JFP **26**, e2, 61 pages, 2016.
doi:10.1017/S0956796816000022

Well-founded recursion with copatterns and sized types

ANDREAS ABEL

Department of Computer Science and Engineering
Gothenburg University, Sweden
(*e-mail:* andreas.abel@gu.se)

BRIGITTE PIENTKA

School of Computer Science, McGill University, Montreal, Canada
(*e-mail:* bpientka@cs.mcgill.ca)

Abstract

In this paper, we study strong normalization of a core language based on System F_ω which supports programming with finite and infinite structures. Finite data such as finite lists and trees is defined via constructors and manipulated via pattern matching, while infinite data such as streams and infinite trees is defined by observations and synthesized via copattern matching. Taking a type-based approach to strong normalization, we track size information about finite and infinite data in the type. We exploit the duality of pattern and copatterns to give a unifying semantic framework which allows us to elegantly and uniformly support both well-founded induction and coinduction by rewriting. The strong normalization proof is structured around Girard's reducibility candidates. As such, our system allows for non-determinism and does not rely on coverage. Since System F_ω is general enough that it can be the target of compilation for the Calculus of Constructions, this work is a significant step towards representing observation-based infinite data in proof assistants such as Coq and Agda.

1 Introduction

Integrating infinite data and coinduction with dependent types is tricky. For example, in the Calculus of (Co)Inductive Constructions, the core theory underlying Coq (INRIA, 2012), coinduction is broken, since computation does not preserve types (Giménez, 1996; Oury, 2008). In Agda (AgdaTeam, 2015), a dependently typed proof and programming environment based on Martin-Löf Type Theory, inductive and coinductive types cannot be mixed in a compositional way.[1] In previous work (Abel *et al.*, 2013), we have introduced *copatterns* as a novel perspective on defining infinite structures that might serve as a new foundation for coinduction in dependently typed languages, overcoming the problems in the present solutions.

[1] In Agda (up to version 2.4), one can encode the property "infinitely often" from temporal logic, but not its dual "eventually forever". Due to the limitations of the termination/guardedness checker, can only nest inductive types inside coinductive ones (needed for "infinitely often"), but not vice versa (needed for "eventually forever") (Altenkirch & Danielsson, 2012).

In the copattern approach, finite data such as finite lists and trees are defined as usual via constructors and manipulated via pattern matching, while infinite data such as streams and infinite trees are defined by observations and synthesized via copattern matching. For example, instead of conceiving streams as built by the constructor cons, we consider the observations head and tail about streams as primitive. Programs about streams are defined in terms of the observations head and tail.

Our previous work left the question of termination of recursive function and the productivity of infinite objects open. Both issues are crucial since we want to program inductive proofs as recursive functions and coinductive proofs as infinite objects or corecursive functions producing infinite objects. In this paper, we adapt type-based termination (Hughes *et al.*, 1996; Amadio & Coupet-Grimal, 1998; Barthe *et al.*, 2004; Blanqui, 2004; Abel, 2006; Abel, 2008b; Sacchini, 2011; Sacchini, 2013) to definitions by copatterns.

A syntactic termination check would ensure that recursive calls occur only with arguments smaller than the ones of the original call. In type-based termination, inductive types are tagged with a size expression that denotes the (ordinal) maximal height of the trees inhabiting it, i. e., an upper bound on the number of constructors in the longest path of the tree. To prove termination of a recursive function means to show that it can safely handle arguments of arbitrary size. This can be established by well-founded induction: to show that a function can handle arguments up to a fixed size a, we may assume it already safely processes arguments of any smaller size $b < a$. This induction principle can be turned into a typing rule for recursive functions, using sized types and size quantification. How can this be dualized to coinduction? A stream is *productive* if we can make arbitrarily deep observations, i. e., if we can take its tail arbitrarily many times. To show that a stream definition is productive, we also proceed by well-founded induction. To show that it can safely handle a observations, we may assume that b observations are fine for any $b < a$. The number of observations we can safely make is called the *depth* of the stream, or more generally, of the coinductive structure. One should not be mislead and think of the depth as "size"; streams do not have a size since they are not tree-structures in memory—they only exist as processes that continuously yield elements on demand. But it is fruitful to transfer the concept of *depth* to (co)recursive functions. The depth of a function is the maximal size of arguments it can safely handle. As we are only interested in streams of infinite depth in the end, we care only about functions of infinite depth. Yet to establish productivity and termination, we need to induct on depth.

The type-based termination approach is in contrast to common approaches taken in systems such as Coq and Agda (up to version 2.4) which employ a syntactic guardedness check to ensure that corecursive programs are productive: all corecursive calls must occur under a constructor. This ensures that the next unit of information can be computed in a finite amount of time (Sijtsma, 1989). However, this approach has also known limitations: it is difficult to handle higher order programs such as $g\, f = \mathsf{cons}\, 0\, (f\, (g\, f))$, where the productivity of g depends on the behavior of the function f. It is also not compositional, i. e., we cannot easily abstract

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

over a constructor cons in a productive program and replace it with a function f. Both limitations are due to the lack of information we have about f in the syntactic guardedness check. Types on the other hand already track information about each argument to a definition and its output. Type-based termination piggy-backs on the typing analysis and avoids a separate formal system to traverse the definitions. By indexing types with sizes, we are able to carry more precise information about input and output arguments and their relation which is then verified simultaneously while type checking the definitions.

The contributions of our work are:

- We present $\mathsf{F}_\omega^{\mathsf{cop}}$, an extension of System F_ω by inductive and coinductive types, sizes and bounded size quantification, pattern and copattern matching and lexicographic termination measures.
- In contrast to previous approaches on type-based termination, we use well-founded induction on ordinals instead of conventional induction that distinguishes between zero, successor and limit ordinals. Disposing of this case distinction, we may operate within constructive foundations of mathematics (Taylor, 1996).
- Well-founded induction leads to a construction of inductive types by inflationary iteration, which has been utilized to justify cyclic proofs in the sequent calculus (Sprenger & Dam, 2003). We seem to be the first to utilize inflationary iteration in a type system.
- Well-founded induction alleviates the need for a semi-continuity check for sized types of recursive functions (Hughes *et al.*, 1996; Abel, 2008b) which is, under loss of expressivity, sometimes reduced to a monotonicity check (Barthe *et al.*, 2004; Blanqui, 2004; Barthe *et al.*, 2008; Sacchini, 2013). Thus, we put type-based termination on leaner and easier understandable foundations.
- Since we construct infinite objects by copattern matching, standard rewriting becomes strongly normalizing even for corecursive definitions, and productivity becomes an instance of termination. Thus, we achieve a unified treatment of recursion and corecursion that is central to type-based termination.
- Our typing rules are formulated as a bidirectional type-checking algorithm that can be implemented as such, and has been, in MiniAgda (Abel, 2012). Further, sized types and copatterns have been integrated into Agda 2.4.
- We prove soundness of $\mathsf{F}_\omega^{\mathsf{cop}}$ by an untyped term model based on Girard's reducibility candidates. The proof exhibits semantic counterparts of pattern and copattern typing and accounts for incomplete and overlapping rewrite rules.

The paper is structured as follows: In Section 2, we review the idea of copatterns and describe size-based reasoning using several examples. This will motivate the design of the overall system and demonstrate the strength of the resulting language. In Section 3, we present grammar and typing rules of $\mathsf{F}_\omega^{\mathsf{cop}}$. From its operational semantics, we construct a term model based on Girard's reducibility candidates (Girard *et al.*, 1989) in Section 4 which shows strong normalization of well-typed terms. This result is finally extended to well-typed rewrite rules in Section 5.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

2 Copatterns and termination

Let us illustrate how to program with copatterns using a simple example of generating a stream of zeros. A streams s over an element type A is given by the two *observations* head and tail: We can inspect the head of s by applying the projection s .head and obtain an element of A. To obtain the tail of s, we use the projection s .tail. We can then define the stream of zeros recursively by the following two clauses:

$$\begin{aligned} \mathsf{zeros}\ .\mathsf{head} &= 0, \\ \mathsf{zeros}\ .\mathsf{tail} &= \mathsf{zeros}. \end{aligned}$$

More generally, zeros can be coded as repeat 0 with

$$\begin{aligned} \mathsf{repeat}\ a\ .\mathsf{head} &= a, \\ \mathsf{repeat}\ a\ .\mathsf{tail} &= \mathsf{repeat}\ a. \end{aligned}$$

The left-hand side (lhs) of each clause is considering the definiendum, here repeat, in a *copattern*, here $\cdot\ a$ .head and $\cdot\ a$ .tail, resp. A copattern consists of a hole, $\cdot$, applied to a sequence of patterns and/or projections. The hole is filled, e. g., by the definiendum. In this case, we have first a variable pattern, a, and then a projection head/tail.

The definition of repeat is *complete* because the given copatterns are covering all possible cases (Abel *et al.*, 2013). In this paper, we investigate the *termination* of definitions by copatterns if read as rewrite rules, regardless of their completeness. In systems without the copattern facility, repeat would be defined using a stream constructor cons as follows:

$$\mathsf{repeat}\ a = \mathsf{cons}\ a\ (\mathsf{repeat}\ a).$$

Read as rewrite rule, this equation leads immediately to non-termination; this is why in the absence of copatterns, one speaks about *productivity* instead of termination (Coquand, 1994). A definition is productive if it unfolds to an infinite stream in all cases—which certainly holds for repeat a. In the presence of copatterns, productivity is subsumed under plain termination.

Coming back to our copattern-based definition, we see that repeat a *terminates* in all contexts since it does not unfold by itself and consumes one projection in each unfolding. For example, projecting the $(n+1)$st element (counting from 0) of repeat a, i. e., repeat a .tail^{n+1} .head reduces in one step to repeat a .tail^{n} .head and after n more steps to repeat a .head.

There are many formalisms that ensure termination or productivity of recursive definitions. In this paper, we adapt type-based termination (Hughes *et al.*, 1996; Barthe *et al.*, 2004; Abel, 2006) to copatterns, i. e., we will present a type system that only accepts terminating definitions. There are good reasons to integrate termination checking into the type system, the foremost one is *compositionality*. Good type systems are defined in a compositional way, i. e., one can replace any expression with a different one of the same type without destroying well-typedness, in particular, one can replace a complex expression by a variable, abstracting from the concrete behavior or the expression. In contrast, syntactic termination checks often lack

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

similarly powerful means of abstraction. For instance, if we abstract the constructor

$$f\ a = \mathsf{cons}\ a$$

in the second, non-copattern definition of repeat, obtaining

$$\mathsf{repeat}\ a = f\ a\ (\mathsf{repeat}\ a),$$

then syntactic productivity checks such as constructor-counting will fail unless they have access to the definition of f. Put f into a different module and per-module termination checking will fail.

Type-based termination restores compositionality by giving function f a refined type that not only expresses that it takes an element and a stream and produces a stream, but also that the generated stream is extended by one element in the front. In this way, productivity of repeat is guaranteed by the typing of f, without need to reveal its definition. One could say that type-based termination facilitates *termination checking under assumptions.*

2.1 Example: Fibonacci

Let us look at programming with copatterns and type-based termination for a more interesting example, the stream of Fibonacci numbers. It can be elegantly implemented in terms of zipWith $f\ s\ t$ which pointwise applies the binary function f to the elements of streams s and t.

$$\begin{aligned}
\mathsf{zipWith}\ f\ s\ t\ .\mathsf{head} &= f\ (s\ .\mathsf{head})\ (t\ .\mathsf{head}) \\
\mathsf{zipWith}\ f\ s\ t\ .\mathsf{tail} &= \mathsf{zipWith}\ f\ (s\ .\mathsf{tail})\ (t\ .\mathsf{tail}) \\
\\
\mathsf{fib}\ .\mathsf{head} &= 0 \\
\mathsf{fib}\ .\mathsf{tail}\ .\mathsf{head} &= 1 \\
\mathsf{fib}\ .\mathsf{tail}\ .\mathsf{tail} &= \mathsf{zipWith}\ (+)\ \mathsf{fib}\ (\mathsf{fib}\ .\mathsf{tail}).
\end{aligned}$$

The last equation states in terms of streams that the $(n + 2)$nd element of the Fibonacci stream is the sum of the nth and the $(n + 1)$st. It looks like fib is a terminating definition since fib .tail .tail only refers to fib and fib .tail, thus, one projection is removed in each recursive call. However, termination of fib is also dependent on good properties of zipWith. For instance, the following faulty clause for zipWith would make fib .tail .tail .head loop:

$$\mathsf{zipWith}\ f\ s\ t\ .\mathsf{head} = f\ (s\ .\mathsf{tail}\ .\mathsf{head})\ (t\ .\mathsf{tail}\ .\mathsf{head})$$

$$\begin{aligned}
&\mathsf{fib}\ .\mathsf{tail}\ .\mathsf{tail}\ .\mathsf{head} \\
&\quad = \mathsf{zipWith}\ (+)\ \mathsf{fib}\ (\mathsf{fib}\ .\mathsf{tail})\ .\mathsf{head} \\
&\quad = (\mathsf{fib}\ .\mathsf{tail}\ .\mathsf{head}) + (\mathsf{fib}\ .\mathsf{tail}\ .\mathsf{tail}\ .\mathsf{head}) \\
&\quad = (\mathsf{fib}\ .\mathsf{tail}\ .\mathsf{head}) + (\mathsf{fib}\ .\mathsf{tail}\ .\mathsf{head}) + (\mathsf{fib}\ .\mathsf{tail}\ .\mathsf{tail}\ .\mathsf{head}) \\
&\quad = \ldots
\end{aligned}$$

The problem is that the faulty zipWith adds again one tail projection that has been removed in going from the original call fib .tail .tail to the recursive call fib .tail, thus, we are left with the same number of projections, leading to an infinite call cycle.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

What we learn from this counterexample is that in order to reason about termination of stream expressions, we need to trade the naive image of streams as infinite sequences for a notion of streams that can safely be subjected to α many projections, where $\alpha \leqslant \omega$ can be a natural number or (the smallest) infinity ω. We refer to such streams as *sized streams*, or streams having *depth* α. Clearly, if a stream of depth α is required, we can safely supply a stream of depth $\beta \geqslant \alpha$, thus, sized streams are subject to contravariant subtyping.

The original zipWith delivers, if called with input streams of depth α, an output stream of the same depth. This allows us to reason about the termination of fib as follows. We show that fib is a stream of arbitrary depth α by induction on $\alpha \leqslant \omega$. Cases $\alpha < 2$ are easy. The interesting case is $\alpha = n + 2$ when we take two tail projections and then another n projections, thus, $n+2$ projections in total. Then, we may assume (by induction hypothesis) that on the right-hand side (rhs) taking up to $n + 1$ projections of fib is fine, thus, fib and fib.tail behave well under another n projections—they both can be assigned depth n using subtyping. Passing them to zipWith (+) returns in turn a stream of the same depth n, hence the lhs fib.tail.tail can be assigned depth n and, consequently, fib depth $n + 2$, which was our goal.

The faulty zipWith, however, needs streams of depth $n + 1$ to deliver a stream of depth n. Since fib.tail can only safely be assumed to have depth n, not depth $n + 1$, the termination proof attempt fails, and rightfully so.

In this model proof, we assumed that taking a projection will decrease the depth by exactly one. In the following, we will loosen this assumption and let projections take us to any strictly smaller depth.

2.2 Type-based termination for copatterns

In this section, we present the key ideas behind $\mathsf{F}^{\mathsf{cop}}_{\omega}$, our polymorphic core language for type-based termination checking of recursive definitions involving inductive and coinductive types. We illustrate how the integration of size expressions into the type system captures and mechanizes the informal reasoning about termination employed in the previous section.

2.2.1 Size quantification for inductive and coinductive types

Besides quantification over types $\forall A{:}*.\, B$, we have quantification over sizes $\forall i{<}a.\, B$. To unify these two forms of quantification, we add to the base kind $*$ of types the base kinds $<a$ denoting sets of ordinals below a and conceive $\forall i{<}a.\, B$ as shorthand for $\forall i{:}(<a).\, B$. Thus, size expressions fall in the same syntactic class as type expressions. We introduce a special ordinal ∞, the closure ordinal for all (co)inductive types we consider. As far as streams are concerned, ∞ can be thought of as ω. In general, valid size expressions are of the form $a ::= i + n \mid \infty + n$, where i is a size variable and n a concrete number (we drop $+0$).

The type of streams of depth a over element type A will be denoted by $\mathsf{Stream}^a A$, and we consider the following typing rules for the projections:

$$\frac{s : \mathsf{Stream}^a A}{s.\mathsf{head} : \forall i{<}a^{\uparrow}.\, A} \qquad \frac{s : \mathsf{Stream}^a A}{s.\mathsf{tail} : \forall i{<}a^{\uparrow}.\, \mathsf{Stream}^i A}. \tag{1}$$

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

These rules state that if you want to project a stream of depth a, you will need to provide a *witness* that you are able to do so, i.e., an ordinal $i < a^{\uparrow}$. In case of tail, this witness serves also as the depth of the projected stream. For instance, if $s : \mathsf{Stream}^{i+2}A$, then $s.\mathsf{tail}\,(i+1).\mathsf{head}\,i : A$. *Bound normalization* $a^{\uparrow}$, defined by $(i+n)^{\uparrow} = i+n$ and $(\infty+n)^{\uparrow} = \infty+1$, allows us to turn bounds $a \geqslant \infty$ into $\infty+1$ and project from the fixpoint $\mathsf{Stream}^{\infty}A$ without information loss. For $s : \mathsf{Stream}^{\infty}A$, we have $s.\mathsf{tail}\,\infty : \mathsf{Stream}^{\infty}A$ since $\infty < \infty^{\uparrow} = \infty + 1$, reflecting that the tail of a fully defined stream has infinite depth as well.

In practice, we often use the following derived rules which eliminate the universal quantifier and directly compares sizes.

$$\frac{s : \mathsf{Stream}^{a}A}{s.\mathsf{head}\,b : A}\; b < a^{\uparrow} \qquad \frac{s : \mathsf{Stream}^{a}A}{s.\mathsf{tail}\,b : \mathsf{Stream}^{b}A}\; b < a^{\uparrow}.$$

More generally, following previous work (Abel *et al.*, 2013), we represent coinductive types as recursive records νR, with $R = \{d_1 : F_1; \ldots; d_n : F_n\}$ giving (sized) types to the projections $d_{1..n}$ as follows:

$$\frac{r : \nu^{a} R}{r.d_k : \forall i{<}a^{\uparrow}.\, F_k(\nu^{i} R)}.$$

For instance, with $\mathsf{Stream}^{i}\,A = \nu^{i}\{\mathsf{head} : \lambda X.\,A; \mathsf{tail} : \lambda X.\,X\}$, we obtain the typing of head and tail presented above Equation (1). Considering R as a finite map from projections to type constructors, we write R_{d_k} for F_k.

Dually, inductive types are recursive variants μS with $S = \langle c_1 : F_1; \ldots; c_n : F_n\rangle$ and constructor typing

$$\frac{t : \exists i{<}a^{\uparrow}.\, F_k(\mu^{i} S)}{c_k\, t : \mu^{a} S}.$$

For example, finite lists can be defined as $\mathsf{List}^{i}A = \mu^{i}\langle \mathsf{nil} : \lambda X.\,1;\ \mathsf{cons} : \lambda X.\,A \times X\rangle$. Integrating the quantifier rules, we derive the following inferences for constructors and destructors:

$$\frac{s : S_c(\mu^{b} S)}{c^{b} s : \mu^{a} S}\; b < a^{\uparrow} \qquad \frac{r : \nu^{a} R}{r.d\,b : R_d(\nu^{b} R)}\; b < a^{\uparrow}.$$

2.2.2 *Specifying termination measures*

The polymorphically typed version of zipWith officially looks as follows, where we write $\forall i{\leqslant}a$ as abbreviation for $\forall i{<}(a+1)$:

$$\begin{aligned}&\mathsf{zipWith} : \forall i{\leqslant}\infty.\,|i| \Rightarrow \forall A{:}*.\,\forall B{:}*.\,\forall C{:}*.\\ &\qquad (A \to B \to C) \to \mathsf{Stream}^{i}A \to \mathsf{Stream}^{i}B \to \mathsf{Stream}^{i}C\end{aligned}$$

$$\begin{aligned}&\mathsf{zipWith}\ i\ A\ B\ C\ f\ s\ t\ .\mathsf{head}\ j = f\ (s\ .\mathsf{head}\ j)\ (t\ .\mathsf{head}\ j)\\ &\mathsf{zipWith}\ i\ A\ B\ C\ f\ s\ t\ .\mathsf{tail}\ j\ \ = \mathsf{zipWith}\ j\ A\ B\ C\ f\ (s\ .\mathsf{tail}\ j)\ (t\ .\mathsf{tail}\ j).\end{aligned}$$

The first equation has type C and the second one type $\mathsf{Stream}^{j}C$. The kind of j is $<i$ due to the typing of head and tail, thus, zipWith is well-defined (and terminating)

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

by induction on its first argument, the size argument. The associated termination measure is located after the size variable(s) and, in general, a tuple $|a, b, c|$ of size expressions under the lexicographic order.[2] In this case, it is just the unary tuple $|i|$, meaning that the termination measure is just the value of size variable i. A type with an embedded termination measure is a blueprint to generate constrained types to check the recursive calls in the clauses. In the following, we give an intuition how this works; in detail, this is explained in Section 5.

2.2.3 High-level idea of size-based termination checking

When we check a corecursive definition such as the second clause of zipWith, we start with traversing the lhs. We first introduce assumption $i \leqslant \infty$ into the context and now hit the measure annotation $|i|$ in the type. At this point, we introduce the assumption $\mathsf{zipWith} : \forall j \leqslant \infty.\, |j| < |i| \Rightarrow \forall A{:}*.\, \forall B{:}*.\, \forall C{:}*.\, (A \to B \to C) \to \mathsf{Stream}^j A \to \mathsf{Stream}^j B \to \mathsf{Stream}^j C$ which will be used to check the recursive call on the rhs. It has a constraint $|j| < |i|$, a lexicographic comparison of size expression tuples (which here just means $j < i$), that is checked before applying $\mathsf{zipWith}\ j$ to A. Continued checking of the lhs introduces further assumptions $A, B, C : *$, $f : A \to B \to C$, $s : \mathsf{Stream}^i A$, $t : \mathsf{Stream}^i B$, and $j < i$. Checking the rhs succeeds since the constraint $|j| < |i|$ is satisfied and $s\ .\mathsf{tail}\ j : \mathsf{Stream}^j A$ and $t\ .\mathsf{tail}\ j : \mathsf{Stream}^j B$.

In the following, we abbreviate $\forall A{:}*$ to just $\forall A$ and $\forall i \leqslant \infty$ to just $\forall i$. With all size and type-arguments, the definition of the Fibonacci stream becomes:

$$
\begin{aligned}
&\mathsf{fib} \ : \ \forall i.\, |i| \Rightarrow \mathsf{Stream}^i \mathbb{N} \\
&\mathsf{fib}\ i\ .\mathsf{head}\ j \qquad\quad = 0 \\
&\mathsf{fib}\ i\ .\mathsf{tail}\quad j\ .\mathsf{head}\ k = 1 \\
&\mathsf{fib}\ i\ .\mathsf{tail}\quad j\ .\mathsf{tail}\quad k = \mathsf{zipWith}\ k\ \mathbb{N}\ \mathbb{N}\ \mathbb{N}\ (+)\ (\mathsf{fib}\, k)\ (\mathsf{fib}\, j\, .\mathsf{tail}\, k).
\end{aligned}
$$

In the last line, the lhs introduces size variables i and $j < i$ and $k < j$ and an assumption $\mathsf{fib} : \forall i'.\, |i'| < |i| \Rightarrow \mathsf{Stream}^{i'} \mathbb{N}$ and expects a rhs of type $\mathsf{Stream}^k \mathbb{N}$. Since $k < j < i$, both recursive calls are valid, and the expressions $\mathsf{fib}\, k$ and $\mathsf{fib}\, j\, .\mathsf{tail}\, k$ both have type $\mathsf{Stream}^k \mathbb{N}$. With $\mathsf{zipWith}\, k\, \mathbb{N}\, \mathbb{N}\, \mathbb{N} : \mathsf{Stream}^k \mathbb{N} \to \mathsf{Stream}^k \mathbb{N} \to \mathsf{Stream}^k \mathbb{N}$, the rhs is well-typed, and fib is terminating.

2.3 Example: Colists

So far, we have only looked at streams, which have a single constructor. Colists are lists that are a possibly infinite sequence of cons, but may also terminate with a nil constructor. Semantically, the type of colists $\mathsf{CoList}\, A$ is the greatest fixpoint of the

[2] The notation for termination measures is taken from Xi (2002).

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

following functor $\mathsf{F}\,A$, or the terminal F-coalgebra:

$$\begin{aligned}
&\mathsf{F}\ A\ X &&= \mu^{\infty}\{\mathsf{nil} : \lambda_.\ 1; \mathsf{cons} : \lambda_.\ A \times X\}\\
&\mathsf{CoList}^i\ A &&= \nu^{i}\{\mathsf{out} : \lambda X.\ \mathsf{F}\ A\ X\}
\end{aligned}$$

$$\begin{aligned}
&\mathsf{fmap}_1\ :\ \forall A{:}*.\forall B{:}*.\forall X{:}*.\ (A \to B) \to \mathsf{F}\ A\ X \to \mathsf{F}\ B\ X\\
&\mathsf{fmap}_1\ A\ B\ X\ f\ (\mathsf{nil}\ _) &&= \mathsf{nil}\,()\\
&\mathsf{fmap}_1\ A\ B\ X\ f\ (\mathsf{cons}\ a\ x) &&= \mathsf{cons}\ (f\ a)\ x
\end{aligned}$$

$$\begin{aligned}
&\mathsf{fmap}_2\ :\ \forall A{:}*.\forall X{:}*.\forall Y{:}*.\ (X \to Y) \to \mathsf{F}\ A\ X \to \mathsf{F}\ A\ Y\\
&\mathsf{fmap}_2\ A\ X\ Y\ f\ (\mathsf{nil}\ _) &&= \mathsf{nil}\,()\\
&\mathsf{fmap}_2\ A\ X\ Y\ f\ (\mathsf{cons}\ a\ x) &&= \mathsf{cons}\ a\ (f\ x)
\end{aligned}$$

$$\begin{aligned}
&\mathsf{unfold}\ :\ \forall i\,\forall A{:}*.\forall S{:}*.\ (S \to \mathsf{F}\ A\ S) \to S \to \mathsf{CoList}^i\ A\\
&\mathsf{unfold}\ i\ A\ S\ f\ s\ .\mathsf{out}\ j &&= \mathsf{fmap}_2\ A\ S\ (\mathsf{CoList}^j\ A)\ (\mathsf{unfold}\ j\ A\ S\ f)\ (f\ s).
\end{aligned}$$

Without type arguments, the last line reads $\mathsf{unfold}\ f\ s\ .\mathsf{out} = \mathsf{fmap}_2\ (\mathsf{unfold}\ f)\ (f\ s)$. Structural (non-type based) guardedness checkers would need to inline the definition of fmap_2 in order to see that unfold is productive. In our calculus, productivity is immediate since $j < i$, thus, the size argument decreases in the recursive call.

As an instance of unfold, we can get infinite repetition of a fixed element $a : A$ by using a single state () in the trivial set of states $S = 1$. The transition function $f : 1 \to \mathsf{F}\ A\ 1$ produces always $\mathsf{cons}(a, ())$, thus, repeat will never terminate, but produce an infinite colist of as.

$$\begin{aligned}
&\mathsf{repeat}\ :\ \forall A{:}*.\ A \to \mathsf{CoList}^{\infty} A\\
&\mathsf{repeat}\ A\ a = \mathsf{unfold}\ \infty\ A\ 1\ (\lambda_.\ \mathsf{cons}(a, ()))\ ().
\end{aligned}$$

Of course, we can also implement repeat directly, like we did for streams:

$$\begin{aligned}
&\mathsf{repeat}\ :\ \forall i\forall A{:}*.\ A \to \mathsf{CoList}^{\infty} A\\
&\mathsf{repeat}\ i\ A\ a\ .\mathsf{out}\ j = \mathsf{cons}(a, \mathsf{repeat}\ j\ A\ a)).
\end{aligned}$$

If we want to get the map function for colists, we need a more precise typing of unfold:

$$\begin{aligned}
&\mathsf{unfold}\ :\ \forall i\,\forall A{:}*.\forall S : \mathsf{size} \to *.\ (\forall i.\ S\ i \to \forall j < i.\ \mathsf{F}\ A\ (S\ j)) \to S\ i \to \mathsf{CoList}^i\ A\\
&\mathsf{unfold}\ i\ A\ S\ f\ s\ .\mathsf{out}\ j = \mathsf{fmap}_2\ A\ (S\ j)\ (\mathsf{CoList}^j\ A)\ (\mathsf{unfold}\ j\ A\ S\ f)\ (f\ i\ s\ j)
\end{aligned}$$

$$\begin{aligned}
&\mathsf{map}\ :\ \forall i\,\forall A{:}*.\forall B{:}*.\ (A \to B) \to \mathsf{CoList}^i\ A \to \mathsf{CoList}^i\ B\\
&\mathsf{map}\ i\ A\ B\ f = \mathsf{unfold}\ i\ B\ (\lambda i.\ \mathsf{CoList}^i\ A)\ (\lambda i.\lambda s.\lambda j.\ \mathsf{fmap}_1\ A\ B\ (\mathsf{CoList}^j\ A)\ f\ (s\ .\mathsf{out}\ j)).
\end{aligned}$$

Here, we use unfold with size-indexed state type $S\ i = \mathsf{CoList}^i A$. The state holds the input colist s, which in the transition function we deconstruct with .out into a $\mathsf{F}\ A\ (\mathsf{CoList}^j A)$, followed by mapping f which gives us $\mathsf{F}\ B\ (\mathsf{CoList}^j A)$. If that is nil, then unfold terminates with nil, otherwise it creates a cons with the element of B and recurses on the new state in $\mathsf{CoList}^j A$.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

2.4 Inflationary least and deflationary greatest fixed-point types

Let us consider generic inductive and coinductive types generated by some type transformer $F : * \to *$.

$$\begin{aligned}
&\mathsf{Mu} \quad : +\mathsf{size} \to +(* \to *) \to * \\
&\mathsf{Mu}^i F = \mu^i\{\mathsf{in} : F\}
\end{aligned}$$

$$\begin{aligned}
&\mathsf{Nu} \quad : -\mathsf{size} \to +(* \to *) \to * \\
&\mathsf{Nu}^i F = \nu^i\{\mathsf{out} : F\}.
\end{aligned}$$

Usually, F would be required to be monotone, which would read $F : +* \to *$ in our notation. However, we have not asked for monotonicity. This is because we consider the sized inductive type $\mathsf{Mu}^i F$ as the ith approximation of the *inflationary* least fixed point $\mathsf{Mu}^\infty F$, and the sized coinductive type $\mathsf{Nu}^i F$ as the ith approximation of the *deflationary* greatest fixed point $\mathsf{Nu}^\infty F$ (formal definitions see Section 4.5). Thus, we can consider *arbitrary* F without running into the usual inconsistencies (Mendler, 1987).

