leftarrow \mathit{inst}(\sigma_k) \qquad \overline{A} \leftarrow \mathit{fresh}^{|B|}$$
$$\mathit{unify}(B,\, \overline{A} \to T\,\overline{\tau}\,\overline{\tau}_k) \quad \Sigma;\Delta;\Gamma,\overline{x:A} \vdash t \rhd B' \quad \mathit{unify}(B',\ \psi(\overline{\tau}_k))$$

# 5 Embedding Nax into $\mathsf{F}_i$

TODO

# 6 Future Work

TODO

# 7 Conclusion

TODO

[1, 2] just dummy citation

# References

[1] A. Ut, H. Or & Co Author (1987): *Title A: An Article*. *Jounal* 443(21):4, doi:10.4204/EPTCS. Available at `http://arxiv.org/abs/1009.3306`. Note.

[2] A. Ut, H. Or & Co Author (1987): *Title B1: A Book with authors*, second edition. *Series* 443, Publisher, Address, doi:10.4204/EPTCS. Available at `http://arxiv.org/abs/1009.3306`. Note.