From the typing rules concerning μ and ν, we immediately get sized and unsized constructors for the inductive types and sized and unsized destructors for the coinductive types.

$$\begin{aligned}
&\mathsf{in}_{\mathsf{Mu}} \quad : \quad \forall F : * \to *.\, \forall i.\, (\exists j < i.\, F\ (\mathsf{Mu}^j F)) \to \mathsf{Mu}^i F \\
&\mathsf{in}_{\mathsf{Mu}}\ F\ i\ t \quad = \quad \mathsf{in}\ t
\end{aligned}$$

$$\begin{aligned}
&\mathsf{in}^\infty_{\mathsf{Mu}} \quad : \quad \forall F : * \to *.\, F\ (\mathsf{Mu}^\infty F) \to \mathsf{Mu}^\infty F \\
&\mathsf{in}^\infty_{\mathsf{Mu}}\ F\ t \quad = \quad \mathsf{in}^\infty t
\end{aligned}$$

$$\begin{aligned}
&\mathsf{out}_{\mathsf{Nu}} \quad : \quad \forall F : * \to *.\, \forall i.\, \mathsf{Nu}^i F \to \forall j < i.\, F\ (\mathsf{Nu}^j F) \\
&\mathsf{out}_{\mathsf{Nu}}\ F\ i\ r \quad = \quad \mathsf{out}\ r
\end{aligned}$$

$$\begin{aligned}
&\mathsf{out}^\infty_{\mathsf{Nu}} \quad : \quad \forall F : * \to *.\, \mathsf{Nu}^\infty F \to F\ (\mathsf{Nu}^\infty F) \\
&\mathsf{out}^\infty_{\mathsf{Nu}}\ F\ r \quad = \quad \mathsf{out}\ r\ \infty.
\end{aligned}$$

The unsized versions rely on subtyping. *A priori*, $\mathsf{in}^\infty t$ has type $\mathsf{Mu}^{\infty+1} F$ which is equal to $\mathsf{Mu}^\infty F$, hence, trivially also a subtype. Similarly, $\mathsf{out}\ r\ \infty : F\,(\mathsf{Nu}^\infty F)$ is possible since we cast $r : \mathsf{Nu}^\infty F$ to $\mathsf{Nu}^{\infty+1} F$, which is an equal type, thus, size ∞ is a valid instantiation of the quantifier $\forall i{<}\infty{+}1.\, F\,(\mathsf{Nu}^i F)$.

We can implement the sized destructor for inductive types and the sized constructor for coinductive types, still needing no monotonicity of F.

$$\begin{aligned}
&\mathsf{out}_{\mathsf{Mu}} \quad : \quad \forall F : * \to *.\, \forall i.\, \mathsf{Mu}^i F \to \exists j < i.\, F\,(\mathsf{Mu}^j F) \\
&\mathsf{out}_{\mathsf{Mu}}\ F\ i\,(\mathsf{in}^j t) \quad = \quad {}^j t
\end{aligned}$$

$$\begin{aligned}
&\mathsf{in}_{\mathsf{Nu}} \quad : \quad \forall F : * \to *.\, \forall i.\, (\forall j < i.\, F\,(\mathsf{Nu}^j F)) \to \mathsf{Nu}^i F \\
&\mathsf{in}_{\mathsf{Nu}}\ F\ i\ t\ .\mathsf{out}\ j \quad = \quad t\ j.
\end{aligned}$$

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

However, to get a proper least ($\mathsf{Mu}^\infty F$) or greatest ($\mathsf{Nu}^\infty F$) fixed-point, we need monotonicity of F, otherwise the following definitions would not be well-typed:

$$\begin{array}{lcl} \mathsf{out}^\infty_{\mathsf{Mu}} & : & \forall F : +* \to *.\, \mathsf{Mu}^\infty F \to F\,(\mathsf{Mu}^\infty F) \\ \mathsf{out}^\infty_{\mathsf{Mu}}\, F\,(\mathsf{in}^j t) & = & t \end{array}$$

$$\begin{array}{lcl} \mathsf{in}^\infty_{\mathsf{Nu}} & : & \forall F : +* \to *.\, F\,(\mathsf{Nu}^\infty F) \to \mathsf{Nu}^\infty F \\ \mathsf{in}^\infty_{\mathsf{Nu}}\, F\, t\,.\mathsf{out}\, j & = & t. \end{array}$$

In the first equation, the lhs t has type $F\,(\mathsf{Mu}^j F)$ but is used with type $F\,(\mathsf{Mu}^\infty F)$ on the rhs. As $\mathsf{Mu}^j F$ is a subtype of $\mathsf{Mu}^\infty F$, this is fine by subtyping, but only if F is monotone. Similarly, in the second equation t has type $F\,(\mathsf{Nu}^\infty F)$ on the lhs but is used with type $F\,(\mathsf{Nu}^j F)$ on the rhs. Again, as $\mathsf{Nu}^\infty F$ is a subtype of $\mathsf{Nu}^j F$, this is fine, provided F is monotone.

We see that monotonicity of F is only needed when *deconstructing* something in the least fixed point of F or *constructing* something in the greatest fixed point, meaning at size ∞. Working at general sizes, monotonicity of F is not necessary, but then we are dealing only with approximations of least and greatest fixed point, not the fixed points themselves.

2.5 Example: Stream processor

Ghani *et al.* (2009) describe programs for continuous stream functions $\mathsf{Stream}\,A \to \mathsf{Stream}\,B$ in terms of a mixed coinductive–inductive data type SP with two constructors $\mathsf{get} : (A \to \mathsf{SP}) \to \mathsf{SP}$ and $\mathsf{put} : (B \times \mathsf{SP}) \to \mathsf{SP}$. We use this example to illustrate how our foundation supports size-based reasoning on such mixed datatypes and lexicographic termination measures for mutually recursive functions. A stream processor can either get an element $v : A$ from the input stream and enter a new state, depending on the read value, or it can put an element $w : B$ on the output stream and enter a new state. To be productive, it can only read finitely many values from the input stream before writing a value on the output stream, thus, SP is actually a nesting of a least fixed-point into a greatest one: $\mathsf{SP} = \nu X.\, \mu Y.\, (A \to Y) + (B \times X)$. We express this nesting by the definition of two data types, an inductive variant SP_μ and a coinductive record type SP_ν.

$$\begin{array}{lcl} \mathsf{SP}^i_\mu\, X & = & \mu^i \langle \mathsf{get} : \lambda Y.\, A \to Y\,;\ \mathsf{put} : \lambda Y.\, B \times X \rangle \\ \mathsf{SP}^i_\nu & = & \nu^i \{ \mathsf{out} : \lambda X.\, \mathsf{SP}^\infty_\mu X \}. \end{array}$$

Inside the coinductive type, we use the inductive type SP_μ at size ∞ since we want to allow an arbitrary (finite) number of gets between two puts. We get the following derived rules for typing constructors and destructors, for $b < a^\uparrow$:

$$\frac{f : A \to \mathsf{SP}^b_\mu X}{\mathsf{get}^b f : \mathsf{SP}^a_\mu X} \qquad \frac{w : B \qquad sp : X}{\mathsf{put}^b(w, sp) : \mathsf{SP}^a_\mu X} \qquad \frac{sp : \mathsf{SP}^a_\nu}{sp\,.\mathsf{out}\, b : \mathsf{SP}^\infty_\mu\, \mathsf{SP}^b_\nu}.$$

In the context of stream processors, it is convenient to consider streams as given by a single destructor force which returns head and tail in a pair, thus,

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

$\mathsf{Str}^i A = \nu^i\{\mathsf{force} : \lambda X.\, A \times X\}$. Dedicated projections hd and tl can be defined by

$$\begin{array}{lcl} \mathsf{hd} & : & \forall i.\, \mathsf{Str}^{i+1} A \to A \\ \mathsf{hd}\, i\, s & = & \mathsf{fst}\,(s\,.\mathsf{force}\, i) \end{array}$$

$$\begin{array}{lcl} \mathsf{tl} & : & \forall i.\, \mathsf{Str}^{i+1} A \to \mathsf{Str}^i A \\ \mathsf{tl}\, i\, s & = & \mathsf{snd}\,(s\,.\mathsf{force}\, i) \end{array}$$

with fst and snd the obvious first and second projections from pairs. Via bound normalization, which makes $\mathsf{Str}^\infty = \mathsf{Str}^{\infty+1}$, we obtain instances $\mathsf{hd}\,\infty : \mathsf{Str}^\infty A \to A$ and $\mathsf{tl}\,\infty : \mathsf{Str}^\infty A \to \mathsf{Str}^\infty A$.

Running a stream processor on an input stream produces an output stream as follows (informally coded in a Haskell-like language):

$$\begin{array}{lcl} \mathsf{run}\,(\mathsf{get}\, f)\,(v, vs) & = & \mathsf{run}\,(f\, v)\, vs \\ \mathsf{run}\,(\mathsf{put}(w, sp))\, vs & = & (w,\ \mathsf{run}\, sp\, vs). \end{array}$$

We represent this function via two mutually recursive functions, one handling SP_μ and one SP_ν:

$$\begin{array}{lcl} \mathsf{run}_\mu & : & \forall i \forall j.\ |i, j+1| \Rightarrow \mathsf{SP}^j_\mu(\mathsf{SP}^i_\nu) \to \mathsf{Str}^\infty A \to B \times \mathsf{Str}^i B \\ \mathsf{run}_\mu\ i\ j\ (\mathsf{get}^{j'} f) \quad vs & = & \mathsf{run}_\mu\ i\ j'\ (f\ (\mathsf{hd}\ \infty\ vs))\ (\mathsf{tl}\ \infty\ vs) \\ \mathsf{run}_\mu\ i\ j\ (\mathsf{put}^{j'}(w, sp))\ vs & = & (w,\ \mathsf{run}_\nu\ i\ sp\ vs) \end{array}$$

$$\begin{array}{lcl} \mathsf{run}_\nu & : & \forall i.\ |i, 0| \Rightarrow \mathsf{SP}^i_\nu \to \mathsf{Str}^\infty A \to \mathsf{Str}^i B \\ \mathsf{run}_\nu\ i\ sp\ vs\ .\mathsf{force}\ i' & = & \mathsf{run}_\mu\ i'\ \infty\ (sp\ .\mathsf{out}\ i')\ vs. \end{array}$$

The recursive run_μ handles a sequence of gets terminated by put and emits the head of a forced stream $B \times \mathsf{Str}^i B$. The tail is produced by the corecursive run_ν which, upon forcing, calls run_μ again. The termination is guaranteed by the lexicographic measures, which decrease in each recursive call:

$$\begin{array}{lcll} \mathsf{run}_\mu \to \mathsf{run}_\mu : & |i, j+1| & > |i, j'+1| & \text{since} \quad j > j' \\ \mathsf{run}_\mu \to \mathsf{run}_\nu : & |i, j+1| & > |i, 0| & \\ \mathsf{run}_\nu \to \mathsf{run}_\mu : & |i, 0| & > |i', \infty+1| & \text{since} \quad i > i'. \end{array}$$

Note that since we are not doing induction on SP^i_ν, but coinduction into Str^i, we could use SP^∞_ν instead of SP^i_ν in the types of run_μ and run_ν. However, the given types are more precise: instead of a stream processor of infinite depth, they only require a stream processor of depth i to produce a stream of depth i.

2.6 *Example: breadth-first labeled infinite trees*

Jones and Gibbons (1993) present tree labeling as a cyclic program. We will now describe a modified version for infinite trees and apply type-based termination to it. Figure 1 explains the core idea of this algorithm. Given a stream $vs_1 = \mathsf{cons}\ v_1\ vs_2$ of labels, we construct an infinite tree with root v_1 (at level 1) and use vs_2 to construct the left and right subtree (both at level 2). To provide labels for all levels, a stream of streams $vs_1, vs_2, vs_3, \ldots$ is used as input and a stream of streams of the remaining labels $vs_2, vs_3, \ldots$ as output. In a Haskell-like language, we would code

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

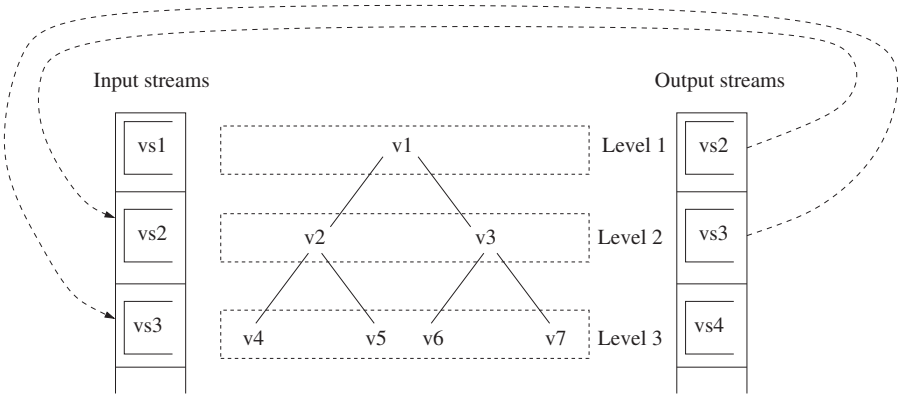

Fig. 1. Breadth-first labeled infinite tree.

this as follows:

$$\begin{array}{rcl} \mathsf{bfs}\ (\mathsf{cons}\ (\mathsf{cons}\ v\ vs)\ vss) & = & (\mathsf{node}\ v\ l\ r,\ \mathsf{cons}\ vs\ vss'') \\ \mathsf{where}\quad (l, vss') & = & \mathsf{bfs}\ vss \\ (r, vss'') & = & \mathsf{bfs}\ vss'. \end{array}$$

The stream vss of streams is created from a single label stream vs by value recursion ("tying the knot"):

$$\mathsf{bf}\ vs = t \quad \mathsf{where}\ (t, vss) = \mathsf{bfs}\ (\mathsf{cons}\ vs\ vss).$$

Note that the input $\mathsf{cons}\ vs\ vss$ to bfs is for the most part constructed from the output vss. Such cyclicity is only available in lazy languages, and may lead to busy loops, e.g., if one wrote $(t, vss) = \mathsf{bfs}\ vss$. The absence of "dead locks" has to be argued, and our type system is able to provide such arguments, as we will see in the following.

So, is this cyclic program productive, or will the creation of tree t get stuck in an infinite loop? Danielsson has shown productivity by coding an interpreter for stream expressions in Agda (Danielsson, 2010); we shall succeed by an appropriate size assignment. At this point, it is worth mentioning that bfs does not fall into the usual scheme of a *corecursive definition* such as supported by the Coq proof assistant (INRIA, 2012), since its target is not a coinductive type, but a tuple type. Our approach, however, breaks out of this restriction since it unifies recursion and corecursion under measure-based termination on ordinals (sizes and depths).

Fixing a type V of labels, we define a coinductive type of infinite binary trees, a type of streams of streams, and a type of results of function bfs.

$$\begin{array}{lcl} \mathsf{SS}^i & = & \mathsf{Stream}^i(\mathsf{Stream}^\infty V) \\ \mathsf{Tree}^i & = & \nu^i\ \{\mathsf{label} : \lambda X.V;\ \mathsf{left} : \lambda X.X;\ \mathsf{right} : \lambda X.X\} \\ \mathsf{Result}^i & = & \nu^\infty\{\mathsf{tree} : \lambda X.\mathsf{Tree}^i;\ \mathsf{rest} : \lambda X.\mathsf{SS}^i\}. \end{array}$$

Since Result is not recursive (X is not used), Result^i is just a lazy product of Tree^i and SS^i. We need a record here instead of a tuple because we want to define bfs by copattern matching, the copatterns being $.\mathsf{tree}\ \_$ and $.\mathsf{rest}\ \_$ for an unused size variable $\_$.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

In the following definition of bfs, each of the five components v, l, r, vs and vss'' of its result (node v l r, cons vs vss'') is given by one equation:

$$
\begin{array}{lcl}
\mathsf{bfs} & : & \forall i.\ |i| \Rightarrow \mathsf{SS}^i \to \mathsf{Result}^i \\
\mathsf{bfs}\ i\ ss\ .\mathsf{tree}\ \_\ .\mathsf{label}\ j & = & v \\
\mathsf{bfs}\ i\ ss\ .\mathsf{tree}\ \_\ .\mathsf{left}\ \ j & = & p_1\ .\mathsf{tree}\ \infty \\
\mathsf{bfs}\ i\ ss\ .\mathsf{tree}\ \_\ .\mathsf{right}\ j & = & p_2\ .\mathsf{tree}\ \infty \\
\mathsf{bfs}\ i\ ss\ .\mathsf{rest}\ \_\ .\mathsf{head}\ j & = & vs \\
\mathsf{bfs}\ i\ ss\ .\mathsf{rest}\ \_\ .\mathsf{tail}\ \ j & = & p_2\ .\mathsf{rest}\ \infty
\end{array}
$$

$$
\begin{array}{rcll}
\mathsf{where}\quad v & : & V & = ss\ .\mathsf{head}\ j\ .\mathsf{head}\ \infty \\
vs & : & \mathsf{Stream}^\infty V & = ss\ .\mathsf{head}\ j\ .\mathsf{tail}\ \infty \\
vss & : & \mathsf{SS}^j & = ss\ .\mathsf{tail}\ j \\
p_1 & : & \mathsf{Result}^j & = \mathsf{bfs}\ j\ vss \\
p_2 & : & \mathsf{Result}^j & = \mathsf{bfs}\ j\ (p_1\ .\mathsf{rest}\ \infty).
\end{array}
$$

For the sake of readability, and to make the connection to the original program obvious, we have taken the liberty to name and type the intermediate results v, vs, vss (decomposition of ss) and p_1 and p_2 (the pairs created by the recursive calls). Well-definedness of bfs is apparent since recursive calls are restricted to depth $j < i$. For well-typedness, it is crucial that the SS of input and output and the output Tree are all considered at the same depth i.

The final step is tying the knot, $(t, vss) = \mathsf{bfs}\ (\mathsf{cons}\ vs\ vss)$. We define the pair (t, vss) by recursion, informally by $\mathsf{bfp}\ vs = \mathsf{bf}\ (\mathsf{cons}\ vs\ (\mathsf{bfp}\ vs\ .\mathsf{rest}))$. How to assign sizes?

$$
\begin{array}{lcl}
\mathsf{bfp} & : & \forall i.\ |i| \Rightarrow \mathsf{Stream}^\infty V \to \mathsf{Result}^i \\
\mathsf{bfp}\ i\ vs & = & \mathsf{bf}\ i\ (\mathsf{cons}\ vs\ (\mathsf{bfp}\ ?\ vs\ .\mathsf{rest}\ \infty)).
\end{array}
$$

For the recursive call, we need a depth ? smaller than i, but we do not have one. Somehow, this is reassuring, since bfp in this form is not strongly normalizing: the lhs $\mathsf{bfp}\ i\ vs$ matches the subterm $\mathsf{bfp}\ ?\ vs$ of the rhs. However, we get a depth $j < i$ by pattern matching if we analyse the result further:

$$
\begin{array}{lcl}
\mathsf{bfp} & : & \forall i.\ |i| \Rightarrow \mathsf{Stream}^\infty V \to \mathsf{Result}^i \\
\mathsf{bfp}\ i\ vs\ .\mathsf{tree}\ \_\ .\mathsf{label}\ j & = & p\ .\mathsf{tree}\ \infty\ .\mathsf{label}\ j \\
\mathsf{bfp}\ i\ vs\ .\mathsf{tree}\ \_\ .\mathsf{left}\ \ j & = & p\ .\mathsf{tree}\ \infty\ .\mathsf{left}\ \ j \\
\mathsf{bfp}\ i\ vs\ .\mathsf{tree}\ \_\ .\mathsf{right}\ j & = & p\ .\mathsf{tree}\ \infty\ .\mathsf{right}\ j \\
\mathsf{bfp}\ i\ vs\ .\mathsf{rest}\ \_\ .\mathsf{head}\ j & = & p\ .\mathsf{rest}\ \infty\ .\mathsf{head}\ j \\
\mathsf{bfp}\ i\ vs\ .\mathsf{rest}\ \_\ .\mathsf{tail}\ \ j & = & p\ .\mathsf{rest}\ \infty\ .\mathsf{tail}\ \ j \\
\quad \mathsf{where} \quad p & : & \mathsf{Result}^{j+1} \\
p & = & \mathsf{bf}\ (j+1)\ (\mathsf{cons}\ vs\ (\mathsf{bfp}\ j\ vs\ .\mathsf{rest}\ \infty)).
\end{array}
$$

This works, but is a lot of boilerplate code. In previously studied type systems for productivity (Pareto, 2000; Abel, 2006) with rewriting only under destructors, one assumes size $i+1$ on the lhs, which in our notation would simply become

$$
\begin{array}{lcl}
\mathsf{bfp} & : & \forall i.\ \mathsf{Stream}^\infty V \to \mathsf{Result}^i \\
\mathsf{bfp}\ (i+1)\ vs & = & \mathsf{bf}\ (i+1)\ (\mathsf{cons}\ vs\ (\mathsf{bfp}\ i\ vs\ .\mathsf{rest}\ \infty)).
\end{array}
$$

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

Our present system disallows such matching on sizes, as it does not preserve termination under erasure of sizes: rewriting with $\mathsf{bfp}\ vs \longrightarrow \mathsf{bf}\ (\mathsf{cons}\ vs\ (\mathsf{bfp}\ vs\ .\mathsf{rest}))$ clearly diverges. However, we can first code a fixpoint combinator for Result and then use it to define bfp, hiding the unpleasant boilerplate.

$$
\begin{array}{lcl}
\mathsf{fixR} & : & \forall i.\ |i| \Rightarrow (\forall j.\ \mathsf{Result}^j \to \mathsf{Result}^{j+1}) \to \mathsf{Result}^i \\
\mathsf{fixR}\ i\ f\ .\mathsf{tree}\ \_\ .\mathsf{label}\ j & = & r\ .\mathsf{tree}\ \infty\ .\mathsf{label}\ j \\
\mathsf{fixR}\ i\ f\ .\mathsf{tree}\ \_\ .\mathsf{left}\ \ j & = & r\ .\mathsf{tree}\ \infty\ .\mathsf{left}\ \ j \\
\mathsf{fixR}\ i\ f\ .\mathsf{tree}\ \_\ .\mathsf{right}\ j & = & r\ .\mathsf{tree}\ \infty\ .\mathsf{right}\ j \\
\mathsf{fixR}\ i\ f\ .\mathsf{rest}\ \_\ .\mathsf{head}\ j & = & r\ .\mathsf{rest}\ \infty\ .\mathsf{head}\ j \\
\mathsf{fixR}\ i\ f\ .\mathsf{rest}\ \_\ .\mathsf{tail}\ \ j & = & r\ .\mathsf{rest}\ \infty\ .\mathsf{tail}\ \ j \\
\quad \mathsf{where} \quad r & : & \mathsf{Result}^{j+1} \\
\quad r & = & f\ j\ (\mathsf{fixR}\ j\ f)
\end{array}
$$

$$
\begin{array}{lcl}
\mathsf{bfp} & : & \forall i.\ \mathsf{Stream}^\infty V \to \mathsf{Result}^i \\
\mathsf{bfp}\ i\ vs & = & \mathsf{fixR}\ i\ f \\
\quad \mathsf{where}\ f\ j\ r & = & \mathsf{bfs}\ (j+1)\ (\mathsf{cons}\ vs\ (r\ .\mathsf{rest}\ \infty)).
\end{array}
$$

Clearly, here is no issue with strong normalization, since $\mathsf{fixR}\ \_\ f$ does not reduce.

2.7 *Programming fixed-point combinators*

For which types C^i can we define a fixpoint combinator of type $\forall i.\ (\forall j.\ C^j \to C^{j+1}) \to C^i$? In the following, we program some standard fixed-point combinators that construct functions out of an inductive type or into a coinductive type. To this end, we use the generic inductive ($\mathsf{Mu}^i F$) and coinductive types ($\mathsf{Nu}^i F$) from Section 2.4. We consider the typical cases $C^i = \mathsf{Mu}^i F \to A^i$ (recursion over $\mathsf{Mu}^i F$) and $C^i = A^i \to \mathsf{Nu}^i F$ (corecursion into $\mathsf{Nu}^i F$).

$$
\begin{array}{lcl}
\mathsf{fix}^{+1}_{\mathsf{Mu}} & : & \forall i.\ \forall F : * \to *.\ \forall A : +\mathsf{size} \to *. \\
 & & (\forall j.\ (\mathsf{Mu}^j F \to A^j) \to (\mathsf{Mu}^{j+1} F \to A^{j+1})) \to (\mathsf{Mu}^i F \to A^i) \\
\mathsf{fix}^{+1}_{\mathsf{Mu}}\ i\ F\ A\ f\ (\mathsf{in}^j t) & = & f\ j\ (\mathsf{fix}^{+1}_{\mathsf{Mu}}\ j\ F\ A\ f)\ (\mathsf{in}^j t)
\end{array}
$$

$$
\begin{array}{lcl}
\mathsf{fix}^{+1}_{\mathsf{Nu}} & : & \forall i.\ \forall F : * \to *.\ \forall A : -\mathsf{size} \to *. \\
 & & (\forall j.\ (A^j \to \mathsf{Nu}^j F) \to (A^{j+1} \to \mathsf{Nu}^{j+1} F)) \to (A^i \to \mathsf{Nu}^i F) \\
\mathsf{fix}^{+1}_{\mathsf{Nu}}\ i\ F\ A\ f\ a\ .\mathsf{out}\ j & = & f\ j\ (\mathsf{fix}^{+1}_{\mathsf{Nu}}\ j\ F\ A\ f)\ a\ .\mathsf{out}\ j.
\end{array}
$$

For the recursion combinator, we need A to be monotone in the size, written $A : +\mathsf{size} \to *$, because we are expecting the rhs to have type A^i, but the application of f yields something of type A^{j+1}, where $j < i$. This is fine by subtyping if A is monotone, as $j + 1 \leqslant i$. Similarly, the corecursion combinator requires A to be antitone, written $A : -\mathsf{size} \to *$. This is because a has type A^i from the lhs, but is used with type A^{j+1} on the rhs, where $j < i$. Again subtyping $A^i \leqslant A^{j+1}$ fixes the typing, since $i \geqslant j + 1$.

Since $\mathsf{fix}^{+1}_{\mathsf{Nu}}$ easily generalizes to a sequence of parameters $\vec{a}$ of antitone types $\vec{A}$, we have just shown that we can express all the functions accepted by System $\widehat{\lambda}$ (Barthe *et al.*, 2004) and its polymorphic variant $\widehat{F}$ (Barthe *et al.*, 2005). The example fixR

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

from the previous section already transcends this scheme, and there might be many more types C^i that admit a similar fixed-point combinator.

However, we do not subsume the admissible types of Pareto (2000) and previous work (Abel, 2008b). The reason is that an upper bound operation $j \vee k$ is missing for sizes. For instance, with $\mathsf{Nat}^i = \mu^i\{\mathsf{suc} : \lambda X.X\,; \mathsf{zero} : \lambda X.1\}$, we cannot complete the following definition of the maximum function with the most precise type $\forall i.\, \mathsf{Nat}^i \to \mathsf{Nat}^i \to \mathsf{Nat}^i$:

$$\begin{array}{l} \mathsf{max} : \forall i.\, \mathsf{Nat}^i \to \mathsf{Nat}^i \to \mathsf{Nat}^i \\ \mathsf{max}\ i\ (\mathsf{suc}^j n)\ (\mathsf{suc}^k m) = \mathsf{suc}^{(j \vee k)}\ (\mathsf{max}\ (j \vee k)\ n\ m) \\ \ldots \end{array}$$

We can only assign it a type like $\forall i.\, \mathsf{Nat}^i \to \mathsf{Nat}^\infty \to \mathsf{Nat}^\infty$.

More natural to our system are fixed-point combinators expressing well-founded recursion on ordinals, i.e., of type $\forall i.\ (\forall j.\ (\forall k{<}j.\ C^k) \to C^j) \to C^i$.

$$\begin{array}{lcl} \mathsf{fix}_{\mathsf{Mu}} & : & \forall i.\ \forall F : * \to *.\ \forall A : \mathsf{size} \to *. \\ & & (\forall j.\ (\forall k{<}j.\ \mathsf{Mu}^k F \to A^k) \to \mathsf{Mu}^j F \to A^j) \to \mathsf{Mu}^i F \to A^i \\ \mathsf{fix}_{\mathsf{Mu}}\ i\ F\ A\ f\ (\mathsf{in}^j t) & = & f\ i\ (\lambda k{<}i.\ \mathsf{fix}_{\mathsf{Mu}}\ k\ F\ A\ f)\ (\mathsf{in}^j t) \end{array}$$

$$\begin{array}{lcl} \mathsf{fix}_{\mathsf{Nu}} & : & \forall i.\ \forall F : * \to *.\ \forall A : \mathsf{size} \to *. \\ & & (\forall j.\ (\forall k{<}j.\ A^k \to \mathsf{Nu}^k F) \to A^j \to \mathsf{Nu}^j F) \to A^i \to \mathsf{Nu}^i F \\ \mathsf{fix}_{\mathsf{Nu}}\ i\ F\ A\ f\ a\ .\mathsf{out}\ j & = & f\ i\ (\lambda k{<}i.\ \mathsf{fix}_{\mathsf{Nu}}\ k\ F\ A\ f)\ a\ .\mathsf{out}\ j. \end{array}$$

Note that for these definitions, we have no variance restriction on A, it is not required to be monotone or antitone.

One might wonder why the application to $(\mathsf{in}^j t)$ is needed in the definition of $\mathsf{fix}_{\mathsf{Mu}}$, and likewise, why the elimination $.\mathsf{out}\ j$ in the definition of $\mathsf{fix}_{\mathsf{Nu}}$. Could not we just have a single fixed-point combinator like the following?

$$\begin{array}{lcl} \mathsf{fix} & : & \forall i.\ \forall C : \mathsf{size} \to *.\ (\forall j.\ (\forall k{<}j.\ C^k) \to C^j) \to C^i \\ \mathsf{fix}\ i\ C\ f & = & f\ i\ (\lambda k{<}i.\ \mathsf{fix}\ k\ C\ f). \end{array}$$

Clearly, this rule is not strongly normalizing, we can forever expand the fixed-point:

$$\begin{array}{lcl} \mathsf{fix}\ i_0\ C\ f & \longrightarrow & f\ i_0\ (\lambda i_1{<}i_0.\ \mathsf{fix}\ i_1\ C\ f) \\ & \longrightarrow & f\ i_0\ (\lambda i_1{<}i_0.\ f\ i_1\ (\lambda i_2{<}i_1.\ \mathsf{fix}\ i_2\ C\ f)) \\ & \longrightarrow & \ldots \end{array}$$

By doing so, we stipulate an infinite descending chain $i_0 > i_1 > i_2 > \ldots$ of ordinals, which is inconsistent. From here, we have a choice to make.

1. Either we forbid reduction under bounded size abstraction like $\lambda i_1{<}i_0$. However, this will make our notion of normal form weak, which is bad for an extension to dependent types, where during type checking we need to check program equivalence, for instance by comparing normal forms.
2. Or, we forbid the formation of bounded size abstractions that may lead to such infinite descending chains during reduction. Then, we can freely apply reduction rules in any position of a term.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

SizeVar	$\ni i, j$		size variable
SizeExp	$\ni a, b$	$::= i+n \mid \infty+n$	size expression $(n \geq 0)$
SizeExp$^+$	$\ni a^+, b^+$	$::= a \mid n$	extended size expression
Measure	$\ni \mathfrak{m}$	$::= \cdot \mid a^+, \mathfrak{m}$	measure expression
Pol	$\ni \pi$	$::= \circ \mid + \mid - \mid \top$	polarity/variance
SizeCxt	$\ni \Psi$	$::= \cdot \mid \Psi, i{:}\pi(<a)$	size variable context

Fig. 2. Sizes and measures.

In this paper, we choose the latter, and add a check[3] $\Delta \vdash \exists k{<}i$ when considering the bounded abstraction $\lambda k{<}i$. Here, Δ is the current size context, and the check requires that for all valuations η of Δ there must be an ordinal $k < \eta(i)$. In case of fix, we need $i{:}\mathsf{size} \vdash \exists k{<}i$ which clearly fails for $\eta(i) = 0$. In the case of $\mathsf{fix}_{\mathsf{Mu}}$ and $\mathsf{fix}_{\mathsf{Nu}}$, we are in size context $\Delta = (i{:}\mathsf{size},\ j < i)$, which forces $\eta(i) > \eta(j) \geqslant 0$ for each of its valuations η. Thus, $\Delta \vdash \exists k{<}i$ holds, and the introduction of the new size variable $k < i$ is guaranteed to be consistent.

Taking a step back, we see that the matching on the inductive input $(\mathsf{in}^j t)$, or the (co)matching on the coinductive result .out j, which is a precondition for the reduction of $\mathsf{fix}_{\mathsf{Mu}}/\mathsf{fix}_{\mathsf{Nu}}$ to take place, justifies the recursive invokation of $\mathsf{fix}_{\mathsf{Mu}}/\mathsf{fix}_{\mathsf{Nu}}$. This allows us to erase sizes along with types without losing strong normalization (we only lose the termination evidence); the rewrite rules

$$\begin{aligned} \mathsf{fix}_{\mathsf{Mu}}\ f\ (\mathsf{in}\ t) &\longrightarrow f\ (\mathsf{fix}_{\mathsf{Mu}}\ f)\ (\mathsf{in}\ t) \\ \mathsf{fix}_{\mathsf{Nu}}\ f\ a\ .\mathsf{out} &\longrightarrow f\ (\mathsf{fix}_{\mathsf{Nu}}\ f)\ a\ .\mathsf{out} \end{aligned}$$

are still strongly normalizing. Not so $\mathsf{fix}\ f \longrightarrow f\ (\mathsf{fix}\ f)$. Validity of size erasure matches our intention: sizes are only there to witness termination, they otherwise do not affect program behavior, even for open terms.

3 Syntax and typing

In this section, we formally define $\mathsf{F}_\omega^{\mathsf{cop}}$, our higher order polymorphic lambda-calculus with sized inductive and coinductive types, polarized higher order subtyping and definitions by pattern and copattern matching. As in previous work (Abel, 2006), we choose System F_ω rather than System F as basis since the notion of a *type constructor* is required (at least, semantically) if one wants to talk about its fixed-points, i. e., about (co)inductive types.

3.1 Sizes

Figure 2 gives a grammar for sizes, measures, and size contexts. A *size expression* a consists of a base, which is either a size variable i or ∞, and an offset, a natural number n.

$$a ::= i + n \mid \infty + n.$$

[3] See judgment $\Psi \vdash \exists \Psi'$ in Figure 3.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

$\Psi \vdash a$	size a is well-formed
$\Psi \vdash a < b$	strict size comparison
$\Psi \vdash a \leq b$	size comparison
$\Psi \vdash a^+$	extended size a^+ is well-formed
$\Psi \vdash a^+ < b^+$	strict comparison
$\Psi \vdash a^+ \leq b^+$	comparison
$\Psi \vdash_n \mathfrak{m}$	measure $\mathfrak{m}$ is a well-formed n-tuple
$\Psi \vdash \mathfrak{m} < \mathfrak{m}'$	strict lexicographic measure comparison
$\Psi \vdash \mathfrak{m} \leq \mathfrak{m}'$	lexicographic measure comparison
$\Psi \vdash \exists \Psi'$	Ψ' is consistent for each valuation of Ψ

Fig. 3. Size-related judgments.

We omit the offset when 0. Each size variable i comes with a bound $i < a$, which is recorded in a *size context*

$$\Psi ::= \cdot \mid \Psi, i{:}\pi(<a).$$

A size context is considered as finite map from size variables i to their *polarity* π (see below) and their *kind* $<a$. We write $\leqslant a$ for $<(a+1)$ and size for $\leqslant\infty$. Given a size context Ψ, its domain, i. e., the sequence of variables bound by Ψ, is denoted by $\boxed{\hat{\Psi}}$. *Extended size expressions* a^+ include natural numbers n. *Measures* $\mathfrak{m}$ are tuples of extended size expressions. There are a number of trivial judgments concerning well-formedness and partial ordering of (extended) size expressions and measures (see Figure 3). These judgments may use the bounds stored in size context Ψ and are all defined as expected; their inference rules can be found in Figure 6.

In constraint-based systems, strong normalization is usually lost in inconsistent contexts.[4] While our size contexts Ψ are always consistent, i. e., enjoy a valuation η of the declared size variables (by natural numbers even), we need sometimes a stronger property that a size context extension Ψ' is consistent with a fixed valuation η of Ψ, i. e., Ψ' must be consistent even when we apply η to its declared bounds. For instance, $i{\leqslant}\infty, j{<}i$ is consistent, but $j{<}i$ is not a consistent extension of $i{\leqslant}\infty$ under valuation $\eta(i) = 0$, since there is no solution for j. We write $\boxed{\Psi \vdash \exists \Psi'}$ if Ψ' consistently extends Ψ in this sense. This judgment is inspired by Blanqui and Riba (2006).

Proposition $\Psi \vdash \exists \Psi'$ can be tested by computing a minimal valuation η of Ψ and then checking whether Ψ' has a (minimal) valuation under η. In the following, let η be a finite map from size variables to natural numbers. Then, $\eta(a)$ is an extended size expression. We say $\eta \models \Psi$ if $\eta(i) < \eta(a)$ for all $(i < a) \in \Psi$. A minimal valuation $\mathsf{val}_\eta(\Psi)$ for Ψ above η can be defined as follows:

$$\begin{array}{lll}
\mathsf{val}_\eta(\cdot) & = \eta & \\
\mathsf{val}_\eta(\Psi, j < a) & = \mathsf{val}_\eta(\Psi) & \text{if } \eta(j) < \eta(a) \\
\text{Otherwise, if } \eta(j) \geqslant \eta(a) : & & \\
\mathsf{val}_\eta(\Psi, j < i + n) & = \mathsf{val}_{\eta[i \mapsto \eta(j)+1-n]}(\Psi) & \text{if } i \in \mathsf{dom}(\Psi) \\
\mathsf{val}_\eta(\Psi, j < i + n) & = \text{undefined} & \text{if } i \notin \mathsf{dom}(\Psi).
\end{array}$$

[4] For instance, in extensional type theory, $X : \mathsf{Type},\ p : X = (X \to X) \vdash (\lambda x{:}X.\, x\, x)(\lambda x{:}X.\, x\, x) : X$. The blame is on the false equality assumption $X = X \to X$ which is used for type conversion.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

SKind	$\ni \iota$	$::= * \mid o \mid \iota \to \iota'$	simple kind
SCxt	$\ni \lvert\Delta\rvert$	$::= \cdot \mid \lvert\Delta\rvert, X{:}\iota$	simple kinding context, $X \notin \mathsf{dom}(\lvert\Delta\rvert)$
Kind	$\ni \kappa$	$::= * \mid {<}a \mid \pi\kappa \to \kappa'$	kind with variance information
TyCxt	$\ni \Delta$	$::= \cdot \mid \Delta, X{:}\pi\kappa$	type variable context, $X \notin \mathsf{dom}(\Delta)$
Cxt	$\ni \Gamma$	$::= \cdot \mid \Gamma, x{:}A \mid \Gamma, x{:}{}^?A$	term variable context, $x \notin \mathsf{dom}(\Gamma)$
TyVar	$\ni X, Y, Z, i, j$		type and size variable
TyAtom	$\ni K$	$::= a \mid X \mid 1 \mid \times \mid \to \mid \forall_\kappa \mid \exists_\kappa$	type operator
Type	$\ni F, G, A, B, C$	$::= K \mid \lambda X{:}\iota.\, F \mid F\, G$	type-level lambda-calculus
		$\mid \mu^a S \mid \nu^a R$	(co)inductive type
Var	$\ni x, y, z$		term variable
Cons	$\ni c$		constructor (variant label)
Proj	$\ni d$		destructor (record label)
Variant	$\ni S$	$::= \langle c_1{:}F_1; \ldots; c_n{:}F_n \rangle$	variant row $(n \geq 0)$
Record	$\ni R$	$::= \{d_1{:}F_1; \ldots; d_n{:}F_n\}$	record row $(n \geq 0)$
MType	$\ni {}'A, {}'B$	$::= \forall \Psi.\, \mathfrak{m} \Rightarrow A$	measured type
CType	$\ni {}^?A, {}^?B$	$::= \forall \Psi.\, \mathfrak{c} \Rightarrow A$	constrained type
Cond	$\ni \mathfrak{c}$	$::= \mathfrak{m} {<} \mathfrak{m}'$	constraint/condition

Fig. 4. Kinds and type constructors.

Note that if $\eta' = \mathsf{val}_\eta(\Psi)$ is defined, then $\eta' \geqslant \eta$ (pointwise), and $\eta' \models \Psi$. To see this note that in the case where we update $\eta(i)$ to $\eta'(i) = \eta(j) + 1 - n \geqslant \eta(i+n) + 1 - n = \eta(i) + 1 \geqslant 1$, we have $\eta'(i+n) = \eta(j) + 1 - n + n > \eta(j)$.

If $\mathsf{val}_\eta(\Psi)$ is undefined and $\eta' \geqslant \eta$ then $\eta' \not\models \Psi$. In particular, if $\eta(i) = 0$ for all $i \in \mathsf{dom}(\Psi)$ and $\mathsf{val}_\eta(\Psi)$ is undefined, then Ψ is inconsistent. To check $\Psi \vdash \exists \Psi'$, we let $\eta_0(i) = 0$ the null-valuation and $\eta = \mathsf{val}_{\eta_0}(\Psi)$. Then, we check whether $\mathsf{val}_\eta(\Psi')$ is defined.

3.2 Kinds and type constructors

The type constructors of F_ω are assigned kinds $\iota ::= * \mid \iota \to \iota'$, with base kind $*$ classifying all proper types and function kinds $\iota \to \iota'$ the (higher order) type operators. We add a second base kind $\iota ::= \cdots \mid o$ that classifies size expressions, which we locate at the type level, since they are computationally irrelevant and can be erased during compilation, just like types.

These *simple kinds* ι form with the type constructors a simply-"typed" type-level lambda calculus. We *refine* these kinds into $\mathsf{F}^{\mathsf{cop}}_\omega$-kinds

$$\kappa ::= * \mid {<}a \mid \kappa \xrightarrow{\pi} \kappa',$$

where ${<}a$ refines o into the kind of size expressions $b < a$. The *polarized function kind* $\kappa \xrightarrow{\pi} \kappa'$, also written $\pi\kappa \to \kappa'$, allows us to express that the classified type constructor is co-variant ($\pi = +$), contravariant ($\pi = -$), constant ($\pi = \top$) or of mixed or unknown variance ($\pi = \circ$). The polarities π are partially ordered $\circ \leqslant +, - \leqslant \top$ according to their information content (see Figure 5). This and the order on size expressions induce a subkinding relation $\Psi \vdash \kappa \leqslant \kappa'$ on kinds of the same structure, i. e., on kinds having the same underlying simple kind $\lvert\kappa\rvert = \lvert\kappa'\rvert$. Here, when comparing two o-kinds $({<}a) \leqslant ({<}b)$, we resort to size comparison $a \leqslant b$. The

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

$\boxed{\pi \leq \pi'}$ Lattice of variances and $\boxed{\pi\pi'}$ variance composition (commutative).

$$\frac{}{\pi \leq \pi} \qquad \frac{}{\circ \leq \pi} \qquad \frac{}{\pi \leq \top} \qquad \top\pi = \top \qquad \circ\pi = \circ \text{ (if } \pi \neq \top) \qquad +\pi = \pi \qquad --= +$$

$\boxed{\pi^{-1}\pi'}$ Variance inverse composition.

$$\top^{-1}\pi = \circ \qquad \circ^{-1}\circ = \circ \qquad \circ^{-1}\pi = \top \text{ (if } \pi \neq \circ) \qquad +^{-1}\pi = \pi \qquad -^{-1}\pi = -\pi$$

$\boxed{\pi\Delta}$ and $\boxed{\pi^{-1}\Delta}$ Variance (inverse) composition with kinding context.

$$\begin{array}{rclcrcl} \pi\cdot & = & \cdot & & \pi(\Delta, X{:}\pi'\kappa) & = & (\pi\Delta), X{:}(\pi\pi')\kappa \\ \pi^{-1}\cdot & = & \cdot & & \pi^{-1}(\Delta, X{:}\pi'\kappa) & = & (\pi^{-1}\Delta), X{:}(\pi^{-1}\pi')\kappa \end{array}$$

Simple facts.

$$+\Delta = \Delta \qquad +^{-1}\Delta = \Delta \qquad -^{-1}\Delta = -\Delta$$

Fig. 5. Variances (polarities).

default variance is $\circ$ (no information) and we may omit it, writing simply $\kappa \to \kappa'$ or $\Psi, i{:}(<a)$, which is further abbreviated by $\Psi, i{<}a$.

Kinding or *type variable contexts* $\Delta ::= \cdot \mid \Delta, X{:}\pi\kappa$, which provide scoping and kinding information for type constructors, generalize size contexts from bounds $(<a)$ to arbitrary kinds κ. We may use a Δ where a Ψ is formally required, silently erasing all non-size variables from Δ. More generally, context *restriction* $\Delta \restriction \vec{X}$ of context Δ to a set of variables $\vec{X}$ deletes the bindings for all $Y \notin \vec{X}$ from Δ. This operation does not always return a well-formed context, but we will take care to only apply it when it is meaningful.

The judgment $\Delta \vdash \exists\Delta'$ (see Figure 8) states that Δ' is consistent for each valuation of Δ. Only the size declarations matter here, thus, it is a straightforward extension of $\Psi \vdash \exists\Psi'$.

Figure 4 contains a grammar for the type constructors of $\mathsf{F}^{\mathsf{cop}}_{\omega}$. Its core is a simply kinded lambda-calculus $X \mid \lambda X{:}\iota.\, F \mid F\, G$ with constants 1, $\times$, $\to$, $\forall_\kappa$, and $\exists_\kappa$ to form unit, product, function, universal and existential types. Size expressions a are considered type constructors so that sizes can be abstracted over and applied. We use the following short-hands:

$\lambda X F$	for	$\lambda X{:}\iota.\, F$	if ι inferable
$A \times B$	for	$(\times)\, A\, B$	product type
$A \to B$	for	$(\to)\, A\, B$	function type
$\forall X{:}\kappa.\, A$	for	$\forall_\kappa(\lambda X{:}\lvert\kappa\rvert.\, A)$	universal type
$\exists X{:}\kappa.\, A$	for	$\exists_\kappa(\lambda X{:}\lvert\kappa\rvert.\, A)$	existential type
$\forall i{<}a.\, A$	for	$\forall_{<a}(\lambda i{:}o.\, A)$	bounded universal
$\exists i{<}a.\, A$	for	$\exists_{<a}(\lambda i{:}o.\, A)$	bounded existential
$\forall i.\, A$	for	$\forall i{:}\mathsf{size}.\, A$	"unbounded" universal
$\exists i.\, A$	for	$\forall i{:}\mathsf{size}.\, A$	"unbounded" existential.

We also write $\forall\Delta.\, A$ for the universal abstraction of all type variables of Δ in type A.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

$\boxed{\Psi \vdash a}$ Well-formed sizes, $\boxed{\vdash \Psi}$ well-formed size contexts, and $\boxed{\Psi \vdash i < a}$ size bound lookup.

$$\frac{}{\Psi \vdash \infty + n} \qquad \frac{\Psi \vdash i < a}{\Psi \vdash i + n} \qquad \frac{}{\vdash \cdot} \qquad \frac{\vdash \Psi \qquad \circ^{-1}\Psi \vdash a}{\vdash \Psi, i{:}\pi(<a)} \qquad \frac{(i{:}\pi(<a)) \in \Psi}{\Psi \vdash i < a}\ \pi \leq +$$

$\boxed{\Psi \vdash \vec{a} \leftleftarrows \Psi'}$ Well-formed size substitution

$$\frac{}{\Psi \vdash \cdot \leftleftarrows \cdot} \qquad \frac{\Psi \vdash \vec{a} \leftleftarrows \Psi' \qquad \Psi \vdash a < b[\vec{a}/\hat{\Psi}']}{\Psi \vdash \vec{a}\, a \leftleftarrows \Psi', i : \pi(<b)}$$

$\boxed{\Psi \vdash a < b}$ Strict and $\boxed{\Psi \vdash a \leq b}$ weak size comparison.

$$\frac{n < m}{\Psi \vdash \infty + n < \infty + m} \qquad \frac{n < m \qquad \Psi \vdash i < a}{\Psi \vdash i + n < i + m} \qquad \frac{\Psi \vdash i < \infty}{\Psi \vdash i + n < \infty + m} \qquad \frac{\Psi \vdash i < \infty + m}{\Psi \vdash i + n < \infty + (m + n)}$$

$$\frac{\Psi \vdash a + n \leq b}{\Psi, i{:}\pi(<a), \Psi' \vdash i + n < b}\ \pi \leq + \qquad \frac{\Psi \vdash a < b + 1}{\Psi \vdash a \leq b}$$

$\boxed{\Psi \vdash_1 a^+}$ Extended size and $\boxed{\Psi \vdash_k \mathfrak{m}}$ $\boxed{\Psi \vdash \mathfrak{m}}$ measure well-formedness.

$$\frac{}{\Psi \vdash_1 n} \qquad \frac{\Psi \vdash a}{\Psi \vdash_1 a} \qquad \frac{\Psi \vdash_1 a^+ \qquad \Psi \vdash_k \mathfrak{m}}{\Psi \vdash_{k+1} a^+, \mathfrak{m}} \qquad \frac{\Psi \vdash_k \mathfrak{m}}{\Psi \vdash \mathfrak{m}}\ k \text{ is length of } \mathfrak{m}$$

$\boxed{\Psi \vdash a^+ < b^+}$ Extending strict and $\boxed{\Psi \vdash a^+ \leq b^+}$ weak size comparison.

$$\frac{n_1 < n_2}{\Psi \vdash n_1 < n_2} \qquad \frac{n_1 < n_2}{\Psi \vdash n_1 < i + n_2} \qquad \frac{}{\Psi \vdash n_1 < \infty + n_2} \qquad \frac{\Psi \vdash a^+ < b^+ + 1}{\Psi \vdash a^+ \leq b^+}$$

$\boxed{\Psi \vdash \mathfrak{c}}$ $\boxed{\Psi \vdash \mathfrak{m}\ \mathrm{R}\ \mathfrak{m}'}$ Strict (R $= <$) and weak (R $= \leq$) measure comparison.

$$\frac{\Psi \vdash a_1^+ < a_2^+}{\Psi \vdash a_1^+, \mathfrak{m}_1\ \mathrm{R}\ a_2^+, \mathfrak{m}_2} \qquad \frac{\Psi \vdash a_1^+ \leq a_2^+ \qquad \Psi \vdash \mathfrak{m}_1\ \mathrm{R}\ \mathfrak{m}_2}{\Psi \vdash a_1^+, \mathfrak{m}_1\ \mathrm{R}\ a_2^+, \mathfrak{m}_2}$$

$\boxed{|\kappa| = \iota}$ Kind erasure defined by $|*| = *$ and $|{<}b| = o$ and $|\pi\kappa \to \kappa'| = |\kappa| \to |\kappa'|$.

$\boxed{\Psi \vdash \kappa}$ Wellformed kinds.

$$\frac{}{\Psi \vdash *} \qquad \frac{\Psi \vdash a}{\Psi \vdash {<}a} \qquad \frac{-\Psi \vdash \kappa \qquad \Psi \vdash \kappa'}{\Psi \vdash \pi\kappa \to \kappa'}$$

$\boxed{\Psi \vdash \kappa \leq \kappa'}$ Subkinding.

$$\frac{}{\Psi \vdash * \leq *} \qquad \frac{\Psi \vdash a \leq b}{\Psi \vdash ({<}a) \leq ({<}b)} \qquad \frac{\pi' \leq \pi \qquad -\Psi \vdash \kappa_1' \leq \kappa_1 \qquad \Psi \vdash \kappa_2 \leq \kappa_2'}{\Psi \vdash \pi\kappa_1 \to \kappa_2 \leq \pi'\kappa_1' \to \kappa_2'}$$

$\boxed{\Psi \vdash O \leq^{\pi} O' \text{ for } O ::= a \mid \mathfrak{m} \mid \kappa}$ Parametrized size, measure, and kind comparison.

$$\frac{\Psi \vdash O \leq O' \qquad \Psi \vdash O' \leq O}{\Psi \vdash O \leq^{\circ} O'} \qquad \frac{\Psi \vdash O \leq O'}{\Psi \vdash O \leq^{+} O'} \qquad \frac{\Psi \vdash O' \leq O}{\Psi \vdash O \leq^{-} O'} \qquad \frac{}{\Psi \vdash O \leq^{\top} O'}$$

Fig. 6. Sizes, measures and kinds.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

$\boxed{\Delta \vdash A}$ Well-formed types (entry point for kinding) and $\boxed{\Delta \vdash F \rightrightarrows \kappa}$ kinding (inference mode).

$$\frac{\Delta \vdash A \rightrightarrows *}{\Delta \vdash A} \qquad \frac{}{\Delta \vdash 1 \rightrightarrows *} \qquad \frac{}{\Delta \vdash \times \rightrightarrows * \overset{+}{\to} * \overset{+}{\to} *} \qquad \frac{}{\Delta \vdash \to \rightrightarrows * \overset{-}{\to} * \overset{+}{\to} *} \qquad \frac{\Delta \vdash a}{\Delta \vdash a \rightrightarrows \leq a}$$

$$\frac{(X{:}\pi\kappa) \in \Delta}{\Delta \vdash X \rightrightarrows \kappa}\ \pi \leq + \qquad \frac{\Delta \vdash F \rightrightarrows \kappa \overset{\pi}{\to} \kappa' \qquad \pi^{-1}\Delta \vdash G \leftleftarrows \kappa}{\Delta \vdash F\,G \rightrightarrows \kappa'}$$

$$\frac{-\Delta \vdash \kappa}{\Delta \vdash \forall_\kappa \rightrightarrows (\kappa \overset{\circ}{\to} *) \overset{+}{\to} *} \qquad \frac{\Delta \vdash \kappa}{\Delta \vdash \exists_\kappa \rightrightarrows (\kappa \overset{\circ}{\to} *) \overset{+}{\to} *}$$

$$\frac{\Delta \vdash a \qquad \Delta \vdash S \leftleftarrows * \overset{\circ}{\to} *}{\Delta \vdash \mu^a S \rightrightarrows *} \qquad \frac{-\Delta \vdash a \qquad \Delta \vdash R \leftleftarrows * \overset{\circ}{\to} *}{\Delta \vdash \nu^a R \rightrightarrows *}$$

$\boxed{\Delta \vdash F \leftleftarrows \kappa}$ Kinding (checking mode).

$$\frac{\Delta \vdash F \rightrightarrows \kappa \qquad \Delta \vdash \kappa \leq \kappa'}{\Delta \vdash F \leftleftarrows \kappa'} \qquad \frac{|\kappa| = \iota \qquad \circ^{-1}\Delta \vdash \kappa \qquad \Delta, X{:}\pi\kappa \vdash F \leftleftarrows \kappa'}{\Delta \vdash \lambda X{:}\iota.\, F \leftleftarrows \pi\kappa \to \kappa'}$$

$$\frac{\Delta \vdash S_c \leftleftarrows \kappa \text{ for all } c \in S}{\Delta \vdash S \leftleftarrows \kappa} \qquad \frac{\Delta \vdash R_d \leftleftarrows \kappa \text{ for all } d \in R}{\Delta \vdash R \leftleftarrows \kappa}$$

$\boxed{\Delta \vdash {}^?A}$ Well-formed constrained types.

$$\frac{\Delta \vdash \mathfrak{m} \qquad \Delta \vdash \Psi \qquad \Delta, \Psi \vdash \mathfrak{m}' \qquad \Delta, \Psi \vdash A}{\Delta \vdash \forall \Psi.\ \mathfrak{m}' < \mathfrak{m} \Rightarrow A}$$

$\boxed{\Delta \vdash \Delta'}$ Well-formed kinding and $\boxed{\Delta \vdash \Gamma}$ typing contexts.

$$\frac{}{\Delta \vdash \cdot} \qquad \frac{\circ^{-1}\Delta \vdash \kappa \qquad \Delta, X{:}\pi\kappa \vdash \Delta'}{\Delta \vdash X{:}\pi\kappa, \Delta'} \qquad \frac{}{\Delta \vdash \cdot} \qquad \frac{\Delta \vdash \Gamma \qquad \Delta \vdash A}{\Delta \vdash \Gamma, x{:}A} \qquad \frac{\Delta \vdash \Gamma \qquad \Delta \vdash {}^?A}{\Delta \vdash \Gamma, x{:}{}^?A}$$

Fig. 7. Kinding.

$\Psi \vdash \kappa$	kind κ is well-formed in Ψ
$\Psi \vdash \kappa \leq \kappa'$	κ is a subkind of κ'
$\Delta \vdash \Delta'$	kinding context Δ' is well-formed in Δ
$\Delta \vdash \exists \Delta'$	Δ' is consistent for each valuation of Δ

Fig. 8. Kind-related judgments.

The simple kind annotation ι in $\lambda X{:}\iota.\, F$ allows us to infer a unique simple kind for closed type constructors. The simple kind of an open type constructor depends only on the simple kinds of its free type variables. This property simplifies the interpretation $[\![F]\!]$ of type constructors as set-theoretic functions on semantic types we will give later.

For the purpose of type checking, we are only interested in β-normal type constructors. We write $F\ @^\iota\ G$ for the normalizing application of F to an argument G of simple kind ι. We may write $@^\kappa$ instead of $@^{|\kappa|}$, or even just $@$. Normalizing application has a structurally recursive implementation (Watkins *et al.*, 2003) via hereditary substitutions $[G/X]^\iota F$ (needed for case $(\lambda X{:}\iota.\, F)\ @^\iota\ G$).

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

$\Delta \vdash A$	type A is well-formed
$\Delta \vdash F \rightrightarrows \kappa$	F has kind κ (inference)
$\Delta \vdash F \leftleftarrows \kappa$	F has kind κ (checking)
$\Delta \vdash \Gamma$	typing context Γ is well-formed
$\Delta \vdash A \leq A'$	A is subtype of A'
$\Delta \vdash F \leq^{\pi} F' \rightrightarrows \kappa$	F is higher-order subtype of F' (κ inferred)
$\Delta \vdash F \leq^{\pi} F' \leftleftarrows \kappa$	F is higher-order subtype of F' (κ given)

Fig. 9. Type-related judgments.

Sized inductive $\mu^a S$ and coinductive types $\nu^a R$ are given in terms of *variant rows* S and *record rows* R. A variant row $S = \langle c_1 : F_1 ; \ldots ; c_n : F_n \rangle$ is a finite map from variant labels c_i, called *constructors*, to type constructors $S_{c_i} = F_i$. Dually, a record row R maps record labels d, called *destructors* or *projections*, to type constructors R_d. Instead of presenting, for instance, streams as $\nu^a X.\{\mathsf{head} : A;\ \mathsf{tail} : X\}$, we move the abstraction over X into the record row as $\nu^a\{\mathsf{head} : \lambda X.A;\ \mathsf{tail} : \lambda X.X\}$, in order to formulate the typing rules more conveniently.

Finally, we have *constrained types* $\forall \Psi.\, \mathfrak{m} < \mathfrak{m}' \Rightarrow A$ that allow its inhabitants to be used only if the condition $\mathfrak{m} < \mathfrak{m}'$ is fulfilled. We use them to restrict recursive calls to situations where the termination measure has decreased. Recursive function definitions come with *measured types* $'A ::= \forall \Delta.\, \mathfrak{m} \Rightarrow A$. These are not proper types but rather blueprints for constrained types. The idea is that kinding context Δ declares some size variables that are used in measure $\mathfrak{m}$ (and type A). When we analyze the body of a recursive function of measure type $'A$ and the variables of Δ are in scope (thus, the measure $\mathfrak{m}$ is well-formed), we make a copy $'B = \forall \Delta'.\, \mathfrak{m}' \Rightarrow A'$ of $'A$ by renaming the variables of Δ to Δ'. Then, by *measure replacement* $'B^{<\mathfrak{m}}$, we create the constrained type $\forall \Delta'.\ \mathfrak{m}' < \mathfrak{m} \Rightarrow A'$ which is used to type the recursive occurrences of the function in its body.

Figure 9 lists judgments for well-kindedness and partial ordering of types and type constructors. The judgments for types A only invoke the judgments for type constructors F in checking mode at base kind ($\leftleftarrows *$). The judgments for constructors are *bidirectional* with inference mode that computes the kind κ and checking mode that starts with a given κ. Bidirectional checking is complete since we are only interested in normal type constructors.

The rules for these judgments are given in Figures 7 and 10. A thorough discussion of polarized higher order subtyping, i.e., subtyping for type constructors that take variance into account, is available in previous work (Steffen, 1998; Abel, 2008a), we just recapitulate the basic principle here: A constructor F with $X_1 : \pi_1 \kappa_1, \ldots, X_n : \pi_n \kappa_n \vdash F \leftleftarrows \kappa$ is interpreted as an operator

$$\lambda X_1 \ldots \lambda X_n . F \ : \ \kappa_1 \xrightarrow{\pi_1} \ldots \kappa_n \xrightarrow{\pi_n} \kappa$$

with variance given as noted in its kinding context. This induces the kinding rules. For instance, $X : -*,\ Y : +* \vdash X \to Y : *$ is valid since function space is contravariant in its domain and covariant in its codomain. In particular, the hypothesis rule $X : \pi\kappa \vdash X : \kappa$ is only valid if $\pi \leqslant +$, i.e., $\pi = \circ$ which just states that $\lambda X.X : \kappa \to \kappa$

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

$\boxed{a^{\uparrow}}$ Bound normalization defined by $(\infty+n)^{\uparrow} = \infty+1$ for $n \geq 0$ and $a^{\uparrow} = a$ for $a ::= i+n$.

$\boxed{\Delta \vdash F \leq^{\pi} F' \rightrightarrows \kappa \text{ for } \pi \neq \top}$ Subtyping and type equality (inference mode).

$$\frac{\Delta \vdash K \rightrightarrows \kappa}{\Delta \vdash K \leq^{\pi} K \rightrightarrows \kappa} \qquad \frac{\Delta \vdash F \leq^{\pi} F' \rightrightarrows \pi_1\kappa_1 \to \kappa_2 \qquad \pi_1^{-1}\Delta \vdash G \leq^{\pi_1\pi} G' \leftleftarrows \kappa_1}{\Delta \vdash F\,G \leq^{\pi} F'\,G' \rightrightarrows \kappa_2}$$

$$\frac{-\Delta \vdash \kappa \leq^{-\pi} \kappa' \qquad \kappa'' = \max^{-\pi}(\kappa,\kappa')}{\Delta \vdash \forall_{\kappa} \leq^{\pi} \forall_{\kappa'} \rightrightarrows (\kappa'' \xrightarrow{\circ} *) \xrightarrow{-} *} \qquad \frac{\Delta \vdash \kappa \leq^{\pi} \kappa' \qquad \kappa'' = \max^{\pi}(\kappa,\kappa')}{\Delta \vdash \exists_{\kappa} \leq^{\pi} \exists_{\kappa'} \rightrightarrows (\kappa'' \xrightarrow{\circ} *) \xrightarrow{+} *}$$

$$\begin{array}{rcl} \max^{+} & = & \max^{\circ} \;=\; \max \\ \max^{-} & = & \min \end{array}$$

$$\frac{\Delta \vdash a^{\uparrow} \leq^{\pi} a'^{\uparrow} \qquad \Delta \vdash S \leq^{\pi} S' \leftleftarrows * \xrightarrow{\circ} *}{\Delta \vdash \mu^{a} S \leq^{\pi} \mu^{a'} S' \rightrightarrows *} \qquad \frac{-\Delta \vdash a^{\uparrow} \leq^{-\pi} a'^{\uparrow} \qquad \Delta \vdash R \leq^{\pi} R' \leftleftarrows * \xrightarrow{\circ} *}{\Delta \vdash \nu^{a} R \leq^{\pi} \nu^{a'} R' \rightrightarrows *}$$

$\boxed{\Delta \vdash F \leq^{\pi} F' \leftleftarrows \kappa}$ Subtyping and type equality (checking mode) and $\boxed{\Delta \vdash A \leq A'}$ entry point for subtyping.

$$\frac{}{\Delta \vdash F \leq^{\top} F' \leftleftarrows \kappa} \qquad \frac{\Delta \vdash A \leq^{\pi} A' \rightrightarrows *}{\Delta \vdash A \leq^{\pi} A' \leftleftarrows *}$$

$$\frac{\circ^{-1}\Delta \vdash \kappa_1 \qquad \Delta, X{:}\pi_1\kappa_1 \vdash (F\ @\ X) \leq^{\pi} (F'\ @\ X) \leftleftarrows \kappa_2}{\Delta \vdash F \leq^{\pi} F' \leftleftarrows \pi_1\kappa_1 \to \kappa_2}$$

$$\frac{\Delta \vdash S_c \leq^{\pi} S'_c \leftleftarrows \kappa \text{ for all } c \in S}{\Delta \vdash S \leq^{\pi} S' \leftleftarrows \kappa} \qquad \frac{\Delta \vdash R_d \leq^{\pi} R'_d \leftleftarrows \kappa \text{ for all } d \in R'}{\Delta \vdash R \leq^{\pi} R' \leftleftarrows \kappa}$$

$$\frac{\Delta \vdash A \leq^{+} A' \rightrightarrows *}{\Delta \vdash A \leq A'}$$

Fig. 10. Subtyping.

is a well-formed operator, or $\pi = +$ which additionally states that $\lambda X.X$ is monotone. Using the hypothesis rule on $\pi = -$ or $\pi = \top$ is invalid since $\lambda X.X$ is neither an antitone nor a constant operator.

Given a partial order $G \leqslant G'$, its π-parameterized version $G \leqslant^{\pi} G'$ can be defined as follows:

$$\begin{array}{rcl} G \leqslant^{+} G' & = & G \leqslant G' \\ G \leqslant^{-} G' & = & G' \leqslant G \\ G \leqslant^{\circ} G' & = & G \leqslant G' \text{ and } G' \leqslant G \\ G \leqslant^{\top} G' & = & \text{true} \end{array}$$

A constructor F is π-variant, $F \rightrightarrows \pi\kappa \to \kappa'$, meaning that $F\,G \leqslant F\,G' \rightrightarrows \kappa'$ whenever $G \leqslant^{\pi} G' \leftleftarrows \kappa$. (The reader is advised to play through the four cases for π in his mind.) Theoretically, the π-parameterized versions $\Delta \vdash F \leqslant^{\pi} F' \ldots$ of higher order subtyping could be defined from a non-parameterized version $\Delta \vdash F \leqslant F' \ldots$, but to avoid the potential exponential blowup due to duplication of work in case of $\leqslant^{\circ}$, the π-parameterized versions are taken as primitive.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

Exp	$\ni r,s,t$	$::= u \mid v \mid \lambda\vec{D}$	term
Intro	$\ni v$	$::= () \mid (t_1,t_2) \mid c\,t \mid {}^{G}t$	introduction term
App	$\ni u$	$::= x \mid f \mid r\,e$	applicative term
Fun	$\ni f,g$		function name
Elim	$\ni e$	$::= t \mid G \mid .d$	elimination
Pat	$\ni p$	$::= x \mid () \mid (p_1,p_2) \mid c\,p \mid {}^{Q}p$	pattern
Copat	$\ni q$	$::= p \mid X \mid .d$	copattern
PatSp	$\ni \mathbf{q}$	$::= \vec{q}$	pattern spine
DCl	$\ni D$	$::= \{\mathbf{q} \to t\}$	definition clause
Def	$\ni \vec{D}$	$::= \{D_1;\ldots;D_n\}$	definition clauses

Fig. 11. Terms, (co)patterns and clauses.

3.3 Terms and (co)patterns

Figure 11 presents the abstract syntax of $\mathsf{F}^{\mathsf{cop}}_{\omega}$ *terms* t, which are categorized into *introductions* v, *applicative terms* u and *anonymous objects* $\lambda\vec{D}$. Introductions $()$, (t_1,t_2), $c\,t$ and ${}^{G}t$ construct tuples and inductive and existential types. Applicative terms x, f and $r\,e$ are identifiers and generalized applications of a term r to an *elimination* e, which can be a term s for function elimination, a type G for instantiation of a polymorphic function, or a destructor $.d$ for projection from a coinductive type.

For each introduction form v, we have the corresponding form of pattern p, and for each elimination form e there is a copattern q. Application copatterns are just patterns p to match the argument, type application copatterns are just type variables X and projection copatterns are simply destructors d that match the same destructor in an elimination. A sequence of $\vec{q}$ of copatterns is called a pattern spine $\mathbf{q}$, in correspondence to an *elimination spine* $\vec{e}$.

Generalized lambda abstraction $\lambda\vec{D}$ introduces an object whose behavior is given by the clauses $\vec{D}$, each of which consists of a lhs, a (possibly empty) copattern sequence $\vec{q}$, and a rhs, a term t. Objects subsume both record and λ expressions of traditional functional languages. Here are a few simple examples:

$\lambda\{x \to t\}$	ordinary λ-abstraction $\lambda x t$
$\lambda\{X \to t\}$	type abstraction $\Lambda X t$
$\lambda\{(x,y) \to x\}$	first projection from pair
$\lambda\{{}^{X}x\,y \to y\,X\,x\}$	elimination of existential $(x : \exists X.\,A;\quad y : \forall X.\,A \to C)$
$\lambda\{.\mathsf{fst} \to t_1$	
$\;;.\mathsf{snd} \to t_2\}$	lazy pairing of t_1 and t_2
$\lambda\{X\,x\,y\,.\mathsf{head}\;\_ \to x$	
$\;;X\,x\,y\,.\mathsf{tail}\;\_ \to y\}$	cons for $\mathsf{Stream}^{\infty}X$
$\lambda\{\cdot \to s;\ \cdot \to t\}$	non-deterministic choice $s \oplus t$.

The meaning, given by the operational semantics (see Figure 12), is that whenever $\lambda\vec{D}$ is applied to a sequence of eliminations $\vec{e}$ that match the copatterns $\vec{q}$ of a clause with rhs t under a substitution σ and a type substitution τ, then $(\lambda\vec{D})\,\vec{e}$ reduces to $t\sigma\tau$, the rhs instantiated by the substitutions computed from pattern matching. Using

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

$\boxed{t \mathbin{/} p \searrow \tau;\sigma}$ Pattern, $\boxed{e \mathbin{/} q \searrow \tau;\sigma}$ destructor pattern, and $\boxed{\vec{e} \mathbin{/} \vec{q} \searrow \tau;\sigma}$ pattern spine matching.

$$\frac{}{t \mathbin{/} x \searrow \cdot;t/x} \qquad \frac{}{() \mathbin{/} () \searrow \cdot;\cdot} \qquad \frac{t_1 \mathbin{/} p_1 \searrow \tau_1;\sigma_1 \qquad t_2 \mathbin{/} p_2 \searrow \tau_2;\sigma_2}{(t_1,t_2) \mathbin{/} (p_1,p_2) \searrow \tau_1,\tau_2;\sigma_1,\sigma_2} \qquad \frac{t \mathbin{/} p \searrow \tau;\sigma}{c\,t \mathbin{/} c\,p \searrow \tau;\sigma}$$

$$\frac{t \mathbin{/} p \searrow \tau;\sigma}{{}^{G}t \mathbin{/} {}^{X}p \searrow G/X,\tau;\sigma} \qquad \frac{}{G \mathbin{/} X \searrow G/X;\cdot} \qquad \frac{}{.d \mathbin{/} .d \searrow \cdot;\cdot}$$

$$\frac{}{\cdot \mathbin{/} \cdot \searrow \cdot;\cdot} \qquad \frac{e \mathbin{/} q \searrow \tau;\sigma \qquad \vec{e} \mathbin{/} \vec{q} \searrow \tau';\sigma'}{e\,\vec{e} \mathbin{/} q\,\vec{q} \searrow \tau,\tau';\sigma,\sigma'}$$

$\boxed{t \mapsto t'}$ Weak head reduction.

$$\frac{\vec{e} \mathbin{/} \vec{q} \searrow \tau;\sigma}{\lambda\{\vec{q} \to t\}\,\vec{e}\,\vec{e}' \mapsto t\,\tau\sigma\,\vec{e}'} \qquad \frac{\lambda D_k\,\vec{e} \mapsto t' \text{ for some } k}{\lambda\vec{D}\,\vec{e} \mapsto t'} \qquad \frac{\lambda\vec{D}\,\vec{e} \mapsto t'}{f\,\vec{e} \mapsto t'}\ (f{:}A = \vec{D}) \in \Sigma$$

$\boxed{t \longrightarrow t'}$ Reduction of terms, $\boxed{D \longrightarrow D'}$ clauses, and $\boxed{\vec{D} \longrightarrow \vec{D}'}$ definitions.

$$\frac{t \mapsto t'}{t \longrightarrow t'} \qquad \frac{t_1 \longrightarrow t_1'}{(t_1,t_2) \longrightarrow (t_1',t_2)} \qquad \frac{t_2 \longrightarrow t_2'}{(t_1,t_2) \longrightarrow (t_1,t_2')} \qquad \frac{t \longrightarrow t'}{c\,t \longrightarrow c\,t'} \qquad \frac{t \longrightarrow t'}{{}^{G}t \longrightarrow {}^{G}t'}$$

$$\frac{r \longrightarrow r'}{r\,e \longrightarrow r'\,e} \qquad \frac{s \longrightarrow s'}{r\,s \longrightarrow r\,s'}$$

$$\frac{\vec{D} \longrightarrow \vec{D}'}{\lambda\vec{D} \longrightarrow \lambda\vec{D}'} \qquad \frac{t \longrightarrow t'}{\{\vec{q} \to t\} \longrightarrow \{\vec{q} \to t'\}} \qquad \frac{D \longrightarrow D'}{\vec{D}^1,D,\vec{D}^2 \longrightarrow \vec{D}^1,D',\vec{D}^2}$$

Fig. 12. Operational semantics.

$\boxed{\vec{e} \mathbin{/} \vec{q} \searrow \sigma;\tau}$ for *pattern matching*, the basic rule for *contraction* $\boxed{r \mapsto r'}$ becomes

$$\frac{\vec{e} \mathbin{/} \mathbf{q}_k \searrow \sigma;\tau}{\lambda\{\overrightarrow{\mathbf{q} \to t}\}\ \vec{e}\,\vec{e}\,' \mapsto t_k\sigma\tau\,\vec{e}\,'}.$$

As usual, r is called a *redex* and r' its *reduct* if $r \mapsto r'$. We allow overlapping lhs: a spine $\vec{e}$ may match different pattern spines $\mathbf{q}$, resulting in different contractions of the same redex. Also, if no lhs in the clauses $\vec{D}$ matches $\vec{e}$, the expression $\lambda\vec{D}\ \vec{e}$ is *stuck*. While a coverage checker as described in previous work (Abel *et al.*, 2013) could exclude overlapping and incomplete clauses in well-typed programs, we do not require coverage in this paper and confine ourselves to show *strong normalization*, i.e., the absence of infinite reduction sequences.

Not all stuck terms are pathological; since we are matching the whole pattern spine in one go, partially applied functions such as $\lambda\{xy \to t\}s$ are stuck, but can become unstuck if more arguments are supplied. The existence of partially applied functions will require careful treatment in the normalization proof, because non-contractibility of a non-introduction term is not preserved under application (as would be in the case of λ-calculus).

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

Decl	$\ni \delta$	$::= f : A = \vec{D}$	declaration
MDecl	$\ni {}'\delta$	$::= f : {}'A = \vec{D}$	declaration with measure
Block	$\ni \beta$	$::= \mathsf{mutual}_m\ {}'\vec{\delta}$	mutual block
Prg	$\ni P$	$::= \vec{\beta}; u$	program
Sig	$\ni \Sigma$	$::= \vec{\delta}$	signature

Fig. 13. Declarations, blocks and programs.

$\Delta;\Gamma \vdash r \rightrightarrows C$	Infer type C for term r
$\Delta;\Gamma \vdash t \Leftarrow C$	Term t checks against type C
$\Delta;\Gamma \vdash \{\mathbf{q} \to t\} \Leftarrow A$	Clause $\{\mathbf{q} \to t\}$ checks against type A
$\Delta;\Gamma \vdash \vec{D} \Leftarrow A$	Clauses D check against type A
$\Delta;\Gamma \vdash_{\Delta_0} p \Leftarrow A$	Pattern p checks against type A
$\Delta;\Gamma \mid A \vdash_{\Delta_0} \mathbf{q} \rightrightarrows C$	Pattern spine $\mathbf{q}$ eliminates A into C

Fig. 14. Type checking.

3.4 Declarations and programs

An $\mathsf{F}^{\mathsf{cop}}_{\omega}$ program consists of a sequence $\vec{\beta}$ of mutual blocks and an applicative term u, the *entry point* (this could be the name of the main function or a call to the main function with some initial arguments). Each *mutual block* $\mathsf{mutual}_m\,{}'\vec{\delta}$ is a sequence ${}'\vec{\delta}$ of mutually recursive declarations with a lexicographic termination measure of length m. Each *declaration* $f : {}'A = \vec{D}$ assigns to a function symbol f its measured type ${}'A$ and its clauses $\vec{D}$. Measures serve their purpose during checking of the mutual block and are discarded afterwards. Erasure of measure $(\!|{}'\delta|\!)$ yields a (unmeasured) declaration $f : A = \vec{D}$; after checking a mutual block and erasing the measures, the individual declarations of the block become part of the signature Σ which is used for type-checking and evaluation of the remainder of the program. An applied function $f\,\vec{e}$ reduces if one of its clauses does

$$\frac{(\lambda\vec{D})\,\vec{e} \mapsto t}{f\,\vec{e} \mapsto t}(f : A = \vec{D}) \in \Sigma.$$

The one-step reduction relation $\boxed{t \longrightarrow t'}$ is the compatible closure of the contraction relation $t \mapsto t'$, i. e., $t \longrightarrow t'$ if t' is the result of contracting exactly one redex in (an arbitrary subterm of) t. Strong normalization of reduction will be shown to hold for well-typed programs.

3.5 Type checking

Figure 14 lists the judgments involved in type checking $\mathsf{F}^{\mathsf{cop}}_{\omega}$ programs. Type-checking terms is bidirectional and a straightforward adaption of previous work (Abel *et al.*, 2013) to polymorphism, bounded quantification and constraints. The rules are given in Figures 15 and 16, and we briefly explain them.

Inference $\boxed{\Delta;\Gamma \vdash r \rightrightarrows C}$. A function symbol f's type $\Sigma(f)$ is looked up in the signature, and a variable x's type $\Gamma(x)$ in the typing context. If $\Gamma(x)$ is a constrained type $\forall\Psi.\ \mathfrak{c} \Rightarrow A$, the variable x must be immediately applied to size arguments $\hat{a}$

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

$\boxed{\Delta;\Gamma \vdash r \rightrightarrows C}$ Expression typing (inference mode). In: $\vdash \Delta$ and $\Delta \vdash \Gamma$ and r.
Out: C with $\Delta \vdash C$, or failure.

$$\frac{}{\Delta;\Gamma \vdash f \rightrightarrows \Sigma(f)} \qquad \frac{(x{:}A) \in \Gamma}{\Delta;\Gamma \vdash x \rightrightarrows A} \qquad \frac{(x : \forall \Psi.\ \mathfrak{c} \Rightarrow A) \in \Gamma \qquad \Delta \vdash \vec{a} \leftleftarrows \Psi \qquad \Delta \vdash \mathfrak{c}[\vec{a}/\hat{\Psi}]}{\Delta;\Gamma \vdash x\,\vec{a} \rightrightarrows A[\vec{a}/\hat{\Psi}]}$$

$$\frac{\Delta;\Gamma \vdash r \rightrightarrows A \to B \qquad \Delta;\Gamma \vdash s \leftleftarrows A}{\Delta;\Gamma \vdash r\,s \rightrightarrows B} \qquad \frac{\Delta;\Gamma \vdash r \rightrightarrows \forall_\kappa F \qquad \Delta \vdash G \leftleftarrows \kappa}{\Delta;\Gamma \vdash r\,G \rightrightarrows F\ @^\kappa\ G}$$

$$\frac{\Delta;\Gamma \vdash r \rightrightarrows \nu^a R}{\Delta;\Gamma \vdash r.d \rightrightarrows \forall j{<}a^\uparrow.\, R_d\,(\nu^j R)}$$

Switching.

$$\frac{\Delta \vdash A \qquad \Delta;\Gamma \vdash t \leftleftarrows A}{\Delta;\Gamma \vdash (t : A) \rightrightarrows A} \qquad \frac{\Delta;\Gamma \vdash r \rightrightarrows A \qquad \Delta \vdash A \leq C}{\Delta;\Gamma \vdash r \leftleftarrows C}$$

$\boxed{\Delta;\Gamma \vdash t \leftleftarrows C}$ Expression typing (checking mode). In: $\vdash \Delta$ and $\Delta \vdash \Gamma$ and $\Delta \vdash C$ and t.
Out: success/failure.

$$\frac{}{\Delta;\Gamma \vdash () \leftleftarrows 1} \qquad \frac{\Delta;\Gamma \vdash t_1 \leftleftarrows A_1 \qquad \Delta;\Gamma \vdash t_2 \leftleftarrows A_2}{\Delta;\Gamma \vdash (t_1,t_2) \leftleftarrows A_1 \times A_2} \qquad \frac{\Delta;\Gamma \vdash t \leftleftarrows \exists j{<}a^\uparrow.\, S_c\,(\mu^j S)}{\Delta;\Gamma \vdash c\,t \leftleftarrows \mu^a S}$$

$$\frac{\Delta \vdash G \leftleftarrows \kappa \qquad \Delta;\Gamma \vdash t \leftleftarrows F\ @^\kappa\ G}{\Delta;\Gamma \vdash {}^G t \leftleftarrows \exists_\kappa F} \qquad \frac{\Delta;\Gamma \vdash \vec{D} \leftleftarrows A}{\Delta;\Gamma \vdash \lambda \vec{D} \leftleftarrows A}$$

$\boxed{\Delta;\Gamma \vdash D \leftleftarrows A}$ and $\boxed{\Delta;\Gamma \vdash \vec{D} \leftleftarrows A}$ definition typing. In: $\vdash \Delta$ and $\Delta \vdash \Gamma$ and $\Gamma \vdash A$ and D or $\vec{D}$.
Out: success/failure.

$$\frac{\Delta';\Gamma' \mid A \vdash_\Delta \vec{q} \rightrightarrows C \qquad \Delta \vdash \exists \Delta' \qquad \Delta,\Delta';\Gamma,\Gamma' \vdash t \leftleftarrows C}{\Delta;\Gamma \vdash \{\vec{q} \to t\} \leftleftarrows A} \qquad \frac{\Delta;\Gamma \vdash D_k \leftleftarrows A \text{ for all } k}{\Delta;\Gamma \vdash \vec{D} \leftleftarrows A}$$

Fig. 15. Type checking rules.

$\boxed{\Delta;\Gamma \vdash_{\Delta_0} p \leftleftarrows A}$ Pattern typing (linear). In: $\vdash \Delta_0$ and $\Delta_0 \vdash A$ and p.
Out: $\Delta_0 \vdash \Delta$ and $\Delta_0,\Delta \vdash \Gamma$ with $\Delta_0,\Delta;\Gamma \vdash p \leftleftarrows A$ (as term), or failure.

$$\frac{}{\cdot;x{:}A \vdash_{\Delta_0} x \leftleftarrows A} \qquad \frac{}{\cdot;\cdot \vdash_{\Delta_0} () \leftleftarrows 1} \qquad \frac{\Delta_1;\Gamma_1 \vdash_{\Delta_0} p_1 \leftleftarrows A_1 \qquad \Delta_2;\Gamma_2 \vdash_{\Delta_0} p_2 \leftleftarrows A_2}{\Delta_1,\Delta_2;\Gamma_1,\Gamma_2 \vdash_{\Delta_0} (p_1,p_2) \leftleftarrows A_1 \times A_2}$$

$$\frac{\Delta;\Gamma \vdash_{\Delta_0} p \leftleftarrows \exists j{<}a^\uparrow.\, S_c\,(\mu^j S)}{\Delta;\Gamma \vdash_{\Delta_0} c\,p \leftleftarrows \mu^a S} \qquad \frac{\Delta;\Gamma \vdash_{\Delta_0,X:\kappa} p \leftleftarrows F\ @^\kappa\ X}{X{:}\kappa,\Delta;\Gamma \vdash_{\Delta_0} {}^X p \leftleftarrows \exists_\kappa F}$$

$\boxed{\Delta;\Gamma \mid A \vdash_{\Delta_0} \vec{q} \rightrightarrows C}$ Pattern spine typing (linear). In: $\vdash \Delta_0$ and $\Delta_0 \vdash A$ and $\vec{q}$.
Out: $\Delta_0 \vdash \Delta$ and $\Delta_0,\Delta \vdash \Gamma$ and $\Delta_0,\Delta;\Gamma \vdash C$ with $\Delta_0,\Delta;\Gamma,z{:}A \vdash z\,\vec{q} \rightrightarrows C$ (for some fresh variable z), or failure.

$$\frac{}{\cdot;\cdot \mid C \vdash_{\Delta_0} \cdot \rightrightarrows C} \qquad \frac{\Delta_1;\Gamma_1 \vdash_{\Delta_0} p \leftleftarrows A \qquad \Delta_2;\Gamma_2 \mid B \vdash_{\Delta_0} \vec{q} \rightrightarrows C}{\Delta_1,\Delta_2;\Gamma_1,\Gamma_2 \mid A \to B \vdash_{\Delta_0} p\,\vec{q} \rightrightarrows C}$$

$$\frac{\Delta;\Gamma \mid \forall j{<}a^\uparrow.\, R_d\,(\nu^j R) \vdash_{\Delta_0} \vec{q} \rightrightarrows C}{\Delta;\Gamma \mid \nu^a R \vdash_{\Delta_0} .d\,\vec{q} \rightrightarrows C} \qquad \frac{\Delta;\Gamma \mid F\ @^\kappa\ X \vdash_{\Delta_0,X:\kappa} \vec{q} \rightrightarrows C}{X{:}\kappa,\Delta;\Gamma \mid \forall_\kappa F \vdash_{\Delta_0} X\,\vec{q} \rightrightarrows C}$$

Fig. 16. Pattern typing.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

satisfying both Ψ and the condition $\mathfrak{c}$; after all, a constrained type is, for consistency reasons, not a proper type for an expression. An application $r\,s$ of a function r of inferred type $A \to B$ has type B if the argument s checks against type A. Instantiation $r\,G$ of a polymorphic term r of inferred type $\forall_\kappa F$ has type $F\ @^\kappa\ G$ if G has kind κ. In particular, r could be of type $\forall i{<}a.\,A$, then G must be a size expression $< a$ to succeed. If r is of coinductive type $\nu^a R$, then $r.d$ has type $\forall j{<}a^\uparrow.R_d\,(\nu^j R)$, see Section 2.5.

There are two rules to switch direction. Checking r against type C succeeds if r's type is inferred as A and A is a subtype of C. Also, we can add *type ascription* $(t : A)$ to the term language; then inference of $(t : A)$ succeeds and yields A if A is a well-formed type and t checks against A. While type ascription is needed to bidirectionally type check redexes or stuck terms, it is dispensable if one confines to checking normal terms (in the sense that no elimination is applied to a λ in the source program). We will consider type ascriptions be removed before execution of the program, so they do not pop up in the operational and denotational semantics.

Checking $\boxed{\Delta;\Gamma \vdash t \leftleftarrows C}$. Introductions and λs are checked against a given type. Checking a pair ${}^G t$ of a type expression G and a term t against an existential type $\exists_k F$ succeeds if G has kind κ and t is of the correct instance $F\ @^\kappa\ G$. Checking a constructor term $c\,t$ against an inductive type $\mu^a S$ succeeds if t checks against $\exists j < a^\uparrow.\,S_c\,(\mu^j S)$. This means that t should be essentially a pair ${}^b t'$ of a size $b < a^\uparrow$ and t' be a correct argument to constructor c, i. e., having variant S_c applied to $\mu^j S$. If $a \geqslant \infty$, by bound normalization $a^\uparrow = \infty + 1$ the size index $b = \infty$ fulfills $b < a^\uparrow$, which implies that in a value v in the fixpoint $\mu^\infty S$ all size witnesses can uniformly be ∞ (assuming S does not mention types with non-∞ size). To check $\lambda\vec{D}$ we check all clauses D_k.

Clause checking $\boxed{\Delta;\Gamma \vdash \{\mathbf{q} \to t\} \leftleftarrows A}$. We first check that pattern spine $\mathbf{q}$ indeed eliminates type A. As a result, we obtain a kinding context Δ' which binds the type variables X contained in $\mathbf{q}$ and a typing context Γ' which binds the pattern variables x contained in $\mathbf{q}$'s patterns, and a remaining type C of lhs and rhs. We now need to make sure that $\Delta \vdash \exists\Delta'$ such that any valuation of Δ can be extended to a valuation of Δ'. Complementing the original contexts $\Delta;\Gamma$ by the pattern contexts $\Delta';\Gamma'$ we check the rhs t against C.

Pattern spine checking $\boxed{\Delta;\Gamma \mid A \vdash_{\Delta_0} \mathbf{q} \rightrightarrows C}$. We eliminate type A which is well-formed in Δ_0. If there are no copatterns in $\mathbf{q}$, thus, the clause has an empty lhs, we simply return A which must be the type of the rhs. If we encounter an application pattern p, the eliminated type must be a function type $A \to B$. We check p against A and obtain pattern contexts $\Delta_1;\Gamma_1$. We continue to check the remaining copatterns, obtaining more pattern contexts $\Delta_2;\Gamma_2$ and a result type C, which we return together with the concatenated pattern contexts. Concatenation, and thus, pattern spine checking fails if the contexts do not have disjoint domains. A common variable would mean a non-linear lhs, which we exclude. While our semantics might extend to patterns that are non-linear in term variables, non-linearity in type variables would destroy the possibility of type-erasure. Consider the lhs

$$X{:}*\ ;\ x{:}X \mid \forall X.\forall Y.\ X \to Y\ \vdash X\,X\,x \rightrightarrows X.$$

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

Accepting this lhs, we could write a function

$$\begin{aligned}&\mathsf{cast} : \forall X.\ \forall Y.\ X \to Y\\ &\mathsf{cast}\ X\ X\ x = x\end{aligned}$$

that would happily allow us to cast a value from any type to any other, clearly going wrong at runtime after type-erasure.

If we encounter a projection pattern $.d$, the eliminated type must be a coinductive type $\nu^a R$. Taking projection $.d$ yields type $\forall j{<}a^{\uparrow}.\, R_d(\nu^j R)$, thus, we continue to eliminate this type by applying it to a fresh size variable. The general form of a universal type $\forall_\kappa F$ is eliminated by a type variable pattern X; we record $X{:}\kappa$ in the type variable pattern context and continue eliminating $F\ @^\kappa\ X$.

Pattern typing $\boxed{\Delta;\Gamma \vdash_{\Delta_0} p \leftleftarrows A}$. This judgment checks pattern p against type A which is valid in kinding context Δ_0, and returns pattern contexts $\Delta;\Gamma$. Pattern x succeeds against any type, returning singleton context $x{:}A$. The empty tuple $()$ succeeds against the unit type 1, binding no variables. The pair pattern (p_1, p_2) succeeds against the product type $A_1 \times A_2$ if each component p_i checks against its type A_i. The resulting pattern contexts are concatenated, checking for disjointness. A constructor pattern $c\,p$ checks against an inductive type $\mu^a S$ if p checks against $\exists j < a^{\uparrow}.\, S_c\,(\mu^j S)$. The latter succeeds if p is of the form ${}^j p'$, then we add size variable $j{<}a$ to the pattern context and continue checking p' against $S_c\,(\mu^j S)$. This is an instance of checking against the general existential type $\exists_\kappa F$.

In Section 4, we will validate all the typing rules by exhibiting a semantics of strongly normalizing terms based on Girard's reducibility candidates (Girard *et al.*, 1989).

3.6 Some subtleties of constrained types

In this section, we present two short examples that illustrate pitfalls concerning (failure of) strong normalization under unsatisfiable constraints.

3.6.1 On the context extension check

Here is an example of what can go wrong when we omit the check $\Delta \vdash \exists\Delta'$ from definition typing.

$$\begin{aligned}&\mathsf{kUnit} &&: \forall A.\ A \to 1\\ &\mathsf{kUnit}\ A\ a &&= ()\\ \\ &\mathsf{badLam} &&: \forall i.\ |i| \Rightarrow 1\\ &\mathsf{badLam}\ i &&= \mathsf{kUnit}\ (\forall j{<}i.\ 1)\ \lambda\{j \to \mathsf{badLam}\ j\}.\end{aligned}$$

Without a separate context check, badLam type-checks since $j < i$, thus the recursive call badLam j is valid. But surely, badLam i is the start of an infinite reduction sequence, leading to an infinite descending chain of sizes $i > j > j_1 > j_2 > \ldots$. The context check $i \leqslant \infty \vdash \exists j{<}i$ however fails, since for $i = 0$ there is no instance for j. Thus, badLam is rejected, rightfully so.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

3.6.2 On first-class constrained types

Treating conditional types $\mathfrak{c} \Rightarrow A$ as first-class would jeopardize strong normalization, as the following example shows

$$\begin{array}{lcl} \mathsf{badCond} & : & \forall i.\ |i| \Rightarrow 1 \\ \mathsf{badCond}\ i & = & \mathsf{kUnit}\ (|i|{<}|i| \Rightarrow 1)\ (\mathsf{badCond}\ i). \end{array}$$

The recursive call $\mathsf{badCond}\, i$ makes the promise $i < i$ which can never be fulfilled. Thus, $\mathsf{badCond}\, i$ should not appear on the rhs. However, types that combine a quantifier with a constraint should be fine, e. g., $\forall j.\ |j|{<}|i| \Rightarrow 1$, which is equivalent to $\forall j{<}i.\, 1$. Also, constraints that can never be fulfilled are fine under a quantifier, e. g., $\forall j.\ |0|{<}|0| \Rightarrow 1$. Constraints need to be checked immediately after the quantifier has been eliminated (Blanqui & Riba, 2006).

4 Semantics

In this section, we show strong normalization of $\mathsf{F}_\omega^{\mathsf{cop}}$ by a term model. Types are interpreted as reducibility candidates à la Girard adapted to our needs. Our semantic constructions rely only on the terms and the operational semantics of $\mathsf{F}_\omega^{\mathsf{cop}}$, not to the types, kinds, or inference rules. Based on the operational semantics, semantic types and kinds are constructed that interpret the syntactic types, yet syntactic types are never used for semantic constructions.[5] We consider this conceptual hygiene important from a philosophic perspective: we use types just as a vehicle to assign properties to our programs; clearly, they have no run-time significance. While in the end we managed to keep syntactic types out of the semantic constructions, it was hard to get the semantic counterpart (Lemma 33) of pattern spine typing (Figure 16) right.

One clarification: Since $\mathsf{F}_\omega^{\mathsf{cop}}$ has Church-style polymorphism with explicit type abstraction and application, we can of course not talk about terms and operational semantics without mentioning syntactic types. However, we never refer to the structure of syntactic types, they remain abstract, and we could remove everything but type variables from our type language without altering the construction of semantic types and semantic typing "judgments". In particular, in the construction of the semantic universal type $\forall_{\mathscr{K}} \mathscr{F} = \{r \in \mathsf{SN} \mid r\, G \in \mathscr{F}(\mathscr{G}),\ \text{for all } G \in \mathsf{Type}, \mathscr{G} \in \mathscr{K}\}$ there is no connection between the syntactic type constructor G and the semantic type constructor $\mathscr{G}$ (of semantic kind $\mathscr{K}$). Type applications serve only to make type-checking decidable, they do not play any role in evaluation. As one reviewer observed, we could erase types altogether from terms and define our semantic types as sets of erased, Curry-style terms.

4.1 Preliminaries

We use partially applied relations to denote sets. For instance, we write $(t \longrightarrow \_)$ or simply $t\longrightarrow$ for the set $\{t' \mid t \longrightarrow t'\}$ of reducts of t. Similarly, $<\alpha = \{\beta \mid \beta < \alpha\}$. The identity substitution is denoted by σ_{id}.

[5] Humbly following the masters (Vouillon & Melliès, 2004).

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

Lemma 1 (*Soundness and completeness of matching*)
$s \;/\; p \searrow \tau; \sigma$ iff $s = p\tau\sigma$.

Proof
By induction on judgment $s \;/\; p \searrow \tau; \sigma$ as given by the rules in Figure 12. □

4.2 Strong normalization

Classically, a term t is strongly normalizing if it admits no infinite reduction sequences $t \longrightarrow t_1 \longrightarrow t_2$ starting with t. Inductively, we define $t \in \mathsf{SN}$ if all of its reducts are already in SN:

$$\frac{(t \longrightarrow \_) \subseteq \mathsf{SN}}{t \in \mathsf{SN}}.$$

Naturally, if $t \in \mathsf{SN}$, then all its reducts and subterms are also strongly normalizing.

We extend the notion SN to other syntactic categories: An elimination e is strongly normalizing, $e \in \mathsf{SN}$, if it either is not a term (but a type G or a projection $.d$), or if it is a strongly normalizing term. A definition clause $D = \{\vec{q} \to t\}$ is strongly normalizing if $t \in \mathsf{SN}$.

4.3 Simulation

Our typing rules (see Figure 15) state that a definition $\lambda\vec{D} : A$ or $(f : A = \vec{D})$ is well-typed if each of the clauses D_k is of type A, individually. In the absence of a coverage check, there is no concept of "the clauses make sense *together*". We would like to see this independence of clauses reflected in our semantics. In particular, we would like to have *compositionality*, i. e., if each clause of a definition is semantically meaningful (in particular, does not lead to non-termination), then the clauses are meaningful together. For functions, our type-checker works exactly like that: each clause is checked individually, using the termination measure; an interaction between clauses need not be taken into account.[6]

One idea is to say that a defined function $f : A = \vec{D}$ reduces non-deterministically to one of its clauses D_k, however, this immediately destroys strong normalization, because D_k might mention f. We need to defer unfolding of f until the pattern of one of its clauses matches. Thus, instead we say that $f\,\vec{e}$ reduces if $(\lambda\vec{D})\vec{e}$ reduces; f is simulated by its clauses $\vec{D}$. In general, a term r is *simulated* by terms $\vec{r}$, written $\boxed{r \rhd \vec{r}}$, iff each of its contractions under some eliminations is accounted for by one of the terms $\vec{r}$, formally

$$\forall \vec{e}, t.\;\; r\,\vec{e} \mapsto t \implies \exists k.\; r_k\,\vec{e} \mapsto t.$$

Closing reducibility candidates by simulation is one of the new ideas of our proof.

Lemma 2 (*Simulation*)
1. $\lambda\{D_1; \ldots; D_n\} \rhd \lambda D_1, \ldots, \lambda D_n$.

[6] In general, normalization of rewriting is of course not compositional. E. g., the rule $\mathsf{f\,true} \longrightarrow \mathsf{f\,false}$ by itself terminates, but adding $\mathsf{f\,false} \longrightarrow \mathsf{f\,true}$ destroys normalization.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

2. If $(f : A = \vec{D}) \in \Sigma$ then $f \rhd \lambda\vec{D}$.
3. If $r \rhd r_1, \ldots, r_n$ then $r\, e \rhd r_1\, e, \ldots, r_n\, e$.

Proof

1. Assume $(\lambda\vec{D})\vec{e} \mapsto t$. By inversion, $(\lambda D_k)\vec{e} \mapsto t$ for some k.
2. Assume $f\, \vec{e} \mapsto t$. By inversion $(\lambda\vec{D})\vec{e} \mapsto t$.
3. We have to show $\forall \vec{e}, t.\ r\, e\, \vec{e} \mapsto t \implies \exists k.\ r_k\, e\, \vec{e} \mapsto t$. This holds directly by assumption $r \rhd \vec{r}$ with elimination vector $e, \vec{e}$. □

Naturally, simulation is reflexive and transitive, i.e., if $r \rhd r_1, \ldots, r_n$ and $r_i \rhd \vec{s}^{\,i}$ for all i, then $r \rhd \vec{s}^{\,1}, \ldots, \vec{s}^{\,n}$.

4.4 Semantic types

In order to show strong normalization, we model types as sets of strongly normalizing terms, more precisely, as reducibility candidates à la Girard. We choose reducibility candidates over Tait's saturated sets, since they allow us to show strong normalization in the absence of standardization and confluence. As a consequence, we can model definitions with incomplete and overlapping patterns.

A set of terms $\mathscr{A}$ is a *reducibility candidate* (Girard *et al.*, 1989), written $\mathscr{A} \in \mathsf{CR}$, if the following conditions hold.

CR1 $\mathscr{A} \subseteq \mathsf{SN}$: "each term in $\mathscr{A}$ is strongly normalizing".
CR2 if $t \in \mathscr{A}$, then $(t \longrightarrow \_) \subseteq \mathscr{A}$: "$\mathscr{A}$ is closed under reduction".
CR3 if $t \in \mathsf{Ne}$ and $(t \longrightarrow \_) \subseteq \mathscr{A}$, then $t \in \mathscr{A}$: "$\mathscr{A}$ contains a neutral already if all its redexes are in $\mathscr{A}$".
CR4 if $t \notin \mathsf{Intro}$ and $(t \longrightarrow \_) \subseteq \mathscr{A}$ and $t \rhd \vec{t} \in \mathscr{A}$, then $t \in \mathscr{A}$: "$\mathscr{A}$ is closed under simulation".

Condition **CR4**, is new; it introduces multi-clause objects $\lambda\vec{D}$ and function symbols f into a semantic type (candidate).

Lemma 3 (*Multi-clause objects*)

1. If $\lambda D_1, \ldots, \lambda D_n \in \mathscr{A}$, then $\lambda\vec{D} \in \mathscr{A}$.
2. If $(f : A = \vec{D}) \in \Sigma$ and $\lambda\vec{D} \in \mathscr{A}$, then $f \in \mathscr{A}$.

Proof

1. We show $\lambda\vec{D} \in \mathscr{A}$ by induction on $\vec{D} \in \mathsf{SN}$. Since $\lambda\{\vec{D}\} \rhd \overrightarrow{\lambda D}$, we may use **CR4**. It remains to show that $\lambda\vec{D} \longrightarrow t$ implies $t \in \mathscr{A}$. If $\lambda\vec{D} \mapsto t$, then $\lambda D_k \mapsto t$ for some k, and since $\lambda D_k \in \mathscr{A}$ we infer $t \in \mathscr{A}$ by **CR2**. Otherwise, the reduction takes place in some body and we have $t = \lambda\vec{D}'$ with $\vec{D} \longrightarrow \vec{D}'$. Since $\lambda\vec{D}' \rhd \overrightarrow{\lambda D'}$, we conclude by induction hypothesis.
2. Directly by **CR4**, since $f \rhd \lambda\vec{D}$ by Lemma 2 and all reducts of f are reducts of $\lambda\vec{D}$. □

In **CR3**, Ne is a suitable set of so-called *neutral* terms. These are "good", i.e., inhabit a candidate, as soon as all their reducts are good. For Girard's technique to work, neutral terms need to include redexes such as $(\lambda x.t)\, s\, \vec{e}$ and variables x, and

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

need to be closed under application, i. e., r neutral implies $r\,s$ neutral. In case of pure lambda calculus, any term which is not a lambda-abstraction can be considered neutral.

In our setting of matching the whole pattern spine $\vec{q}$ against the eliminations $\vec{e}$, things are more subtle. For instance, the partial application $\lambda\{x\,y \to x\,x\}\,\delta$ with $\delta = \lambda\{x \to x\,x\}$ is stuck (and even in normal form). However, it cannot be neutral and inhabit every candidate (following **CR3**), in particular semantic function types, since it reduces to the diverging term $\delta\,\delta$ if applied to one more argument. Thus, we can only accept stuck terms as neutral which cannot become unstuck by extra eliminations. This leads to the following definition:

Definition 4 (*Neutral term, terminally stuck*)

1. An applicative term $u \in \mathsf{App}$ is *terminally stuck* if $u\,\vec{e}$ is not a redex for all eliminations $\vec{e}$.
2. A term r is *neutral*, written $r \in \mathsf{Ne}$, if it is a redex or terminally stuck.

As Girard's, our refined notion of neutrality includes redexes, variables and is closed under eliminations. Further, if $r \in \mathsf{Ne}$, then any reduction in $r\,e$ is either a reduction in r or in e. A reducibility candidate $\mathscr{A}$ is never empty since $\mathsf{Var} \subseteq \mathscr{A}$ by virtue of **CR3**.

4.4.1 Closure

For a set $\mathscr{A} \subseteq \mathsf{SN}$ which is closed under reduction let $\overline{\mathscr{A}}$ be the least reducibility candidate $\supseteq \mathscr{A}$. Inductively, $\overline{\mathscr{A}}$ is defined as the closure under neutrals and simulation:

$$\frac{t \in \mathscr{A}}{t \in \overline{\mathscr{A}}} \qquad \frac{t \in \mathsf{Ne} \qquad (t \longrightarrow \_) \subseteq \overline{\mathscr{A}}}{t \in \overline{\mathscr{A}}} \qquad \frac{t \notin \mathsf{Intro} \qquad (t \longrightarrow \_) \subseteq \overline{\mathscr{A}} \qquad t \rhd \vec{t} \in \overline{\mathscr{A}}}{t \in \overline{\mathscr{A}}}.$$

The map $\mathscr{A} \mapsto \overline{\mathscr{A}}$ is a *closure operation*, i. e., it is *monotone* ($\mathscr{A} \subseteq \mathscr{B}$ implies $\overline{\mathscr{A}} \subseteq \overline{\mathscr{B}}$), *extensive* ($\mathscr{A} \subseteq \overline{\mathscr{A}}$), and *idempotent* ($\overline{\overline{\mathscr{A}}} \subseteq \overline{\mathscr{A}}$). Note that the closure operator never adds introduction terms such as $()$, (t_1, t_2), $c\,t$, or ${}^{G}t$ to a term set $\mathscr{A}$. Thus, for introductions $v \in \overline{\mathscr{A}}$, we have $v \in \mathscr{A}$ already.

CR is closed under arbitrary intersections $\bigcap_{i \in I} \mathscr{A}_i$. Under the inclusion order $\subseteq$, it forms a complete lattice with greatest element SN and least element $\overline{\emptyset}$.

4.4.2 Semantic types

In the following, let $\mathscr{A}, \mathscr{B} \in \mathsf{CR}$ be candidates, P a proposition, $\mathscr{K}$ some index set and $\mathscr{F} \in \mathscr{K} \to \mathsf{CR}$ a family of reducibility candidates. The following operations,

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

except the conditional $P \Rightarrow \mathscr{A}$, construct new candidates from existing ones.

$$\begin{aligned}
\mathscr{A} \to \mathscr{B} &= \{r \in \mathsf{SN} \mid \forall s \in \mathscr{A}.\, r\,s \in \mathscr{B}\} \\
\forall_{\mathscr{K}} \mathscr{F} &= \{r \in \mathsf{SN} \mid \forall G \in \mathsf{Type}, \mathscr{G} \in \mathscr{K}.\, r\,G \in \mathscr{F}(\mathscr{G})\} \\
P \Rightarrow \mathscr{A} &= \{r \in \mathsf{Exp} \mid r \in \mathscr{A} \text{ if } P\} \\
\mathbf{1} &= \overline{\{()\}} \\
\mathscr{A}_1 \times \mathscr{A}_2 &= \overline{\{(t_1, t_2) \mid t_1 \in \mathscr{A}_1 \text{ and } t_2 \in \mathscr{A}_2\}} \\
\exists_{\mathscr{K}} \mathscr{F} &= \overline{\{{}^G t \mid G \in \mathsf{Type}, \exists \mathscr{G} \in \mathscr{K}.\, t \in \mathscr{F}(\mathscr{G})\}}.
\end{aligned}$$

Note that the condition $r \in \mathsf{SN}$ in the definition of $\mathscr{A} \to \mathscr{B}$ is redundant, since $x \in \mathscr{A}$ by **CR3** and $r\,x \in \mathsf{SN}$ implies $r \in \mathsf{SN}$. However, in the definition of $\forall_{\mathscr{K}} \mathscr{F}$, it is important since $\mathscr{K}$ could be empty, e. g., $\mathscr{K} = {<}0$; the set $\forall_{\emptyset} \mathscr{F}$ is the greatest candidate. Conditional types are not first-class; $P \Rightarrow \mathscr{A}$ only forms a candidate if P is true, otherwise, it is just a set of expressions, namely, the set Exp of all expressions.

Lemma 5 (*Function space candidate*)
If $\mathsf{Var} \subseteq \mathscr{A} \subseteq \mathsf{SN}$ and $\mathscr{B} \in \mathsf{CR}$, then $\mathscr{A} \to \mathscr{B} \in \mathsf{CR}$.

Proof

CR1 Strong normalization: Let $r \in \mathscr{A} \to \mathscr{B}$. Since $x \in \mathscr{A}$, we have $r\,x \in \mathscr{B} \subseteq \mathsf{SN}$, thus, $r \in \mathsf{SN}$.

CR2 Closure under reduction: Let $r \in \mathscr{A} \to \mathscr{B}$ and $r \longrightarrow r'$. Assume $s \in \mathscr{A}$ and show $r'\,s \in \mathscr{B}$, which we conclude by **CR2** on $r\,s \in \mathscr{B}$, since $r\,s \longrightarrow r'\,s$.

CR3 Closure under neutrals: Let $r \in \mathsf{Ne}$ and $(r \longrightarrow \_) \subseteq \mathscr{A} \to \mathscr{B}$. Since $\mathscr{A} \to \mathscr{B} \subseteq \mathsf{SN}$, we have $r \in \mathsf{SN}$. Assume $s \in \mathscr{A}$. We show $r\,s \in \mathscr{B}$ by **CR3**, exploiting $r\,s \in \mathsf{Ne}$. Consider $r\,s \longrightarrow t$; we show $t \in \mathscr{B}$ by induction on $r, s \in \mathsf{SN}$. Since $r \in \mathsf{Ne}$, either $t = r'\,s$ with $r \longrightarrow r'$ and we conclude by induction hypothesis on $r' \in \mathsf{SN}$, or $t = r\,s'$ with $s \longrightarrow s'$ and we conclude by induction hypothesis on $s' \in \mathsf{SN}$.

CR4 Closure under simulation: Let $r \notin \mathsf{Intro}$ and $(r \longrightarrow \_) \subseteq \mathscr{A} \to \mathscr{B}$ and $r \rhd \vec{r} \in \mathscr{A} \to \mathscr{B}$. Assume $s \in \mathscr{A}$ and show $r\,s \in \mathscr{B}$ by **CR4**, exploiting that $r\,s \notin \mathsf{Intro}$ and $r\,s \rhd r_1\,s, \ldots, r_n\,s \in \mathscr{B}$. Assume $r\,s \longrightarrow t$ and show $t \in \mathscr{B}$ by induction on $r, s \in \mathsf{SN}$. In cases $t = r'\,s$ or $t = r\,s'$, we conclude by induction hypothesis. In the remaining case $r\,s \mapsto t$, we have $r_k\,s \mapsto t$ for some $k \in 1..n$. Since $r_k\,s \in \mathscr{B}$, we conclude $t \in \mathscr{B}$ by **CR2**. □

Lemma 6 (*Semantic typing rules*)
The following inferences are trivial consequences of the construction of semantic types:

$$\frac{r \in \mathscr{A} \to \mathscr{B} \qquad s \in \mathscr{A}}{r\,s \in \mathscr{B}} \qquad \frac{r \in \forall_{\mathscr{K}} \mathscr{F} \qquad \mathscr{G} \in \mathscr{K}}{r\,G \in \mathscr{F}(\mathscr{G})}$$

$$\frac{}{() \in \mathbf{1}} \qquad \frac{t_1 \in \mathscr{A}_1 \qquad t_2 \in \mathscr{A}_2}{(t_1, t_2) \in \mathscr{A}_1 \times \mathscr{A}_2} \qquad \frac{\mathscr{G} \in \mathscr{K} \qquad t \in \mathscr{F}(\mathscr{G})}{{}^G t \in \exists_{\mathscr{K}} \mathscr{F}}.$$

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

Besides definitions (which we will treat in Section 4.8), rules for constructors and destructors are missing. We will describe semantic (co)inductive types in the next section.

4.5 Ordinals and fixed-points

Previous approaches to type-based termination (Hughes *et al.*, 1996; Amadio & Coupet-Grimal, 1998; Barthe *et al.*, 2004; Blanqui, 2004; Barthe *et al.*, 2008; Sacchini, 2013) have defined approximants of least $\boldsymbol{\mu}^\alpha\mathscr{F}$ and greatest fixed-points $\boldsymbol{\nu}^\alpha\mathscr{F}$ of monotone type constructors $\mathscr{F} \in \mathsf{CR} \xrightarrow{+} \mathsf{CR}$ by conventional induction on ordinal α, distinguishing zero (0), successor $(\alpha+1)$ and limit ordinals (λ).

$$\begin{array}{llll} \boldsymbol{\mu}^0\ \mathscr{F} & = & \overline{\emptyset} & \qquad \boldsymbol{\nu}^0\ \mathscr{F} = \mathsf{SN} \\ \boldsymbol{\mu}^{\alpha+1}\mathscr{F} & = & \mathscr{F}\,(\boldsymbol{\mu}^\alpha\,\mathscr{F}) & \qquad \boldsymbol{\nu}^{\alpha+1}\mathscr{F} = \mathscr{F}\,(\boldsymbol{\nu}^\alpha\,\mathscr{F}) \\ \boldsymbol{\mu}^\lambda\ \mathscr{F} & = & \overline{\bigcup_{\alpha<\lambda} \boldsymbol{\mu}^\alpha\mathscr{F}} & \qquad \boldsymbol{\nu}^\lambda\ \mathscr{F} = \bigcap_{\alpha<\lambda} \boldsymbol{\nu}^\alpha\mathscr{F}. \end{array}$$

In this work, we adopt the approach of Sprenger and Dam (2003) for approximations in μ-calculus and use *well-founded induction* instead, which amounts to construct $\boldsymbol{\mu}^\alpha\mathscr{F}$ by *inflationary iteration* and $\boldsymbol{\nu}^\alpha\mathscr{F}$ by *deflationary iteration.*

$$\boldsymbol{\mu}^\alpha\mathscr{F} = \overline{\bigcup_{\beta<\alpha} \mathscr{F}\,(\boldsymbol{\mu}^\beta\mathscr{F})} \qquad \boldsymbol{\nu}^\alpha\mathscr{F} = \bigcap_{\beta<\alpha} \mathscr{F}\,(\boldsymbol{\nu}^\beta\mathscr{F}).$$

In this definition, $\mathscr{F}$ does not have to be monotone to obtain an ascending chain of approximants in case of $\boldsymbol{\mu}$ and a descending chain for $\boldsymbol{\nu}$. However, if $\mathscr{F}$ is monotone, one can derive above equations as special cases for α being zero, successor, or limit ordinal, *if such a distinction on ordinals exists.* Intuitionistically, this distinction is not valid (Taylor, 1996); by building on well-founded induction, we keep the option of a constructive proof.

Let α, β, γ range over ordinals. We write $\forall_{\beta<\alpha}\mathscr{F}(\beta)$ for $\forall_{<\alpha}\mathscr{F}$ and analogously for $\exists$. Let $\mathscr{S} \in \mathsf{Cons} \rightharpoonup \mathsf{CR} \to \mathsf{CR}$ and $\mathscr{R} \in \mathsf{Proj} \rightharpoonup \mathsf{CR} \to \mathsf{CR}$, where we write the first argument, the constructor c, or the destructor d, resp., as index, thus, $\mathscr{S}_c$ and $\mathscr{R}_d$ resp. We define the αth approximants $\boldsymbol{\mu}^\alpha\mathscr{S}, \boldsymbol{\nu}^\alpha\mathscr{R} \in \mathsf{CR}$ of recursive variant and record type as follows:

$$\begin{array}{lcl} \boldsymbol{\mu}^\alpha\mathscr{S} & = & \overline{\{c\,t \mid c \in \mathsf{dom}(\mathscr{S}) \text{ and } t \in \exists_{\beta<\alpha}\mathscr{S}_c(\boldsymbol{\mu}^\beta\mathscr{S})\}} \\ \boldsymbol{\nu}^\alpha\mathscr{R} & = & \{r \in \mathsf{SN} \mid \forall d \in \mathsf{dom}(\mathscr{R}).\, r.d \in \forall_{\beta<\alpha}\mathscr{R}_d(\boldsymbol{\nu}^\beta\mathscr{R})\}. \end{array}$$

Since $\exists_{<\alpha}\mathscr{F}$ is monotonic in α for any $\mathscr{F}$, so is $\boldsymbol{\mu}^\alpha\mathscr{S}$. Dually, $\forall_{<\alpha}\mathscr{F}$ and $\boldsymbol{\nu}^\alpha\mathscr{R}$ are antitonic in α. We obtain chains:

$$\begin{array}{l} \overline{\emptyset} = \boldsymbol{\mu}^0\mathscr{S} \subseteq \boldsymbol{\mu}^1\mathscr{S} \subseteq \ldots \subseteq \boldsymbol{\mu}^\gamma\mathscr{S} \subseteq \boldsymbol{\mu}^{\gamma+1}\mathscr{S} \subseteq \ldots \\ \mathsf{SN} = \boldsymbol{\nu}^0\mathscr{R} \supseteq \boldsymbol{\nu}^1\mathscr{R} \supseteq \ldots \supseteq \boldsymbol{\nu}^\gamma\mathscr{R} \supseteq \boldsymbol{\nu}^{\gamma+1}\mathscr{R} \supseteq \ldots \end{array}$$

If $\boldsymbol{\mu}^\alpha\mathscr{S} = \boldsymbol{\mu}^\gamma\mathscr{S}$ for some $\alpha > \gamma$, then $\boldsymbol{\mu}^\beta\mathscr{S} = \boldsymbol{\mu}^\gamma\mathscr{S}$ for all $\beta > \gamma$ and we say that the chain has become *stationary* at γ. Since the set Exp of expressions is countable and all elements of these chains are subsets of Exp, the chains must become stationary

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

latest at the first uncountable ordinal Ω. We call the ordinal at which all such chains of our language are stationary the *closure ordinal* and denote it by ∞.

Since it does not make sense to inspect chains beyond the closure ordinal, we introduce *bound normalization*

$$\alpha^{\uparrow} = \begin{cases} \infty + 1 & \text{if } \alpha \geqslant \infty, \\ \alpha & \text{otherwise.} \end{cases}$$

Note that $\boldsymbol{\mu}^{\alpha}\mathscr{S} = \boldsymbol{\mu}^{\alpha^{\uparrow}}\mathscr{S}$ and $\boldsymbol{\nu}^{\alpha}\mathscr{R} = \boldsymbol{\nu}^{\alpha^{\uparrow}}\mathscr{R}$. In the following, we will talk about ordinals that are as big as $\infty + n$ for finite n, but not bigger ones, so all ordinals will be in $\mathsf{O} = \{\alpha \mid \alpha < \infty + \omega\}$, a set closed under successor. As size index to a least or greatest fixed point, only the ordinals $\alpha \leqslant \infty$ are interesting. Thus, if no bound for an ordinal β is given, we assume $\beta \leqslant \infty$, for instance, we write $\exists_{\beta}\mathscr{F}(\beta)$ instead of $\exists_{\beta \leqslant \infty}\mathscr{F}(\beta)$.

The stationary point $\boldsymbol{\mu}^{\infty}\mathscr{S}$ is a pre-fixed point in the sense that $t \in \mathscr{S}_c(\boldsymbol{\mu}^{\infty}\mathscr{S})$ implies $c\,{}^{\infty}t \in \boldsymbol{\mu}^{\infty+1}\mathscr{S} = \boldsymbol{\mu}^{\infty}\mathscr{S}$. Dually, $\boldsymbol{\nu}^{\infty}\mathscr{R}$ is a post-fixed point as $r \in \boldsymbol{\nu}^{\infty}\mathscr{R} = \boldsymbol{\nu}^{\infty+1}\mathscr{R}$ implies $r.d\,\infty \in \mathscr{R}_d(\boldsymbol{\nu}^{\infty}\mathscr{R})$. Note that we do not require $\mathscr{R}$ or $\mathscr{S}$ to be monotone for the implications to hold in these directions. Yet, we do if we want $\boldsymbol{\mu}^{\infty}\mathscr{S}$ and $\boldsymbol{\nu}^{\infty}\mathscr{R}$ to be fixed-points.

Lemma 7 (*Pre-/post-fixed points*)

1. If $t \in \exists_{\beta \leqslant \infty}\mathscr{S}_c(\boldsymbol{\mu}^{\beta}\mathscr{S})$, then $c\,t \in \boldsymbol{\mu}^{\infty}\mathscr{S}$.
2. If $r \in \boldsymbol{\nu}^{\infty}\mathscr{R}$, then $r.d \in \forall_{\beta \leqslant \infty}\mathscr{R}_d(\boldsymbol{\nu}^{\beta}\mathscr{R})$.

Proof

1. By definition, $c\,t \in \boldsymbol{\mu}^{\infty+1}\mathscr{S} = \boldsymbol{\mu}^{\infty}\mathscr{S}$.
2. By definition, since $r \in \boldsymbol{\nu}^{\infty+1}\mathscr{R}$.

Lemma 8 (*Fixed-points*)
If $\mathscr{S}_c, \mathscr{R}_d$ be monotone for all $c \in \mathsf{dom}(\mathscr{S})$ and $d \in \mathsf{dom}(\mathscr{R})$, then

1. $\boldsymbol{\mu}^{\infty}\mathscr{S} = \overline{\{c\,{}^{b}t \mid c \in \mathsf{dom}(\mathscr{S}), b \in \mathsf{Type}, t \in \mathscr{S}_c(\boldsymbol{\mu}^{\infty}\mathscr{S})\}}$, and
2. $\boldsymbol{\nu}^{\infty}\mathscr{R} = \{r \mid \forall d \in \mathsf{dom}(\mathscr{R}), b \in \mathsf{Type}.\ r.d\ b \in \mathscr{R}_d(\boldsymbol{\nu}^{\infty}\mathscr{R})\}$.

Proof
For 1, it is sufficient to show $\subseteq$, meaning that $\boldsymbol{\mu}^{\infty}\mathscr{S}$ is a post-fixed point. Note that by definition

$$\boldsymbol{\mu}^{\infty}\mathscr{S} = \overline{\bigcup_{\beta<\infty}\{c\,{}^{b}t \mid c \in \mathsf{dom}(\mathscr{S}), b \in \mathsf{Type}, t \in \mathscr{S}_c(\boldsymbol{\mu}^{\beta}\mathscr{S})\}},$$

so we conclude by monotonicity of $\mathscr{S}_c$ and the closure operator, using $\boldsymbol{\mu}^{\beta}\mathscr{S} \subseteq \boldsymbol{\mu}^{\infty}\mathscr{S}$.

For 2, it is sufficient to show that $\boldsymbol{\nu}^{\infty}\mathscr{R}$ is a pre-fixed point. So, if $r.d\ b \in \mathscr{R}_d(\boldsymbol{\nu}^{\infty}\mathscr{R})$ for all $d \in \mathsf{dom}(\mathscr{R})$ and $b \in \mathsf{Type}$, then $r \in \boldsymbol{\nu}^{\infty}\mathscr{R}$. It is sufficient to show $r.d\ b \in \mathscr{R}_d(\boldsymbol{\nu}^{\beta}\mathscr{R})$ for all $\beta < \infty$, and this follows from $\boldsymbol{\nu}^{\infty}\mathscr{R} \subseteq \boldsymbol{\nu}^{\beta}\mathscr{R}$ by monotonicity of $\mathscr{R}_d$. □

Corollary 9

1. If $c\,{}^{b}t \in \boldsymbol{\mu}^{\infty}\mathscr{S}$ and $\mathscr{S}_c$ is monotone, then $t \in \mathscr{S}_c(\boldsymbol{\mu}^{\infty}\mathscr{S})$.
2. If $r.d\,b \in \mathscr{R}_d(\boldsymbol{\nu}^{\infty}\mathscr{R})$ and $\mathscr{R}_d$ is monotone, then $r \in \boldsymbol{\nu}^{\infty}\mathscr{R}$.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

4.6 Kinds

In this section, we construct semantic kinds to interpret the syntactic kinds of $\mathsf{F}^{\mathsf{cop}}_{\omega}$. Since types $A : *$ are interpreted as reducibility candidates, base kind $*$ will be interpreted as CR, the set of all reducibility candidates, partially ordered by inclusion. Sizes $a < b$ denote ordinals $\alpha < \beta$, thus, kind $<b$ will be interpreted as initial segment $\{\alpha \mid \alpha < \beta\}$ of the ordinals, ordered by size. A type constructor $F : \kappa \to \kappa'$ denotes an operator $\mathscr{F}$ mapping semantic objects $\mathscr{G}$ of kind κ to semantic objects $\mathscr{F}(\mathscr{G})$ of kind κ', thus, kind $\kappa \to \kappa'$ can be interpreted as the full set-theoretic function space $\mathscr{K} \to \mathscr{K}'$, where $\mathscr{K}$ is the interpretation of κ and $\mathscr{K}'$ the one of κ'. Variances π denote monotonicity behavior, e.g., $+\kappa \to \kappa'$ will be interpreted as the set of *monotone* operators from $\mathscr{K}$ to $\mathscr{K}'$.

We consider kinds κ with variance information as refinements of simple kinds ι that lack such information, thus, the interpretation $[\![\iota]\!]$ of simple kinds is given first.

$$\begin{array}{lcl} [\![*]\!] & = & \mathsf{CR} \\ [\![o]\!] & = & \mathsf{O} \\ [\![\iota \to \iota']\!] & = & [\![\iota]\!] \to [\![\iota']\!]. \end{array}$$

A simple function kind $\iota \to \iota'$ is interpreted as the function space $[\![\iota]\!] \to [\![\iota']\!]$ of the meta-language (e.g., the set-theoretical function space).

With each simple kind ι, we associate a set $\mathsf{Kl}(\iota)$ of *semantic kinds* $\mathscr{K} \subseteq [\![\iota]\!]$. Semantic kinds $\mathscr{K}$ are pointed preorders. We write $\bot_{\mathscr{K}}$ for the least element of $\mathscr{K}$ and $\mathscr{F} \leqslant \mathscr{F}' \in \mathscr{K}$ for the preorder relation, omitting "$\in \mathscr{K}$" when clear from the context of discourse. In general, for a preorder $\leqslant$ let

$$\begin{array}{ll} \mathscr{F} \leqslant^{\circ} \mathscr{F}' & :\Longleftrightarrow \mathscr{F} \leqslant \mathscr{F}' \text{ and } \mathscr{F}' \leqslant \mathscr{F} \\ \mathscr{F} \leqslant^{+} \mathscr{F}' & :\Longleftrightarrow \mathscr{F} \leqslant \mathscr{F}' \\ \mathscr{F} \leqslant^{-} \mathscr{F}' & :\Longleftrightarrow \mathscr{F}' \leqslant \mathscr{F} \\ \mathscr{F} \leqslant^{\top} \mathscr{F}' & :\Longleftrightarrow \text{true}. \end{array}$$

For the special case of posets, $\leqslant^{\circ}$ coincides with equality, but we will later encounter proper preordered sets, where $\leqslant^{\circ}$ is just an equivalence relation and not identity.

Lemma 10 (*Soundness of variance ordering*)
If $\pi \leqslant \pi'$ and $\mathscr{F} \leqslant^{\pi} \mathscr{F}'$, then $\mathscr{F} \leqslant^{\pi'} \mathscr{F}'$.

We sometimes may write $\mathscr{F} \leqslant \mathscr{F}' \in \pi\mathscr{K}$ for $\mathscr{F} \leqslant^{\pi} \mathscr{F}' \in \mathscr{K}$, and this notation extends beyond semantics kinds to any preorder $(\mathscr{K}, \leqslant)$. Note that for $\mathscr{F} \in \mathscr{K}$, we have not only reflexivity $\mathscr{F} \leqslant \mathscr{F} \in \mathscr{K}$, but also generalized reflexivity $\mathscr{F} \leqslant^{\pi} \mathscr{F} \in \mathscr{K}$ for any π.

If $\mathscr{K} \in \mathsf{Kl}(\iota)$ and $\mathscr{K}' \in \mathsf{Kl}(\iota')$ is a pointed preorder, then the function space

$$\mathscr{K} \to \mathscr{K}' \in \mathsf{Kl}(\iota \to \iota')$$

$$\mathscr{K} \to \mathscr{K}' = \{\mathscr{F} \in [\![\iota]\!] \to [\![\iota']\!] \mid \forall \mathscr{G} \in \mathscr{K}.\ \mathscr{F}(\mathscr{G}) \in \mathscr{K}'\}$$

is a pointed preorder with least element $\bot_{\mathscr{K} \to \mathscr{K}'}(\mathscr{G}) = \bot_{\mathscr{K}'}$, pointwise ordered by $\mathscr{F} \leqslant \mathscr{F}' \in \mathscr{K} \to \mathscr{K}'$ iff $\mathscr{F}(\mathscr{G}) \leqslant \mathscr{F}'(\mathscr{G}) \in \mathscr{K}'$, for all $\mathscr{G} \in \mathscr{K}$.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

For posets $\mathscr{K}, \mathscr{K}'$ let $\mathscr{K} \xrightarrow{\circ} \mathscr{K}'$ be just $\mathscr{K} \to \mathscr{K}'$, the full function space, $\mathscr{K} \xrightarrow{+} \mathscr{K}'$ denote the subspace of monotone functions, $\mathscr{K} \xrightarrow{-} \mathscr{K}'$ the antitone ones and $\mathscr{K} \xrightarrow{\top} \mathscr{K}'$ the constant functions. Clearly, if $\mathscr{F} \in \mathscr{K} \xrightarrow{\pi} \mathscr{K}'$ and $\mathscr{G} \leqslant^{\pi} \mathscr{G}' \in \mathscr{K}$, then $\mathscr{F}(\mathscr{G}) \leqslant \mathscr{F}(\mathscr{G}') \in \mathscr{K}'$.

We define the type of semantic kinds $\mathsf{KI}(\iota)$ associated to simple kind ι inductively by the rules

$$\frac{}{\mathsf{CR} \in \mathsf{KI}(*)} \qquad \frac{\beta \in \mathsf{O}}{(<\beta) \in \mathsf{KI}(o)} \qquad \frac{\mathscr{K} \in \mathsf{KI}(\iota) \qquad \mathscr{K}' \in \mathsf{KI}(\iota')}{\mathscr{K} \xrightarrow{\pi} \mathscr{K}' \in \mathsf{KI}(\iota \to \iota')}.$$

(Alternatively, $\mathsf{KI}(\iota)$ could be defined by recursion on ι.) Note that $\bot_{\mathsf{CR}} = \overline{\emptyset}$ and $\bot_{\mathsf{O}} = 0$.

Not only is each semantic kind $\mathscr{K} \in \mathsf{KI}(\iota)$ a preorder, but semantics kinds $\mathscr{K}, \mathscr{K}' \in \mathsf{KI}(\iota)$ can be themselves compared by inclusion $\mathscr{K} \subseteq \mathscr{K}'$, thus, each $\mathsf{KI}(\iota)$ is a partial order. This models subkinding, see Theorem 16.

4.6.1 Type environments

We pointwise extend the kind erasure $|\kappa| = \iota$ to kinding contexts Δ: $|\cdot| = \cdot$ and $|\Delta, X{:}\pi\kappa| = |\Delta|, X{:}|\kappa|$. Erased kinding contexts are interpreted as sets $[\![|\Delta|]\!]$ of environments $\rho \in [\![|\Delta|]\!]$ inductively defined by

$$\frac{}{\cdot \in [\![\cdot]\!]} \qquad \frac{\rho \in [\![|\Delta|]\!] \qquad \mathscr{G} \in [\![\iota]\!]}{(\rho, \mathscr{G}/X) \in [\![|\Delta|, X{:}\iota]\!]}.$$

(Alternatively, $[\![|\Delta|]\!]$ could be defined by recursion on the length of $|\Delta|$.) Environments ρ can be understood as finite maps from type constructor variables X to an appropriate semantic object $\mathscr{G} \in [\![|\Delta(X)|]\!]$ (an ordinal, a semantic type or a type operator). We will also use the notation ρ, ρ' for environment concatenation, with the precondition that $\mathsf{dom}(\rho)$ is disjoint from $\mathsf{dom}(\rho')$.

4.6.2 Semantic kinding contexts

In the following, we define semantic kinding contexts $\mathscr{D} \in \mathsf{KICXT}(|\Delta|)$ as counterparts of syntactic kinding contexts Δ. Each $\mathscr{D}$ induces a preordered subset $[\mathscr{D}] \subseteq [\![|\Delta|]\!]$ of (semantic) type environments $\rho \in [\mathscr{D}]$ (written just $\rho \in \mathscr{D}$). Analogously to syntactic contexts, semantic kinding contexts are finite maps from type constructor variables X to a pair of variance π and semantic kind $\mathscr{K}$ which may depend on "earlier variables" of mixed variance only. This dependency is expressed by $\mathscr{D}' \in \circ^{-1}\mathscr{D} \to \mathsf{KICXT}(|\Delta'|)$ in the rule for $\Sigma_{\mathscr{D}}\mathscr{D}' \in \mathsf{KICXT}(|\Delta, \Delta'|)$ below. Intuitively, it means that $\mathscr{D}'$ respects relatedness in $\mathscr{D}$ given by $\rho \leqslant \rho' \in \mathscr{D}$ (see below), meaning that then $\mathscr{D}'(\rho) = \mathscr{D}'(\rho')$. Formally, it states that $\mathscr{D}'(\rho) = \mathscr{D}'(\rho')$ is implied by $\rho \leqslant^{\circ} \rho' \in \circ^{-1}\mathscr{D}$ which means that $\mathscr{D}'$ maps "equal" ($\leqslant^{\top}$) environments with regard to $\circ^{-1}\mathscr{D}$ to equal semantic kinding contexts. Semantic kinding contexts $\boxed{\mathscr{D} \in \mathsf{KICXT}(|\Delta|)}$ are defined inductively by the

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

rules

$$\frac{}{\cdot \in \mathsf{KICXT}(\cdot)} \qquad \frac{\mathscr{K} \in \mathsf{KI}(\iota)}{(X{:}\pi\mathscr{K}) \in \mathsf{KICXT}(X{:}\iota)}$$

$$\frac{\mathscr{D} \in \mathsf{KICXT}(|\Delta|) \qquad \mathscr{D}' \in \circ^{-1}\mathscr{D} \to \mathsf{KICXT}(|\Delta'|)}{\Sigma_{\mathscr{D}}\mathscr{D}' \in \mathsf{KICXT}(|\Delta, \Delta'|)}.$$

Note that for any $\mathscr{D} \in \mathsf{KICXT}(|\Delta|)$, we have $\mathsf{dom}(\mathscr{D}) = \mathsf{dom}(|\Delta|)$, thus, $\mathscr{D}$ and $\mathscr{D}'(\rho)$ have disjoint domain in the last rule for any $\rho \in [\![|\Delta|]\!]$. We may simply say that $\mathscr{D}$ and $\mathscr{D}'$ are "disjoint".

Simultaneously with $\mathscr{D} \in \mathsf{KICXT}(|\Delta|)$, we construct a preordered set of type environments; for $\rho, \rho' \in [\![|\Delta|]\!]$, we define $\boxed{\rho \leqslant \rho' \in \mathscr{D}}$ by recursion on $\mathscr{D} \in \mathsf{KICXT}(|\Delta|)$—an inductive–recursive definition (Dybjer, 2000).

$$\begin{array}{rcl} \cdot \leqslant \cdot \in \cdot & :\Longleftrightarrow & \mathsf{true} \\ (\mathscr{G}/X) \leqslant (\mathscr{G}'/X) \in (X{:}\pi\mathscr{K}) & :\Longleftrightarrow & \mathscr{G} \leqslant^{\pi} \mathscr{G}' \in \mathscr{K} \\ (\rho_1, \rho_2) \leqslant (\rho_1', \rho_2') \in \Sigma_{\mathscr{D}}\mathscr{D}' & :\Longleftrightarrow & \rho_1 \leqslant \rho_1' \in \mathscr{D} \text{ and } \rho_2 \leqslant \rho_2' \in \mathscr{D}'(\rho_1). \end{array}$$

The last line shows that it is important that $\mathscr{D}'$ respects $\mathscr{D}$, because how would we otherwise know that $\mathscr{D}'(\rho_1) = \mathscr{D}'(\rho_1')$, and thus $\rho_2' \in \mathscr{D}'(\rho_1)$?[7]

Inverse application of polarities $\boxed{\pi^{-1}\mathscr{D}}$ is defined simultaneously with KICXT as well, in analogy to the syntactic variant $\pi^{-1}\Delta$ as given in Figure 5.

$$\begin{array}{lcl} \pi^{-1}(\cdot) & = & \cdot \\ \pi^{-1}(X{:}\pi'\mathscr{K}) & = & (X{:}(\pi^{-1}\pi')\mathscr{K}) \\ \pi^{-1}(\Sigma_{\mathscr{D}}\mathscr{D}') & = & \Sigma_{(\pi^{-1}\mathscr{D})}(\pi^{-1}\mathscr{D}'). \end{array}$$

In the last clause, $\pi^{-1}\mathscr{D}'$ is defined pointwise as $(\pi^{-1}\mathscr{D}')(\rho) = \pi^{-1}(\mathscr{D}'(\rho))$. Note that the laws for $\pi^{-1}\Delta$ hold also for $\pi^{-1}\mathscr{D}$, in particular, $+^{-1}\mathscr{D} = \mathscr{D}$ and $-^{-1}\mathscr{D} = -\mathscr{D}$.

Lemma 11 (*Well-definedness of partial order on type environments*)
If $\mathscr{D} \in \mathsf{KICXT}(|\Delta|)$, then $\rho \leqslant \rho' \in \mathscr{D}$ is well-defined. Further, if $\rho \leqslant \rho' \in \mathscr{D}$, then $\rho \leqslant \rho' \in \circ^{-1}\mathscr{D}$ and even $\rho \leqslant^{\circ} \rho' \in \circ^{-1}\mathscr{D}$.

Proof
By induction on $\mathscr{D} \in \mathsf{KICXT}(|\Delta|)$. It is even true that $\rho \leqslant \rho' \in \pi_1^{-1}\mathscr{D}$ implies $\rho \leqslant \rho' \in \pi_2^{-1}\mathscr{D}$, for any $\pi_1 \geqslant \pi_2$ (antitonicity of inverse application). Instantiating this with $\pi_1 = +$ and $\pi_2 = \circ$ yields the first statement on orders; for the second, we observe that $\rho \leqslant^{\pi} \rho' \in \mathscr{D}$ iff $\rho \leqslant \rho' \in \pi\mathscr{D}$ and that $\circ\circ^{-1}\mathscr{D} = \circ^{-1}\mathscr{D}$. Well-definedness follows in case $\Sigma_{\mathscr{D}}\mathscr{D}'$ since $\rho_1 \leqslant \rho_1' \in \mathscr{D}$ implies $\rho_1 \leqslant^{\circ} \rho_1' \in \circ^{-1}\mathscr{D}$ and thus $\mathscr{D}'(\rho_1) = \mathscr{D}'(\rho_1')$. □

[7] The weaker requirement $\mathscr{D}' \in -\mathscr{D} \to \mathsf{KICXT}(|\Delta'|)$, antitonicity of $\mathscr{D}'$, would still allow us to define $(\rho_1, \rho_2) \leqslant (\rho_1', \rho_2') \in \Sigma_{\mathscr{D}}\mathscr{D}'$, since $\rho_1 \leqslant \rho_1'$ then implies that $\mathscr{D}'(\rho_1') \subseteq \mathscr{D}'(\rho_1)$. However, inverse application of polarities $\pi^{-1}\mathscr{D}$ would then not be well-defined, for instance in case $\pi = -$. Concretely, while context $\Delta = (i{:}-(\leqslant\infty), j{:}+(<i))$ is well-formed, $-^{-1}\Delta = (i{:}+(\leqslant\infty), j{:}-(<i))$ is not. A similar problem arises with monotone $\mathscr{D}' \in \mathscr{D} \to \mathsf{KICXT}(|\Delta'|)$ and ordering of pairs modified to $\rho_2 \leqslant \rho_2' \in \mathscr{D}'(\rho_1')$.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

$\boxed{\rho \in \mathscr{D}}$ is now simply defined as $\rho \leqslant \rho \in \mathscr{D}$. If in singleton contexts $(X{:}\pi\mathscr{K})$, we restrict $\mathscr{K}$ to be of the form $<\beta$, we obtain *semantic size contexts* $\boxed{\mathscr{D} \in \mathsf{SICXT}(|\Psi|)}$. Clearly, these are special semantic kinding contexts.

Lemma 12 (*Transitivity of environment comparison*)
Let $\mathscr{D} \in \mathsf{KICXT}(|\Delta|)$. If $\rho_1 \leqslant \rho_2 \in \mathscr{D}$ and $\rho_2 \leqslant \rho_3 \in \mathscr{D}$, then $\rho_1 \leqslant \rho_3 \in \mathscr{D}$.

Proof
By induction on $\mathscr{D} \in \mathsf{KICXT}(|\Delta|)$. The interesting case is pairing

$$\frac{\mathscr{D} \in \mathsf{KICXT}(|\Delta|) \qquad \mathscr{D}' \in \circ^{-1}\mathscr{D} \to \mathsf{KICXT}(|\Delta'|)}{\Sigma_{\mathscr{D}}\mathscr{D}' \in \mathsf{KICXT}(|\Delta, \Delta'|)}.$$

By decomposition of the assumptions, we have $\rho_1 \leqslant \rho_2 \in \mathscr{D}$ and $\rho_1' \leqslant \rho_2' \in \mathscr{D}'(\rho_1)$ and also $\rho_2 \leqslant \rho_3 \in \mathscr{D}$ and $\rho_2' \leqslant \rho_3' \in \mathscr{D}'(\rho_2)$. The first induction hypothesis gives us $\rho_1 \leqslant \rho_3 \in \mathscr{D}$. By respect, $\mathscr{D}'(\rho_1) = \mathscr{D}'(\rho_2)$ which allows us to apply the second induction hypothesis on $\mathscr{D}'(\rho_1)$ to obtain $\rho_1' \leqslant \rho_3' \in \mathscr{D}'(\rho_1)$. □

This makes each $\mathscr{D} \in \mathsf{KICXT}(|\Delta|)$ a preorder, as reflexivity holds by definition of $\rho \in \mathscr{D}$. Note that we equivalently could have defined $\rho \in \mathscr{D}$ inductively by

$$\begin{array}{rcll} \cdot & \in & \cdot & :\Longleftrightarrow \text{ true} \\ (\mathscr{G}/X) & \in & (X{:}\pi\mathscr{K}) & :\Longleftrightarrow \mathscr{G} \in \mathscr{K} \\ (\rho, \rho') & \in & \Sigma_{\mathscr{D}}\mathscr{D}' & :\Longleftrightarrow \rho \in \mathscr{D} \text{ and } \rho' \in \mathscr{D}'(\rho) \end{array}$$

and proven that $\rho \in \mathscr{D}$ implies $\rho \leqslant \rho \in \mathscr{D}$.

Lemma 13 (*Preservation of context well-formedness*)
If $\mathscr{D} \in \mathsf{KICXT}(|\Delta|)$, then $\pi^{-1}\mathscr{D} \in \mathsf{KICXT}(|\Delta|)$.

Proof
By induction on $\mathscr{D} \in \mathsf{KICXT}(|\Delta|)$. The interesting case is concatenation:

$$\frac{\mathscr{D} \in \mathsf{KICXT}(|\Delta|) \qquad \mathscr{D}' \in \circ^{-1}\mathscr{D} \to \mathsf{KICXT}(|\Delta'|)}{\Sigma_{\mathscr{D}}\mathscr{D}' \in \mathsf{KICXT}(|\Delta, \Delta'|)}.$$

By induction hypothesis $\pi^{-1}\mathscr{D} \in \mathsf{KICXT}(|\Delta|)$ and $\pi^{-1}\mathscr{D}'(\rho) \in \mathsf{KICXT}(|\Delta'|)$, for all $\rho \in \circ^{-1}\mathscr{D}$. It remains to show that $\pi^{-1}\mathscr{D}'$ respects $\pi^{-1}\circ^{-1}\mathscr{D}$ which is equal to $(\pi\circ)^{-1}\mathscr{D}$. Assume $\rho \leqslant^{\circ} \rho' \in (\pi\circ)^{-1}\mathscr{D}$. Since $\rho \leqslant^{\circ} \rho' \in \circ^{-1}\mathscr{D}$ by antitonicity $(\pi\circ \geqslant \circ)$, we have $\mathscr{D}'(\rho) = \mathscr{D}'(\rho')$ and, thus, $\pi^{-1}\mathscr{D}'(\rho) = \pi^{-1}\mathscr{D}'(\rho')$ as desired. □

We shall omit $|\Delta|$ from $\mathsf{KICXT}(|\Delta|)$ when inessential or inferable. We drop singleton function domains, e.g., we identify $\cdot \to \mathsf{KICXT}$ with KICXT. Given a parametrized kinding context $\mathscr{D}_2 \in \mathscr{D} \to \mathsf{KICXT}$, we can weaken it to $\mathsf{W}_{\mathscr{D}_1}\mathscr{D}_2 \in (\mathscr{D}_1 \times \mathscr{D}) \to \mathsf{KICXT}$, where $(\mathsf{W}_{\mathscr{D}_1}\mathscr{D}_2)(\rho_1 \in \mathscr{D}_1, \rho) = \mathscr{D}_2(\rho)$. For non-dependent concatenation of semantic kinding contexts $\mathscr{D}_1$ and $\mathscr{D}_2$, we introduce the notation $(\mathscr{D}_1, \mathscr{D}_2)$ defined as $\Sigma_{\mathscr{D}_1}(\mathsf{W}_{\mathscr{D}_1}\mathscr{D}_2)$. As a derived rule we have

$$\frac{\mathscr{D}_1 \in \mathsf{KICXT}|\Delta_1| \qquad \mathscr{D}_2 \in \mathsf{KICXT}|\Delta_2|}{(\mathscr{D}_1, \mathscr{D}_2) \in \mathsf{KICXT}|\Delta_1, \Delta_2|}.$$

Note that $\mathscr{D}_1$ and $\mathscr{D}_2$ necessarily have disjoint domain when this rule applies.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

Remark 14 (*Polarity application*)
For $\pi \neq \top$, we can define polarity application $\boxed{\pi\mathscr{D}}$ pointwise by induction on $\mathscr{D} \in \mathsf{KICXT}$:

$$\begin{array}{lcl} \pi(\cdot) & = & \cdot \\ \pi(X{:}\pi'\mathscr{K}) & = & (X{:}(\pi\pi')\mathscr{K}) \\ \pi(\Sigma_{\mathscr{D}}\mathscr{D}') & = & \Sigma_{(\pi\mathscr{D})}(\pi\mathscr{D}'). \end{array}$$

To show well-definedness in case of pairing,

$$\frac{\mathscr{D} \in \mathsf{KICXT}(|\Delta|) \qquad \mathscr{D}' \in \circ^{-1}\mathscr{D} \to \mathsf{KICXT}(|\Delta'|)}{\Sigma_{\mathscr{D}}\mathscr{D}' \in \mathsf{KICXT}(|\Delta, \Delta'|)},$$

we have as second induction hypothesis $\pi\mathscr{D}' \in \circ^{-1}\mathscr{D} \to \mathsf{KICXT}$ but need $\pi\mathscr{D}' \in \circ^{-1}\pi\mathscr{D} \to \mathsf{KICXT}$. This follows as $\rho \leqslant \rho' \in \circ^{-1}\pi\mathscr{D}$ entails $\rho \leqslant \rho' \in \circ^{-1}\mathscr{D}$ for $\pi \neq \top$. In general, $\circ^{-1}\pi\pi' \leqslant \circ^{-1}\pi'$ for $\pi \neq \top$ (remember that $\circ^{-1}\pi' = \top$ except for $\pi' = \circ$, then $\circ^{-1}\circ = \circ$. In case of $\pi = \top$, we have the counterexample $\pi' = \circ$, as $\circ^{-1}\top\circ = \top \not\leqslant \circ^{-1}\circ = \circ$. More concretely, while $\Delta = (i{:}\circ(\leqslant\infty), X{:}(< i) \to (< i))$ is well-formed and its associated environment ordering $(\alpha/i, \mathscr{F}/X) \leqslant (\alpha'/i, \mathscr{F}'/X) \iff \alpha = \alpha'$ and $\mathscr{F} \leqslant \mathscr{F}' \in (< \alpha) \to (< \alpha)$ is meaningful, $\top\Delta = (i{:}\top(\leqslant\infty), X{:}\top((< i) \to (< i)))$ is not well-formed.

4.6.3 *Interpretation of sizes, measures, kinds and kinding contexts*

In the following, let $\rho \in [\![|\Delta_0|]\!]$ for some erased kinding context $|\Delta_0|$. (Extended) sizes a^+ are interpreted as ordinals $[\![a^+]\!]_\rho \in \mathsf{O}$ and measures $\mathfrak{m}$ as ordinal tuples $[\![\mathfrak{m}]\!]_\rho \in \mathsf{O}^*$.

$$\begin{array}{rcl} [\![i + n]\!]_\rho & = & [\![i]\!]_\rho + n \\ [\![\infty + n]\!]_\rho & = & \infty + n \\ [\![n]\!]_\rho & = & n \\ [\![a^+, \mathfrak{m}]\!]_\rho & = & ([\![a^+]\!]_\rho, [\![\mathfrak{m}]\!]_\rho). \end{array}$$

Kinds κ are interpreted as semantic kinds $[\![\kappa]\!]_\rho \in \mathsf{KI}(|\kappa|)$ and kinding contexts Δ as semantic kinding contexts $[\![\Delta]\!]_\rho \in \mathsf{KICXT}(|\Delta|)$.

$$\begin{array}{rcll} [\![*]\!]_\rho & = & \mathsf{CR} & \\ [\![<b]\!]_\rho & = & <[\![b]\!]_\rho & \\ [\![\pi\kappa \to \kappa']\!]_\rho & = & [\![\kappa]\!]_\rho \overset{\pi}{\to} [\![\kappa']\!]_\rho & \\ [\![\cdot]\!]_\rho & = & \cdot & \\ [\![\Delta, X{:}\pi\kappa]\!]_\rho & = & \Sigma_{\mathscr{D}}(X{:}\pi\mathscr{K}), & \text{where} \\ \mathscr{D} & = & [\![\Delta]\!]_\rho & \\ \mathscr{K}(\rho' \in \mathscr{D}) & = & [\![\kappa]\!]_{(\rho,\rho')}. & \end{array}$$

The structurally recursive interpretation $[\![O]\!]_\rho$ for a kind-level object $O ::= a^+ \mid \mathfrak{m} \mid \kappa$ as given above is well-defined if $\rho(i) \in \mathsf{O}$, for all $i \in \mathsf{FV}(O)$. In the following, we show that the interpretations fit into the appropriate semantic concepts.

Lemma 15 (*Soundness of size (context) formation*)
Let $\vdash \Psi$.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

1. Then, $[\![\Psi]\!] \in \mathsf{SICXT}(|\Psi|)$.
2. If $\Psi \vdash a$, then $[\![a]\!] \in [\![\Psi]\!] \xrightarrow{+} \mathsf{O}$.
3. If $\Psi \vdash i < a$ and $\rho \leqslant \rho' \in [\![\Psi]\!]$, then $[\![a]\!]_\rho \leqslant [\![a]\!]_{\rho'} \in \mathsf{O}$ and $\rho(i) \leqslant \rho'(i) < [\![a]\!]_\rho$.

Proof

By induction on the length of context Ψ. We demonstrate the case for context extension.

$$\frac{\vdash \Psi \qquad \circ^{-1}\Psi \vdash a}{\vdash \Psi, i{:}\pi(<a)}.$$

By induction hyp. 1, $\mathscr{D} := [\![\Psi]\!] \in \mathsf{SICXT}(|\Psi|)$. By induction hyp. 2, $[\![a]\!] \in [\![\circ^{-1}\Psi]\!] \to \mathsf{O}$, thus $[\![a]\!] \in \circ^{-1}\mathscr{D} \to \mathsf{O}$, entailing respect, and $\Sigma_{\mathscr{D}}(i{:}\pi(<[\![a]\!])) \in \mathsf{SICXT}(|\Psi|, i{:}o)$. □

Theorem 16 (*Soundness of kind-level judgments*)

Let $\vdash \Psi$ and let $\rho \leqslant \rho' \in \mathscr{D} := [\![\Psi]\!]$.

1. If $\Psi \vdash a^+$, then $[\![a^+]\!]_\rho \leqslant [\![a^+]\!]_{\rho'} \in \mathsf{O}$.
2. If $\Psi \vdash a^+ \leqslant b^+$, then $[\![a^+]\!]_\rho \leqslant [\![b^+]\!]_{\rho'} \in \mathsf{O}$.
3. If $\Psi \vdash a^+ < b^+$, then $[\![a^+]\!]_\rho < [\![b^+]\!]_{\rho'} \in \mathsf{O}$.
4. If $\Psi \vdash_m \mathfrak{m}$, then $[\![\mathfrak{m}]\!]_\rho \leqslant [\![\mathfrak{m}]\!]_{\rho'} \in \mathsf{O}^m$.
5. If $\Psi \vdash \mathfrak{m} \leqslant \mathfrak{m}'$, then $[\![\mathfrak{m}]\!]_\rho \leqslant [\![\mathfrak{m}']\!]_{\rho'} \in \mathsf{O}^*$.
6. If $\Psi \vdash \mathfrak{m} < \mathfrak{m}'$, then $[\![\mathfrak{m}]\!]_\rho < [\![\mathfrak{m}']\!]_{\rho'} \in \mathsf{O}^*$.
7. If $\Psi \vdash \kappa$, then $[\![\kappa]\!]_\rho \subseteq [\![\kappa]\!]_{\rho'} \in \mathsf{KI}(|\kappa|)$.
8. If $\Psi \vdash \kappa \leqslant \kappa'$, then $|\kappa| = |\kappa'|$ and $[\![\kappa]\!]_\rho \subseteq [\![\kappa']\!]_{\rho'} \in \mathsf{KI}(|\kappa|)$.

Proof

Each by induction on the derivation. □

Model-theoretic strong normalization proofs, such as the one we are studying in this paper, require *context consistency* or *context satisfiability* in the following sense: Since the typing judgment $\Delta; \Gamma \vdash t \leftleftarrows C$ is interpreted as the logical formula (see Theorem 35)

$$\text{for all } \rho \in [\![\Delta]\!] \text{ and } \sigma \in [\![\Gamma]\!]_\rho \text{ and } \tau \text{ have } t\sigma\tau \in [\![C]\!]_\rho,$$

we need at least one of ρ, σ and τ each to get a statement about t. By **CR3** for σ and trivially for τ, one can always choose the identity substitution, giving the statement $t \in [\![C]\!]_\rho$ which implies strong normalization of t by **CR1**. It remains to provide a semantic type substitution $\rho \in [\![\Delta]\!]$, and in the following theorem, we show that this is always possible. Note that this would not necessarily be the case if we allowed finitely bounded size variables $i < n$ in kinding contexts, e. g., context $i < 0$ has no instance.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

Theorem 17 (*Context satisfaction*)
If $\vdash \Delta$, then there is some $\rho_0 \in [\![\Delta]\!]$.

Proof
We prove the following stronger theorem by induction on Δ: For each $\alpha < \infty$, there is some $\rho \in [\![\Delta]\!]$ such that $\rho(i) \geqslant \alpha$ for each size variable i declared in Δ.

Case

$$\frac{\vdash \Delta \qquad \circ^{-1}\Delta \vdash <(\infty + n)}{\vdash \Delta,\ i : \pi(<(\infty + n))}.$$

By induction hypothesis, there is some $\rho \in [\![\Delta]\!]$, thus, $\rho[i \mapsto \alpha]$ is the desired environment.

Case

$$\frac{\vdash \Delta \qquad \circ^{-1}\Delta \vdash <(j + n)}{\vdash \Delta,\ i : \pi(<(j + n))}.$$

By induction hypothesis, there is some $\rho \in [\![\Delta]\!]$ with $\rho(j) \geqslant \alpha + 1$, thus, $\alpha < \rho(j) + n$ and $\rho[i \mapsto \alpha]$ is the desired environment.

Case

$$\frac{\vdash \Delta \qquad \circ^{-1}\Delta \vdash \kappa}{\vdash \Delta, X : \pi\kappa}\ \kappa \neq (<a).$$

Return $\rho[X \mapsto \bot_{[\![\kappa]\!]\rho}]$, where ρ is obtained by induction hypothesis. □

Theorem 18 (*Conditional context satisfaction*)

1. If $\Psi \vdash \exists \Psi'$ and $\rho \in [\![\Psi]\!]$, then there is some $\rho' \in [\![\Psi']\!]_\rho$.
2. If $\Delta \vdash \exists \Delta'$ and $\rho \in [\![\Delta]\!]$, then there is some $\rho' \in [\![\Delta']\!]_\rho$.

4.7 Type constructors

In order to interpret type constructors semantically, we need to restrict to well-kinded ones. However, we do not wish to define the semantics of a type constructor by recursion on its kinding derivation. After all, since we have subkinding, the kinding derivation is not unique. This dilemma can be solved by interpreting all type constructors which have a *simple kind*. Using simple kind annotations in type function $\lambda X{:}\iota.\, F$, we obtain a deterministic simple kinding judgment $\boxed{|\Delta| \vdash F : \iota}$. By induction on this judgment, whose derivation is in one-to-one correspondence with F, we can then define type (constructor) interpretation $[\![F]\!]_\rho \in [\![\iota]\!]$, for $\rho \in [\![|\Delta|]\!]$.

Simple kinding is standard, we only present some of the rules to convey the idea. Here, $|\Delta|$ shall denote a simple kinding context.

$$\frac{}{|\Delta| \vdash \forall_\kappa : (|\kappa| \to *) \to *} \qquad \frac{}{|\Delta| \vdash X : |\Delta|(X)}$$

$$\frac{|\Delta|, X{:}\iota \vdash F : \iota'}{|\Delta| \vdash \lambda X{:}\iota.\, F : \iota \to \iota'} \qquad \frac{|\Delta| \vdash F : \iota \to \iota' \qquad |\Delta| \vdash G : \iota}{|\Delta| \vdash F\ G : \iota'}.$$

Simple kinding is unique, so we have a partial computable function taking a simple kinding context $|\Delta|$ and a type constructor F and computing its simple kind ι, if

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

Type (constructor) interpretation, using the semantic type constructors given on page 34.

$$
\begin{array}{lcl}
[\![\ X\ ]\!]_\rho & = & \rho(X) \\
[\![\ \lambda X{:}\iota.F\ ]\!]_\rho(\mathscr{G} \in [\![\iota]\!]) & = & [\![F]\!]_{\rho[X\mapsto\mathscr{G}]} \\
[\![\ F\,G\ ]\!]_\rho & = & [\![F]\!]_\rho([\![G]\!]_\rho) \\
[\![\ 1\ ]\!]_\rho & = & \mathbf{1} \\
[\![\ \times\ ]\!]_\rho(\mathscr{A},\mathscr{B}) & = & \mathscr{A} \times \mathscr{B} \\
[\![\ \to\ ]\!]_\rho(\mathscr{A},\mathscr{B}) & = & \mathscr{A} \to \mathscr{B} \\
[\![\ \forall_\kappa\ ]\!]_\rho(\mathscr{F} \in [\![|\kappa|]\!] \to \mathsf{CR}) & = & \forall_{[\![\kappa]\!]_\rho}\mathscr{F} \\
[\![\ \exists_\kappa\ ]\!]_\rho(\mathscr{F} \in [\![\kappa|]\!] \to \mathsf{CR}) & = & \exists_{[\![\kappa]\!]_\rho}\mathscr{F} \\
[\![\ \mu^a S\ ]\!]_\rho & = & \boldsymbol{\mu}^{[a]_\rho}[\![S]\!]_\rho \\
[\![\ \nu^a R\ ]\!]_\rho & = & \boldsymbol{\nu}^{[a]_\rho}[\![R]\!]_\rho \\
([\![S]\!]_\rho)_c & = & [\![S_c]\!]_\rho \\
([\![R]\!]_\rho)_d & = & [\![R_d]\!]_\rho
\end{array}
$$

Fig. 17. Type interpretation $[\![F]\!]_\rho$.

it exists. We extend simple kinding to type substitutions by letting $|\Delta| \vdash \tau : |\Delta|'$ iff $|\Delta| \vdash \tau(X) : \iota$, for all $(X{:}\iota) \in |\Delta|'$.

Now given a derivation $J :: |\Delta| \vdash F : \iota$ and an environment $\rho \in [\![|\Delta|]\!]$, we define the type interpretation $[\![J]\!]_\rho \in [\![|\iota|]\!]$ by recursion on J (see Figure 17). Since J is completely determined by F and $|\Delta|$, we simply write $[\![F]\!]_\rho$, hiding $|\Delta|$ as it is implicit in the typing of ρ. Note the necessity of kind annotations of $\lambda X{:}\iota.F$ and $\forall_\kappa$ and $\exists_\kappa$ to define the corresponding set-theoretic functions.

The interpretation of F depends only on the value of ρ for the free variables of F:

Lemma 19 (*Well-definedness*)
Let $\vec{X} = \mathsf{FV}(F)$. If $|\Delta| \vdash F : \iota$, then $(|\Delta| \restriction \vec{X}) \vdash F : \iota$. If $\rho \in [\![|\Delta|]\!]$ and $(\rho' \restriction \vec{X}) = (\rho \restriction \vec{X})$, then $[\![F]\!]_\rho = [\![F]\!]_{\rho'}$.

Theorem 20 (*Soundness of type-level judgments*)
Let $\vdash \Delta$ and $\mathscr{D} := [\![\Delta]\!]$ and $\rho \leqslant \rho' \in \mathscr{D}$.

1. If $\Delta \vdash F \rightrightarrows \kappa$ or $\Delta \vdash F \leftleftarrows \kappa$, then $|\Delta| \vdash F : |\kappa|$ and $[\![F]\!]_\rho \leqslant [\![F]\!]_{\rho'} \in [\![\kappa]\!]_\rho$.
2. If $\Delta \vdash F \leqslant^\pi F' \rightrightarrows \kappa$ or $\Delta \vdash F \leqslant^\pi F' \leftleftarrows \kappa$, then $|\Delta| \vdash F, F' : |\kappa|$ and $[\![F]\!]_\rho \leqslant^\pi [\![F']\!]_{\rho'} \in [\![\kappa]\!]_\rho$.

Proof
By induction on the kinding or subtyping derivation. □

Lemma 21 (*Soundness of normalizing substitution and application*)
Let $|\Delta| \vdash G : \iota_1$.

1. If $|\Delta|, X{:}\iota_1 \vdash F : \iota_2$, then $[\![[G/X]^{\iota_1}F]\!]_\rho = [\![F]\!]_{\rho[X\mapsto[\![G]\!]_\rho]}$.
2. If $|\Delta| \vdash F : \iota_1 \to \iota_2$, then $[\![F\ @^{\iota_1}\ G]\!]_\rho = [\![F]\!]_\rho([\![G]\!]_\rho)$.

Lemma 22 (*Soundness of substitution*)
If $|\Delta'| \vdash F : \iota$ and $|\Delta| \vdash \tau : |\Delta'|$, then $[\![F\tau]\!]_\rho = [\![F]\!]_{[\![\tau]\!]_\rho}$.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

The interpretation can be extended to constrained types $^{?}A$ by adding the case:

$$[\![\mathfrak{m}{<}\mathfrak{m}' \Rightarrow A]\!]_\rho \quad = \quad [\![\mathfrak{m}]\!]_\rho{<}[\![\mathfrak{m}']\!]_\rho \Rightarrow [\![A]\!]_\rho.$$

4.8 Patterns, copatterns, λ-abstractions

In this section, we explain patterns and copatterns by developing semantic notions of pattern and pattern spine typing. These provide us with semantic conditions when a definition $\lambda\vec{D}$ inhabits a semantic type $\mathscr{A}$. As a consequence, we can prove soundness of syntactic pattern, pattern spine and expression typing.

4.8.1 Semantic typing

We want to isolate conditions under which objects $\lambda\vec{D}$ are member or a semantic type $\mathscr{A} \in \mathsf{CR}$. Let us recapitulate the proof for lambda calculus:

Lemma 23 (*Lambda abstraction*)
The following implication, written as a rule, holds for $\mathscr{A}, \mathscr{B} \in \mathsf{CR}$.

$$\frac{\forall s \in \mathscr{A}.\, t[s/x] \in \mathscr{B}}{\lambda x.t \in \mathscr{A} \to \mathscr{B}}.$$

Proof
First note that $t \in \mathscr{B}$ because $x \in \mathscr{A}$ (by **CR3**), so $t \in \mathsf{SN}$ (by **CR1**). By definition of $\mathscr{A} \to \mathscr{B}$, it is sufficient to show $(\lambda x.t)\, s \in \mathscr{B}$ for arbitrary $s \in \mathscr{A}$. Since $(\lambda x.t)\, s$ is neutral, by **CR3** we only need to show that each of its reducts r is in $\mathscr{B}$. By induction on $t \in \mathsf{SN}$ and $s \in \mathsf{SN}$, we prove that $t[s/x] \in \mathscr{B}$ implies $((\lambda x.t)\, s \longrightarrow \_) \subseteq \mathscr{B}$. The possible reducts are:

Case $r = (\lambda x.t')\, s$, where $t \longrightarrow t'$: Since $t[s/x] \longrightarrow t'[s/x]$ and $\mathscr{B}$ is closed under reduction (**CR2**), we can apply the induction hypothesis on $t' \in \mathsf{SN}$, yielding $((\lambda x.t')\, s \longrightarrow \_) \subseteq \mathscr{B}$. By neutrality and **CR3**, we conclude $(\lambda x.t')\, s \in \mathscr{B}$.
Case $r = (\lambda x.t)\, s'$, where $s \longrightarrow s'$: Analogously by induction hypothesis on $s' \in \mathsf{SN}$ using $t[s/x] \longrightarrow^* t[s'/x] \in \mathscr{B}$.
Case $r = t[s/x]$: By assumption. □

This proof illustrates how Girard-neutrality is used to introduce functions in the semantics, the interplay of the conditions on reducibility candidates **CR1-3**, and the typical local induction on strong normalization. *Partially applied* functions cannot be introduced with **CR3**, but with our extension **CR4**. We demonstrate this for a simple example, to give some intuition for the general case (Lemma 32).

Lemma 24 (*Partial application*)
Let $s, t \in \mathsf{SN}$ and $\mathscr{C} \in \mathsf{CR}$. If $u' := \lambda y.t[s/x] \in \mathscr{C}$, then $u := \lambda\{x\, y \mapsto t\}s \in \mathscr{C}$.

Proof
Note that $u \rhd u'$ since $u\, s'$ and $u'\, s'$ contract to the same term $t[s/x][s'/y]$ for any term s'. By **CR4**, it is sufficient to show that the reducts r of u are already in $\mathscr{C}$. We show that $\lambda y.t[s/x] \in \mathscr{C}$ implies $(\lambda\{x\, y \mapsto t\}s \longrightarrow \_) \subseteq \mathscr{C}$ by induction on $s, t \in \mathsf{SN}$. A

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

reduct of u is necessarily of the form $r := \lambda\{x\, y \mapsto t'\}s'$, where $(t,s) \longrightarrow (t',s')$. Note that $\lambda y.t[s/x] \longrightarrow^* \lambda y.t'[s'/x] =: r' \in \mathscr{C}$ and $r \rhd r'$, so we can apply the induction hypothesis to get $(r \longrightarrow \_) \subseteq \mathscr{C}$. By **CR4**, $r \in \mathscr{C}$. □

4.8.2 Semantic typing contexts

A semantic typing context $\mathscr{E} \in \mathsf{CXT}(\cdot)$ (letter $\mathscr{E}$ for typing *environment*) is a finite map from term variables to semantic types, so $\mathscr{E} \in \mathsf{Var} \rightharpoonup \mathsf{CR}$. In the end, semantic typing contexts $\mathscr{E}$ will be obtained as interpretation of syntactic typing contexts Γ, but our semantics is developed independently from syntactic typing. We write $\cdot$ for the empty semantic typing context, $x{:}\mathscr{A}$ for the singleton and $\mathscr{E},\mathscr{E}'$ for the disjoint union. *Semantic substitution typing* $\sigma \in \mathscr{E}$ is defined as $\sigma(x) \in \mathscr{E}(x)$ for all $x \in \mathsf{dom}(\mathscr{E})$.

A parameterized semantic typing context $\mathscr{E} \in \mathsf{CXT}(\mathscr{D})$ is a family $\mathscr{E}(\rho)$ of semantic typing contexts indexed by semantic type substitutions ρ that belong to a semantic kinding context $\mathscr{D}$. Each instance $\mathscr{E}(\rho)$ is a partial function from variables to semantic types. As context domains are not dependent, we require that $\mathsf{dom}(\mathscr{E}(\rho))$ is the same for any ρ. Thus, unless $\mathscr{D}$ is empty, the domain $\mathsf{dom}(\mathscr{E})$ of a parametrized context $\mathscr{E} \in \mathsf{CXT}(\mathscr{D})$ is well-defined. We overload the notation for non-parameterized semantic typing contexts by setting $\cdot(\rho) = \cdot$ and $(x{:}\mathscr{A})(\rho) = x{:}\mathscr{A}(\rho)$ and $(\mathscr{E},\mathscr{E}')(\rho) = \mathscr{E}(\rho),\mathscr{E}'(\rho)$ with $\mathsf{dom}(\mathscr{E}(\rho)) \cap \mathsf{dom}(\mathscr{E}'(\rho)) = \emptyset$.

For two differently parameterized semantic typing contexts $\mathscr{E}_1 \in \mathsf{CXT}(\mathscr{D}_1)$ and $\mathscr{E}_2 \in \mathsf{CXT}(\mathscr{D}_2)$, we let their disjoint union $\mathscr{E}_1 * \mathscr{E}_2 \in \mathsf{CXT}(\mathscr{D}_1,\mathscr{D}_2)$ be defined by $(\mathscr{E}_1 * \mathscr{E}_2)(\rho_1 \in \mathscr{D}_1, \rho_2 \in \mathscr{D}_2) = (\mathscr{E}_1(\rho_1),\mathscr{E}_2(\rho_2))$. Further, if $\mathscr{E} \in \mathsf{CXT}(\Sigma_{\mathscr{D}}\mathscr{D}')$ and $\rho \in \mathscr{D}$ we let the partial application $\mathscr{E}(\rho,\_) \in \mathsf{CXT}(\mathscr{D}'(\rho))$ be defined by $\mathscr{E}(\rho,\_)(\rho') = \mathscr{E}(\rho,\rho')$.

If $\mathscr{C}(\mathscr{G})(\rho)$ is a type parameterized by another type $\mathscr{G}$ and a type substitution ρ, we let $\mathscr{C}X$ be defined by $(\mathscr{C}X)(\rho) = \mathscr{C}(\rho(X))(\rho \setminus X)$. In particular, $(\mathscr{C}X)(\mathscr{G}/X,\rho) = \mathscr{C}(\mathscr{G})(\rho)$, thus, $\mathscr{C}X$ is an uncurried version of $\mathscr{C}$. The notations $\mathscr{D}X$ and $\mathscr{E}X$ are defined analogously.

Given a parameterized semantic type $\mathscr{C} \in \mathscr{D}' \to \mathsf{CR}$, we define weakening $\mathsf{W}_{\mathscr{D}}\mathscr{C} \in (\mathscr{D},\mathscr{D}') \to \mathsf{CR}$ of $\mathscr{C}$ by semantic kinding context $\mathscr{D}$ as $(\mathsf{W}_{\mathscr{D}}\mathscr{C})(\rho \in \mathscr{D}, \rho') = C(\rho')$. Given a semantic type family $\mathscr{C} \in (\mathscr{D},\mathscr{D}') \to \mathsf{CR}$ and a semantic type substitution $\rho \in \mathscr{D}$, we let the partial application $\mathscr{C}(\rho,\_) \in \mathscr{D}' \to \mathsf{CR}$ be defined by $\mathscr{C}(\rho,\_)(\rho') = \mathscr{C}(\rho,\rho')$. *Semantic typing under a context* is defined by

$$\boxed{\mathscr{D};\mathscr{E} \vdash t \in \mathscr{C}} \;:\Longleftrightarrow\; \forall \rho \in \mathscr{D}, \sigma \in \mathscr{E}(\rho), \tau.\;\; t\tau\sigma \in \mathscr{C}(\rho).$$

Note that for inconsistent kinding contexts $\mathscr{D}$, semantic kinding in context does not make any statement about t. In particular, we can only derive $t \in \mathsf{SN}$, if we have a witness $\rho \in \mathscr{D}$ of consistency. For semantic kinding context coming from well-formed syntactic kinding contexts, consistency is ensured by Theorem 17.

Lemma 25 (*Partial instantiation*)
The following implications hold:

$$\frac{\mathscr{D},\mathscr{D}';\mathscr{E} * \mathscr{E}' \vdash t \in \mathscr{C}}{\mathscr{D}';\mathscr{E}' \vdash t\tau\sigma \in \mathscr{C}(\rho,\_)}\ \rho \in \mathscr{D},\ \sigma \in \mathscr{E}(\rho) \qquad \frac{\Sigma_{X:\mathscr{K}}\mathscr{D};\mathscr{E}X \vdash t \in \mathscr{C}X}{\mathscr{D}(\mathscr{G});\mathscr{E}(\mathscr{G}) \vdash t[G/X] \in \mathscr{C}(\mathscr{G})}\ \mathscr{G} \in \mathscr{K}.$$

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

4.8.3 Semantic pattern typing

A pattern p is semantically of type $\mathscr{A}$ in context $\mathscr{E}$ if it acts as a bidirectional (meaning invertible) map from $\mathscr{E}$ to $\mathscr{A}$, i.e., $p\sigma \in \mathscr{A}$ for all $\sigma \in \mathscr{E}$, and, for any substitution σ with $p\sigma \in \mathscr{A}$, we have $\sigma \in \mathscr{E}$. Extending this to type substitutions, we define *semantic pattern typing* by

$$\boxed{\mathscr{A} \;/\; p \searrow \mathscr{D}; \mathscr{E}} \;:\Longleftrightarrow\; \forall \tau, \sigma.\ (\exists \rho \in \mathscr{D}.\ \sigma \in \mathscr{E}(\rho)) \iff p\tau\sigma \in \mathscr{A}.$$

Here, and in the following, τ denotes a syntactic type substitution. Note that it is unconstrained, it needs not bear a relationship with the semantic type substitution ρ.

One could have expected that semantic pattern typing implies that p matches any introduction term $v \in \mathscr{A}$. But since we are not interested in pattern coverage, but merely strong normalization, we do not require this strong guarantee.[8]

Lemma 26 (*Semantic pattern typing*)
The following implications, written as rules, hold.

$$\frac{}{\mathscr{A} \;/\; x \searrow \cdot; (x{:}\mathscr{A})} \qquad \frac{}{\mathbf{1} \;/\; () \searrow \cdot; \cdot} \qquad \frac{\mathscr{A}_1 \;/\; p_1 \searrow \mathscr{D}_1; \mathscr{E}_1 \qquad \mathscr{A}_2 \;/\; p_2 \searrow \mathscr{D}_2; \mathscr{E}_2}{\mathscr{A}_1 \times \mathscr{A}_2 \;/\; (p_1, p_2) \searrow \mathscr{D}_1, \mathscr{D}_2; \mathscr{E}_1 * \mathscr{E}_2}$$

$$\frac{\exists_{\beta<\alpha^\uparrow} \mathscr{S}_c(\boldsymbol{\mu}^\beta \mathscr{S}) \;/\; p \searrow \mathscr{D}; \mathscr{E}}{\boldsymbol{\mu}^\alpha \mathscr{S} \;/\; c\,p \searrow \mathscr{D}; \mathscr{E}} \qquad \frac{\mathscr{F}(\mathscr{G}) \;/\; p \searrow \mathscr{D}(\mathscr{G}); \mathscr{E}(\mathscr{G}) \text{ for all } \mathscr{G} \in \mathscr{K}}{\exists_{\mathscr{K}} \mathscr{F} \;/\; {}^X p \searrow \Sigma_{X:\mathscr{K}} \mathscr{D}; \mathscr{E} X}.$$

Note that implication for pair patterns (p_1, p_2) relies on the linearity of patterns (at least for their type variables), which is implicitly expressed by the disjointness of $\mathscr{D}_1$ and $\mathscr{D}_2$ and of $\mathscr{E}_1$ and $\mathscr{E}_2$. For non-linear patterns, an instantiation σ that is valid for each of p_1 and p_2, meaning there are $\rho_1 \in \mathscr{D}_1$ and $\rho_2 \in \mathscr{D}_2$ such that $\sigma \in \mathscr{E}_1(\rho_1)$ and $\sigma \in \mathscr{E}_2(\rho_2)$, might not valid for the pair (p_1, p_2), as ρ_1 and ρ_2 might differ on a type variable, thus $\rho = (\rho_1, \rho_2)$ might be invalid.

Proof
We spell out the proof for the more interesting rules.

$$\frac{\mathscr{A}_1 \;/\; p_1 \searrow \mathscr{D}_1; \mathscr{E}_1 \qquad \mathscr{A}_2 \;/\; p_2 \searrow \mathscr{D}_2; \mathscr{E}_2}{\mathscr{A}_1 \times \mathscr{A}_2 \;/\; (p_1, p_2) \searrow \mathscr{D}_1, \mathscr{D}_2; \mathscr{E}_1 * \mathscr{E}_2}.$$

We assume $(p_1, p_2)\tau\sigma \in \mathscr{A}_1 \times \mathscr{A}_2$ and find some $\rho \in (\mathscr{D}_1, \mathscr{D}_2)$ with $\sigma \in (\mathscr{E}_1 * \mathscr{E}_2)(\rho)$. The opposite direction is easy. As $p_1\tau\sigma \in \mathscr{A}_1$ and $p_2\tau\sigma \in \mathscr{A}_2$, we can apply the hypotheses to obtain $\rho_1 \in \mathscr{D}_1$ with $\sigma \in \mathscr{E}_1(\rho_1)$ and $\rho_2 \in \mathscr{D}_2$ with $\sigma \in \mathscr{E}_2(\rho_2)$. Since $\mathscr{D}_1$ and $\mathscr{D}_2$ have disjoint domain, $\rho := (\rho_1, \rho_2) \in (\mathscr{D}_1, \mathscr{D}_2)$. Finally, $\sigma \in (\mathscr{E}_1 * \mathscr{E}_2)(\rho) = (\mathscr{E}_1(\rho_1), \mathscr{E}_2(\rho_2))$.

$$\frac{\exists_{\beta<\alpha^\uparrow} \mathscr{S}_c(\boldsymbol{\mu}^\beta \mathscr{S}) \;/\; p \searrow \mathscr{D}; \mathscr{E}}{\boldsymbol{\mu}^\alpha \mathscr{S} \;/\; c\,p \searrow \mathscr{D}; \mathscr{E}}.$$

For $\boldsymbol{\mu}^\alpha \mathscr{S} \;/\; c\,p \searrow \mathscr{D}; \mathscr{E}$, assume $(c\,p)\tau\sigma \in \boldsymbol{\mu}^\alpha \mathscr{S}$ and derive $\sigma \in \mathscr{E}(\rho)$ for some $\rho \in \mathscr{D}$. Note that $\boldsymbol{\mu}^\alpha \mathscr{S} = \boldsymbol{\mu}^{\alpha^\uparrow} \mathscr{S}$, thus, by definition, $p\tau\sigma \in \exists_{\beta<\alpha^\uparrow} \mathscr{S}_c(\boldsymbol{\mu}^\beta \mathscr{S})$. Using

[8] On the contrary, we can live with junk introductions in our semantic types. For instance, it would not endanger normalization to throw the empty tuple into each semantic type.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

the assumption $\exists_{\beta<\alpha\uparrow}\mathscr{S}_c(\boldsymbol{\mu}^\beta\mathscr{S})\ /\ p \searrow \mathscr{D};\mathscr{E}$, we conclude $\sigma \in \mathscr{E}(\rho)$ for some $\rho \in \mathscr{D}$. For the opposite direction, assume $\rho \in \mathscr{D}$ and $\sigma \in \mathscr{E}(\rho)$. By the hypothesis, $p\tau\sigma \in \exists_{\beta<\alpha\uparrow}\mathscr{S}_c(\boldsymbol{\mu}^\beta\mathscr{S})$, hence $(c\,p)\tau\sigma \in \boldsymbol{\mu}^\alpha\mathscr{S}$.

$$\frac{\mathscr{F}(\mathscr{G})\ /\ p \searrow \mathscr{D}(\mathscr{G});\mathscr{E}(\mathscr{G}) \text{ for all } \mathscr{G} \in \mathscr{K}}{\exists_{\mathscr{K}}\mathscr{F}\ /\ {}^X p \searrow \Sigma_{X:\mathscr{K}}\mathscr{D};\mathscr{E}X}.$$

To prove this case, assume $({}^X p)\tau\sigma \in \exists_{\mathscr{K}}\mathscr{F}$ and show $\sigma \in (\mathscr{E}X)(\mathscr{G}/X,\rho) = \mathscr{E}(\mathscr{G})(\rho)$ for some $\mathscr{G} \in \mathscr{K}$ and $\rho \in \mathscr{D}(\mathscr{G})$. Since $p\tau\sigma \in \mathscr{F}(\mathscr{G})$ for some $\mathscr{G} \in \mathscr{K}$, we can apply the hypothesis to obtain $\sigma \in \mathscr{E}(\mathscr{G})(\rho)$ for some $\rho \in \mathscr{D}(\mathscr{G})$. For the other direction, assume $\rho' \in \Sigma_{X:\mathscr{K}}\mathscr{D}$ which is necessarily of the form $\rho' = (\mathscr{G}/X,\rho)$ with $\mathscr{G} \in \mathscr{K}$ and $\rho \in \mathscr{D}(\mathscr{G})$. Further, assume $\sigma \in (\mathscr{E}X)\rho'$ and show $({}^X p)\tau\sigma \in \exists_{\mathscr{K}}\mathscr{F}$. Since $\sigma \in \mathscr{E}(\mathscr{G})(\rho)$, by hypothesis, $p\tau\sigma \in \mathscr{F}(\mathscr{G})$, yielding $({}^X p)\tau\sigma \in \exists_{\mathscr{K}}\mathscr{F}$. □

Theorem 27 (*Soundness of pattern typing*)
Let $\vdash \Delta_0$ and $\Delta_0 \vdash A$. If $\Delta;\Gamma \vdash_{\Delta_0} p \leftleftarrows A$ and $\rho_0 \in [\![\Delta_0]\!]$, then $[\![A]\!]_{\rho_0}\ /\ p \searrow [\![\Delta]\!]_{\rho_0};[\![\Gamma]\!]_{(\rho_0,-)}$.

Proof
By induction on $\Delta;\Gamma \vdash_{\Delta_0} p \leftleftarrows A$ using the inferences of Lemma 26. Note that $\vdash \Delta_0,\Delta$ and $\Delta_0,\Delta \vdash \Gamma$ hold whenever $\Delta;\Gamma \vdash_{\Delta_0} p \leftleftarrows A$ is derivable. □

Having understood patterns semantically, we demonstrate how to introduce functions matching on a single pattern into the semantic function space.

Lemma 28 (*Single pattern abstraction*)
Let $\mathscr{E} \in \mathsf{Var} \to \mathsf{CR}$ and $\mathscr{B} \in \mathsf{CR}$.

$$\frac{\mathscr{A}\ /\ p \searrow \mathscr{D};\mathscr{E} \qquad \mathscr{D};\mathscr{E} \vdash t \in \mathsf{W}_{\mathscr{D}}\mathscr{B}}{\lambda\{p \to t\} \in \mathscr{A} \to \mathscr{B}}.$$

Proof
Assume $s \in \mathscr{A}$ and show $\lambda\{p \to t\}\,s \longrightarrow r$ implies $r \in \mathscr{B}$. The interesting case is $s\ /\ p \searrow \tau;\sigma$ and $r = t\tau\sigma$. Since $s = p\tau\sigma \in \mathscr{A}$, we have $\sigma \in \mathscr{E}(\rho)$ for some $\rho \in \mathscr{D}$, hence $r \in (\mathsf{W}_{\mathscr{D}}\mathscr{B})(\rho) = \mathscr{B}$ by the second assumption. □

Example: If $\mathscr{C} \in [\![*]\!]$ and $t \in \forall_{\mathscr{X}\in[\![*]\!]}(\mathscr{X} \to \mathscr{C})$, then $\lambda\{{}^X x \mapsto t\,X\,x\} \in (\exists_{\mathscr{X}\in[\![*]\!]}\mathscr{X}) \to \mathscr{C}$.

Lemma 29 (*Case*)
Let $p_{1..n}$ be patterns (not necessarily disjoint), $\mathscr{E}_k \in \mathsf{Var} \to \mathsf{CR}$ for $k = 1..n$ and $\mathscr{B} \in \mathsf{CR}$.

$$\frac{\forall k :\ \mathscr{A}\ /\ p_k \searrow \mathscr{D}_k;\mathscr{E}_k \text{ and } \forall \rho \in \mathscr{D}_k, \sigma \in \mathscr{E}_k, \tau.\ t_k\tau\sigma \in \mathscr{B}}{\lambda\{p_1 \to t_1, \ldots, p_n \to t_n\} \in \mathscr{A} \to \mathscr{B}}.$$

Proof
By Lemma 28, $\lambda\{p_k \to t_k\} \in \mathscr{A} \to \mathscr{B}$ for all k. Since $\lambda\{\overrightarrow{p \to t}\} \rhd \overrightarrow{\lambda\{p \to t\}}$, the goal follows by Lemma 3.

Alternatively, for this special situation there is a direct proof: Assume $s \in \mathscr{A}$ and $r := \lambda\{p_1 \to t_1, \ldots, p_n \to t_n\}\,s$. Since r is neutral it is sufficient to show $r \longrightarrow r'$ implies $r' \in \mathscr{B}$. We proceed by induction on $\vec{t}, s \in \mathsf{SN}$. If s matches none of $\vec{p}$, the

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

only redexes are in $\vec{t}, s$. The interesting case is $s \;/\; p_k \searrow \tau;\sigma$ and $r' = t_k\tau\sigma$ for some (not necessarily unique) k. Since $s = p_k\tau\sigma \in \mathscr{A}$, we have $\sigma \in \mathscr{E}_k(\rho)$ for some $\rho \in \mathscr{D}_k$, hence $r' \in \mathscr{B}$ by assumption. □

Simple record expressions can be introduced into semantic record types with little technical machinery.

Lemma 30 (*Single destructor pattern*)

$$\frac{t \in \forall_{\beta<\alpha\uparrow} \mathscr{R}_d(\boldsymbol{v}^\beta \mathscr{R})}{\lambda\{.d \to t\} \in \boldsymbol{v}^\alpha \mathscr{R}}.$$

Proof
It is sufficient to show $\lambda\{.d \to t\}.d' \in \forall_{\beta<\alpha\uparrow} \mathscr{R}_{d'}(\boldsymbol{v}^\beta \mathscr{R})$ for all $d' \in \mathsf{dom}(\mathscr{R})$, by analyzing the reducts of this neutral term. If $d' \neq d$ the redex is stuck, only reductions in t are possible which are covered by $t \in \mathsf{SN}$. Otherwise, $\lambda\{.d \to t\}.d \longrightarrow t$ and we conclude by the assumption. □

Lemma 31 (*Records*)
Let $d_{1..n}$ be projections (not necessarily distinct ones).

$$\frac{\text{for all } k = 1..n: \quad t_k \in \forall_{\beta<\alpha\uparrow} \mathscr{R}_{d_k}(\boldsymbol{v}^\beta \mathscr{R})}{\lambda\{.d_1 \to t_1, \ldots, .d_n \to t_n\} \in \boldsymbol{v}^\alpha \mathscr{R}}.$$

Proof
Assume an arbitrary $d \in \mathsf{dom}(\mathscr{R})$ and let $r := \lambda\{.d_1 \to t_1, \ldots, .d_n \to t_n\}.d$. We show $r \in \forall_{\beta<\alpha\uparrow} \mathscr{R}_d(\boldsymbol{v}^\beta \mathscr{R})$ by analyzing the reducts of this neutral term. If $d \notin \vec{d}$ the redex is stuck, only reductions in $\vec{t}$ are possible which are covered by $\vec{t} \in \mathsf{SN}$. Otherwise, some t_k is a possible reduct of r and we conclude by the hypothesis for t_k. □

In the following, we work our way up to the general case of multiple clauses with multiple patterns per clause.

Let P be a proposition depending on the pattern variables and pattern type variables of a copattern spine $\vec{q}$. We define the following shorthand for the replacement of the pattern variables by expressions obtained from matching $\vec{q}$ against an elimination list $\vec{e}$:

$$\boxed{P[\vec{e}/\vec{q}\,]} \;:\Longleftrightarrow\; \exists\tau,\sigma.\;\; (\vec{e} \;/\; \vec{q} \searrow \tau;\sigma) \;\wedge\; P\tau\sigma.$$

4.8.4 Semantic pattern spines

A pattern spine $\vec{q}$ has to be understood by its purpose, to serve as the lhs of a definition. Semantically, $\vec{q}$ eliminates type $\mathscr{A}$ into $\mathscr{C}$ at contexts $\mathscr{D};\mathscr{E}$ if any definition $\lambda\{\vec{q} \to t\}$ that can be formed with $\vec{q}$ is in $\mathscr{A}$ as long as the rhs t is in $\mathscr{C}$ under contexts $\mathscr{D};\mathscr{E}$. We further generalize this to partially applied definitions $\lambda\{\vec{q}\,'\,\vec{q} \to t\}\vec{e}$, where $\vec{e}$ matches $\vec{q}\,'$. We let

$$\boxed{\mathscr{A} \mid \vec{q} \searrow \mathscr{D};\mathscr{E};\mathscr{C}} \quad :\Longleftrightarrow \quad \forall t, \vec{e} \in \mathsf{SN}.\forall \vec{q}\,'.$$
$$\mathscr{D};\mathscr{E} \vdash t[\vec{e}/\vec{q}\,'] \in \mathscr{C} \implies \lambda\{\vec{q}\,'\vec{q} \to t\}\vec{e} \in \mathscr{A}.$$

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

For reasoning about semantic pattern spines, we will expand the definition of pattern substitution so the implication becomes

$$\forall \tau, \sigma.\ (\vec{e} \mathbin{/} \vec{q}\,' \searrow \tau; \sigma) \ \wedge\ (\mathscr{D}; \mathscr{E} \vdash t\tau\sigma \in \mathscr{C}) \implies \lambda\{\vec{q}\,'\vec{q} \to t\}\vec{e} \in \mathscr{A}.$$

Lemma 32 (*Semantic clause typing*)
The following implication holds:

$$\frac{\mathscr{A} \mid \vec{q} \searrow \mathscr{D}; \mathscr{E}; \mathscr{C} \qquad \mathscr{D}; \mathscr{E} \vdash t \in \mathscr{C} \qquad \rho \in \mathscr{D}}{\lambda\{\vec{q} \to t\} \in \mathscr{A}}.$$

Proof
With $\sigma_{\mathsf{id}} \in \mathscr{E}(\rho)$, we have $t = t\sigma_{\mathsf{id}} \in \mathscr{C}(\rho) \subseteq \mathsf{SN}$. The rest follows by definition of semantic pattern spine typing with empty $\vec{e}$ and empty $\vec{q}\,'$. Note that we cannot proceed if $\mathscr{D}$ is inconsistent; if we do not have a $\rho \in \mathscr{D}$, we do not get $\sigma_{\mathsf{id}} \in \mathscr{E}(\rho)$. □

Lemma 33 (*Semantic pattern spine typing*)
The following implications hold.

$$\frac{}{\mathscr{A} \mid \cdot \searrow \cdot; \cdot; \mathscr{A}} \qquad \frac{\mathscr{A}_1 \mathbin{/} p \searrow \mathscr{D}_1; \mathscr{E}_1 \qquad \mathscr{A}_2 \mid \vec{q} \searrow \mathscr{D}_2; \mathscr{E}_2; \mathscr{C}}{\mathscr{A}_1 \to \mathscr{A}_2 \mid p\,\vec{q} \searrow \mathscr{D}_1, \mathscr{D}_2; \mathscr{E}_1 * \mathscr{E}_2; \mathsf{W}_{\mathscr{D}_1}\mathscr{C}}$$

$$\frac{\forall_{\beta<\alpha^\uparrow} \mathscr{R}_d\,(\boldsymbol{\nu}^\beta \mathscr{R}) \mid \vec{q} \searrow \mathscr{D}; \mathscr{E}; \mathscr{C}}{\boldsymbol{\nu}^\alpha \mathscr{R} \mid .d\,\vec{q} \searrow \mathscr{D}; \mathscr{E}; \mathscr{C}} \qquad \frac{\forall \mathscr{G} \in \mathscr{K}.\ \ \mathscr{F}(\mathscr{G}) \mid \vec{q} \searrow \mathscr{D}(\mathscr{G}); \mathscr{E}(\mathscr{G}); \mathscr{C}(\mathscr{G})}{\forall_{\mathscr{K}} \mathscr{F} \mid X\,\vec{q} \searrow \Sigma_{X:\mathscr{K}} \mathscr{D}; \mathscr{E}X; \mathscr{C}X}.$$

Proof
Let us consider these statements:

$$\frac{}{\mathscr{A} \mid \cdot \searrow \cdot; \cdot; \mathscr{A}}$$

Assume $t, \vec{e} \in \mathsf{SN}$ and $\vec{q}, \sigma, \tau$ such that $\vec{e} \mathbin{/} \vec{q} \searrow \sigma; \tau$ and $t\sigma\tau \in \mathscr{A}$ and show $\lambda\{\vec{q} \to t\}\vec{e} \in \mathscr{A}$. This follows by **CR3** since $\lambda\{\vec{q} \to t\}\vec{e} \longrightarrow t\sigma\tau$. Formally, an induction on $t, \vec{e} \in \mathsf{SN}$ is required (cf. proof of Lemma 23).

$$\frac{\mathscr{A}_1 \mathbin{/} p \searrow \mathscr{D}_1; \mathscr{E}_1 \qquad \mathscr{A}_2 \mid \vec{q} \searrow \mathscr{D}_2; \mathscr{E}_2; \mathscr{C}}{\mathscr{A}_1 \to \mathscr{A}_2 \mid p\,\vec{q} \searrow \mathscr{D}_1, \mathscr{D}_2; \mathscr{E}_1 * \mathscr{E}_2; \mathsf{W}_{\mathscr{D}_1}\mathscr{C}}.$$

Assume $\vec{e} \in \mathsf{SN}$ with $\vec{e} \mathbin{/} \vec{q}\,' \searrow \tau; \sigma$ and $\mathscr{D}_1, \mathscr{D}_2; \mathscr{E}_1, \mathscr{E}_2 \vdash t\tau\sigma \in \mathsf{W}_{\mathscr{D}_1}\mathscr{C}$ and show $\lambda\{\vec{q}\,'p\vec{q} \to t\}\vec{e} \in \mathscr{A}_1 \to \mathscr{A}_2$. Assume $s \in \mathscr{A}_1$.

Case $s \mathbin{/} p \searrow \tau_1; \sigma_1$. Then, $\sigma_1 \in \mathscr{E}_1(\rho_1)$ for some $\rho_1 \in \mathscr{D}_1$ by the first premise of the "rule". Since $\vec{e}s \mathbin{/} \vec{q}\,'p \searrow \tau, \tau_1; \sigma, \sigma_1$ and $(\mathsf{W}_{\mathscr{D}_1}\mathscr{C})(\rho_1) = \mathscr{C}$, we have $\mathscr{D}_2; \mathscr{E}_2 \vdash t(\tau, \tau_1)(\sigma, \sigma_1) \in \mathscr{C}$. Thus, by the second premise, $\lambda\{\vec{q}\,'p\vec{q} \to t\}\vec{e}s \in \mathscr{A}_2$.

Case s does not match p. Then, $\lambda\{\vec{q}\,'p\vec{q} \to t\}\vec{e}s \in \overline{\emptyset} \subseteq \mathscr{A}_2$ because it is terminally stuck.

$$\frac{\forall_{\beta<\alpha^\uparrow} \mathscr{R}_d\,(\boldsymbol{\nu}^\beta \mathscr{R}) \mid \vec{q} \searrow \mathscr{D}; \mathscr{E}; \mathscr{C}}{\boldsymbol{\nu}^\alpha \mathscr{R} \mid .d\,\vec{q} \searrow \mathscr{D}; \mathscr{E}; \mathscr{C}}.$$

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

Here, we proceed analogously to Lemma 30, considering all possible projections d' of record type $\boldsymbol{v}^{x}\mathscr{R}$. For $d = d'$, we use the hypothesis, otherwise, we obtain a terminally stuck term.

$$\frac{\forall \mathscr{G} \in \mathscr{K}.\ \ \mathscr{F}(\mathscr{G}) \mid \vec{q} \searrow \mathscr{D}(\mathscr{G}); \mathscr{E}(\mathscr{G}); \mathscr{C}(\mathscr{G})}{\forall_{\mathscr{K}} \mathscr{F} \mid X\, \vec{q} \searrow \Sigma_{X:\mathscr{K}} \mathscr{D}; \mathscr{E}X; \mathscr{C}X}.$$

Assume $\vec{e} \,/\, \vec{q}\,' \searrow \tau; \sigma$ and $\Sigma_{X:\mathscr{K}} \mathscr{D}; \mathscr{E}X \vdash t\tau\sigma \in \mathscr{C}X$ and show $r := \lambda\{\vec{q}\,' X \vec{q} \to t\}\vec{e} \in \forall_{\mathscr{K}} \mathscr{F}$. First, $r \in \mathsf{SN}$ since $t, \vec{e} \in \mathsf{SN}$ and r is not a redex. Now assume G and $\mathscr{G} \in \mathscr{K}$. Since $\vec{e}\, G \,/\, \vec{q}\,' X \searrow \tau, G/X; \sigma$ and $\mathscr{D}(\mathscr{G}); \mathscr{E}(\mathscr{G}) \vdash t(\tau, G/X)\sigma \in \mathscr{C}(\mathscr{G})$, we can conclude $\lambda\{\vec{q}\,' X \vec{q} \to t\}\vec{e}\, G \in \mathscr{F}(\mathscr{G})$ by the premise. □

Theorem 34 (*Soundness of pattern spine typing*)
Let $\vdash \Delta_0$ and $\Delta_0 \vdash A$.
If $\Delta; \Gamma \mid A \vdash_{\Delta_0} \vec{q} \rightrightarrows C$ and $\rho_0 \in [\![\Delta_0]\!]$, then $[\![A]\!]_{\rho_0} \mid \vec{q} \searrow [\![\Delta]\!]_{\rho_0}; [\![\Gamma]\!]_{(\rho_0,\_)}; [\![C]\!]_{(\rho_0,\_)}$.

Proof
By induction on $\Delta; \Gamma \mid A \vdash_{\Delta_0} \vec{q} \rightrightarrows C$ using Lemma 33. □

4.8.5 Semantic declaration and signature well-formedness

Having understood definitions by clauses $\lambda\vec{D}$, we can now show that any well-typed term inhabits its corresponding semantic type. For function symbols f, we simply assume it, by postulating a semantically well-formed signature Σ. We define $\boxed{\models \delta}$ and $\boxed{\models \Sigma}$ by

$$\begin{array}{lll} \models (f : A = \vec{D}) & :\Longleftrightarrow & f \in [\![A]\!] \\ \models \Sigma & :\Longleftrightarrow & \forall \delta \in \Sigma.\ \models \delta. \end{array}$$

Theorem 35 (*Soundness of expression typing*)
Assume $\models \Sigma$. Let $\vdash \Delta$ and $\Delta \vdash \Gamma$ and $\Delta \vdash C$ and $\mathscr{D} = [\![\Delta]\!]$ and $\mathscr{E}(\rho) = [\![\Gamma]\!]_{\rho}$ and $\mathscr{C}(\rho) = [\![C]\!]_{\rho}$.

1. If $\Delta; \Gamma \vdash r \rightrightarrows C$ in Σ, then $\mathscr{D}; \mathscr{E} \vdash r \in \mathscr{C}$.
2. If $\Delta; \Gamma \vdash t \leftleftarrows C$ in Σ, then $\mathscr{D}; \mathscr{E} \vdash t \in \mathscr{C}$.
3. If $\Delta; \Gamma \vdash \vec{D} \leftleftarrows C$ in Σ, then $\mathscr{D}; \mathscr{E} \vdash \lambda\vec{D} \in \mathscr{C}$.

Proof
Simultaneously by induction on the typing derivation.

Case Function symbol.

$$\frac{}{\Delta; \Gamma \vdash f \rightrightarrows \Sigma(f)}$$

Follows directly by well-formedness of the signature.

Case Type annotation.

$$\frac{\Delta \vdash A \qquad \Delta; \Gamma \vdash t \leftleftarrows A}{\Delta; \Gamma \vdash (t : A) \rightrightarrows A}$$

Assume $\rho \in \mathscr{D}$ and $\sigma \in \mathscr{E}(\rho)$ and show $(t : A)\sigma = t\sigma \in [\![A]\!]_{\rho}$ which follows by induction hypothesis.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

Case Subsumption.

$$\frac{\Delta;\Gamma \vdash r \rightrightarrows A \qquad \Delta \vdash A \leqslant C}{\Delta;\Gamma \vdash r \leftleftarrows C}$$

Follows by soundness of subtyping.

Case Definition clause.

$$\frac{\Delta';\Gamma' \mid A \vdash_\Delta \vec{q} \rightrightarrows C \qquad \Delta \vdash \exists\Delta' \qquad \Delta,\Delta';\Gamma,\Gamma' \vdash t \leftleftarrows C}{\Delta;\Gamma \vdash \{\vec{q} \to t\} \leftleftarrows A}$$

Let $\mathscr{A}(\rho) = [\![A]\!]_\rho$ and $\rho \in \mathscr{D}$ and $\sigma \in \mathscr{E}(\rho)$ and τ arbitrary and show $\lambda\{\vec{q} \to t\tau\sigma\} \in \mathscr{A}(\rho)$. We set $\mathscr{D}' = [\![\Delta']\!]_\rho$ and $\mathscr{E}'(\rho') = [\![\Gamma']\!]_{(\rho,\rho')}$ and $\mathscr{C}'(\rho') = [\![C]\!]_{(\rho,\rho')}$. By induction hypothesis $\mathscr{D}';\mathscr{E}' \vdash t\tau\sigma \in \mathscr{C}'$, and by Theorem 34 $\mathscr{A}(\rho) \mid \vec{q} \searrow \mathscr{D}';\mathscr{E}';\mathscr{C}'$ entailing $\lambda\{\vec{q} \to t\tau\sigma\} \in \mathscr{A}(\rho)$ by Lemma 32. The lemma can be applied since $\Delta \vdash \exists\Delta'$ guarantees that for each $\rho \in \mathscr{D}$ there is some $\rho' \in \mathscr{D}'(\rho)$.

What remains to be proven is that well-typed programs yield, after measure erasure, semantically well-formed signatures. This is shown mutual block by mutual block using a lexicographic induction on ordinals as given by the termination measure assigned to each block. A formal description of program typing and its soundness proof is given in the next section.

5 Program typing and soundness

In Section 4, we have constructed semantic expression and pattern typing from the operational semantics and used it to verify the typing rules for expressions and patterns given in Section 3. In this section, we treat recursion, which is actually the reason we have set up the whole size-based semantic framework. First, we present typing rules to introduce recursive functions, and then we show their soundness.

5.1 Program typing

Figure 18 presents the operations and judgments needed to type-check programs. The rules describe a type-checking process that is at the core of MiniAgda (Abel, 2010).

A *measured type* $'A$ takes the form $\forall\Psi.\ \mathfrak{m} \Rightarrow A$, where Ψ is a size context and $\mathfrak{m}$ a termination measure that can refer to the size variables bound by Ψ. A measured type is wellformed $\boxed{\vdash_m {}'A}$ if $\mathfrak{m}$ and A are wellformed in context Ψ and the arity of $\mathfrak{m}$ is m. In particular, all recursive functions defined in a mutual block should have the same measure arity m.

Measure replacement $\boxed{{}'A^{<\mathfrak{m}} = A}$ is the core concept that allows us to reduce termination checking of single or mutual functions to type checking of their function bodies. It turns a measured type given to a recursive function into a bounded type used for the recursive call(s). For instance,

$$(\forall i.\ |i| \Rightarrow \mathsf{Stream}^i\mathbb{N})^{<i} \quad = \quad \forall j.\ |j|<|i| \Rightarrow \mathsf{Stream}^j\mathbb{N},$$

renaming the bound variable i to j to avoid a name clash with the free variable i. After the termination of a block of mutually recursive functions has been established,

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

$\boxed{{}'A^{<\mathtt{m}} = A}$ Measure replacement and $\boxed{(\!|{}'A|\!) = A}$ $\boxed{(\!|{}'\delta|\!) = \delta}$ $\boxed{(\!|\vec{}'\vec{\delta}|\!) = \Sigma}$ $\boxed{(\!|\beta|\!) = \Sigma}$ deletion.

$$\begin{array}{rclrcl}(\forall\Psi.\,\mathtt{m}' \Rightarrow A)^{<\mathtt{m}} & = & \forall\Psi.\,\mathtt{m}'{<}\mathtt{m} \Rightarrow A & (\!|\vec{}'\vec{\delta}|\!) & = & \overrightarrow{(\!|{}'\delta|\!)} \\ (\!|\forall\Psi.\,\mathtt{m}' \Rightarrow A|\!) & = & \forall\Psi.A & (\!|\mathsf{mutual}_m\,\vec{}'\vec{\delta}|\!) & = & \overrightarrow{(\!|{}'\delta|\!)} \\ (\!|f : {}'A = \vec{D}|\!) & = & f : (\!|{}'A|\!) = \vec{D} & (\!|\mathsf{let}\,\delta|\!) & = & \delta\end{array}$$

$\boxed{\vdash_m {}'A}$ Measured-type well-formedness and $\boxed{\vec{}'\vec{\delta} \vdash {}'\delta}$ declaration typing.

$$\frac{\vdash \Psi \qquad \Psi \vdash A \qquad \Psi \vdash_m \mathtt{m}}{\vdash_m \forall\Psi.\,\mathtt{m} \Rightarrow A} \qquad \frac{\vdash\ \hat{\Psi}\overrightarrow{\mathsf{x}_f}\vec{D} \leftleftarrows \forall\Psi.\,\vec{A}^{<\mathtt{m}} \to A}{\overrightarrow{f : {}'A = \mathbf{D}} \vdash f : (\forall\Psi.\,\mathtt{m} \Rightarrow A) = \hat{\Psi}\vec{D}[\vec{f}/\overrightarrow{\mathsf{x}_f}]}$$

$\boxed{\vdash \beta}$ Block, $\boxed{\vdash \vec{\beta}\ \mathrm{in}\ \Sigma}$ blocks, and $\boxed{\vdash P}$ program typing.

$$\frac{\vdash_m {}'A \text{ for all } (f{:}{}'A = \vec{D}) \in \vec{}'\vec{\delta} \qquad \vec{}'\vec{\delta} \vdash {}'\delta_k \text{ for all } k}{\vdash \mathsf{mutual}_m\,\vec{}'\vec{\delta}} \qquad \frac{\vdash A \qquad \vdash \vec{D} \leftleftarrows A}{\vdash \mathsf{let}\,f{:}A = \vec{D}}$$

$$\frac{}{\vdash \cdot\ \mathrm{in}\ \Sigma} \qquad \frac{\vdash \beta\ \mathrm{in}\ \Sigma \qquad \vdash \vec{\beta}\ \mathrm{in}\ \Sigma, (\!|\beta|\!)}{\vdash \beta, \vec{\beta}\ \mathrm{in}\ \Sigma} \qquad \frac{\vdash \vec{\beta}\ \mathrm{in}\ \cdot \qquad \vdash u \rightrightarrows A\ \mathrm{in}\ (\!|\vec{\beta}|\!)}{\vdash \vec{\beta}; u}$$

Fig. 18. Program and signature typing.

the termination measures are no longer needed. Since they do not contribute to the typing of the subsequent declarations, they are discarded $\boxed{(\!|\_|\!)}$. Note that *size* information *is* often needed for checking later declaration and therefore kept.

A *block* β is either a non-recursive declaration $\mathsf{let}\,f{:}A = \vec{D}$ of a new symbol f of type A by pattern matching clauses $\vec{D}$, or a list $\mathsf{mutual}_m\,\vec{}'\vec{\delta}$ of mutually recursive function declarations $f : {}'A = \vec{D}$. A *program* P is a sequence of blocks $\vec{\beta}$ followed by a single inferable expression u, for instance, just the name of the main symbol. Program checking $\vdash P$ is rather straightforward. The blocks β are checked $\boxed{\vdash \vec{\beta}\ \mathrm{in}\ \Sigma}$ in an initially empty signature Σ of declared symbols, and each checked block is, after erasure of measures, added to the signature to check the subsequent blocks. Finally, well-formedness of u is ensured.

The interesting rule is how to type-check a mutual block $\vec{}'\vec{\delta}$ with measure annotations in the function types. First, we check well-formedness of the measured function types ${}'A$ and ensure that all measures have the same length m. Then, we check each individual declaration ${}'\delta$ in the mutual block. The form of such a declaration is

$$f : (\forall\Psi.\ \mathtt{m} \Rightarrow A) = \hat{\Psi}\vec{D}[\vec{f}/\overrightarrow{\mathsf{x}_f}].$$

This means that f should consist of a list of clauses $\hat{\Psi}\vec{D}$ that all start by abstracting over the size variables $\hat{\Psi}$ declared in size context Ψ. These are the size variables that can be used in measure $\mathtt{m}$. Further, before type-checking is completed, the recursive occurrences of the mutually defined functions $\vec{f}$ are represented as special variables $\overrightarrow{\mathsf{x}_f}$ in the clauses $\vec{D}$; after type-checking, they get substituted by the actual function symbols. This trick allows us to type-check the clauses where we give constrained types $\mathsf{x}_{f'} : \forall\Psi'.\,\mathtt{m}'{<}\mathtt{m} \Rightarrow A'$ to the mutually defined functions $f' : \forall\Psi'.\,\mathtt{m}' \Rightarrow A'$.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

Thus, we ensure that recursive-call sequences are well-founded w. r. t. the termination measure.

To illustrate this process, we recapitulate the definition of the Fibonacci stream:

$$\begin{array}{ll} \mathsf{fib} & : \forall i.\ |i| \Rightarrow \mathsf{Stream}^i\mathbb{N} \\ \mathsf{fib}\ i\ .\mathsf{head}\ j & = 0 \\ \mathsf{fib}\ i\ .\mathsf{tail}\ j\ .\mathsf{head}\ k & = 1 \\ \mathsf{fib}\ i\ .\mathsf{tail}\ j\ .\mathsf{tail}\ k & = \mathsf{zipWith}\ k\ \mathbb{N}\ \mathbb{N}\ \mathbb{N}\ (+)\ (\mathsf{fib}\,k)\ (\mathsf{fib}\,j\,.\mathsf{tail}\,k). \end{array}$$

Here, $\Psi = i{\leqslant}\infty$ and $\mathfrak{m} = |i|$ and $A = \mathsf{Stream}^i\mathbb{N}$. Further, $f = \mathsf{fib}$ and $\vec{D}$ consists of three clauses of which we spell out the last one, D_3, as

$$.\mathsf{tail}\ j\ .\mathsf{tail}\ k\ \mapsto\ \mathsf{zipWith}\ k\ \mathbb{N}\ \mathbb{N}\ \mathbb{N}\ (+)\ (\mathsf{x_{fib}}\,k)\ (\mathsf{x_{fib}}\,j\,.\mathsf{tail}\,k).$$

Checking this clause amounts to derive $\vdash\ \hat{\Psi}\mathsf{x_{fib}}D_3\ \leftleftarrows\ \forall\Psi.\ \vec{'A}^{<\mathfrak{m}} \to A$, which means checking

$$\vdash\ i\ \mathsf{x_{fib}}\ .\mathsf{tail}\ j\ .\mathsf{tail}\ k\ \mapsto\ \mathsf{zipWith}\ldots\mathsf{x_{fib}}\ldots\ \leftleftarrows\ \forall i.\ (\forall j.\ |j|{<}|i| \Rightarrow \mathsf{Stream}^j\mathbb{N}) \to \mathsf{Stream}^i\mathbb{N}.$$

After checking the lhs, this becomes

$$i{\leqslant}\infty,\ j{<}i,\ k{<}j;\ \ \mathsf{x_{fib}} : (\forall j.\ |j|{<}|i| \Rightarrow \mathsf{Stream}^j\mathbb{N})\ \vdash\ \mathsf{zipWith}\ldots\mathsf{x_{fib}}\ldots\ :\ \mathsf{Stream}^k\mathbb{N}$$

and leads to two valid instantiations $\mathsf{x_{fib}}\,j$ and $\mathsf{x_{fib}}\,k$ of the recursive call $\mathsf{x_{fib}}$.

5.2 *Soundness of program typing*

In the following, we prove program typing correct by giving a meaning to measured types and declarations. The correctness of mutually recursive definitions will follow from a lexicographic induction on ordinals.

A measured type $'A$ is not a proper type, it does not have a meaning by itself. *Bounded type interpretation* $\boxed{[\![{'A}]\!]^{<\vec{\alpha}}}$ assigns it a meaning relative to a tuple of ordinals which has the same length as the measure $\mathfrak{m}$ in $'A$.

$$[\![\forall\Psi.\,\mathfrak{m} \Rightarrow A]\!]^{<\vec{\alpha}} = \forall_{\rho\in[\![\Psi]\!]}\ ([\![\mathfrak{m}]\!]_\rho < \vec{\alpha}) \Rightarrow [\![A]\!]_\rho.$$

The bounded type interpretation $[\![{'A}]\!]^{<\vec{\alpha}}$ denotes a constrained type. It is the semantic counterpart of $'A^{<\mathfrak{m}}$, as the following lemma proves:

Lemma 36 (*Soundness of measure replacement*)
Let $'A = (\forall\Psi.\,\mathfrak{m} \Rightarrow A)$. If $\vdash_m {'A}$ and $\rho \in [\![\Psi]\!]$ then $[\![{'A}^{<\mathfrak{m}}]\!]_\rho = [\![{'A}]\!]^{<[\![\mathfrak{m}]\!]_\rho}$.

Proof
Let $\vec{\alpha} = [\![\mathfrak{m}]\!]_\rho$. Recall that $'A^{<\mathfrak{m}} = \forall\Psi'.\,\mathfrak{m}' < \mathfrak{m} \Rightarrow A'$, where Ψ' is a renaming of Ψ and $\mathfrak{m}', A'$ are the corresponding renamings of $\mathfrak{m}, A$. We thus have $[\![{'A}^{<\mathfrak{m}}]\!]_\rho = (\forall_{\rho'\in[\![\Psi']\!]}([\![\mathfrak{m}']\!]_{\rho'} < \vec{\alpha}) \Rightarrow [\![A']\!]_{\rho'}) = [\![{'A}]\!]^{<\vec{\alpha}}$. □

In the following, $\boxed{\vec{b} : \Psi}$ shall mean that $\vec{b}$ is a list of size expressions that has the same length as size context Ψ.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

Erasure of the measure in $'A$ turns a bounded quantification into an unbounded one:

Lemma 37 (*Soundness of measure erasure*)
Let m the length of the measure in measure-decorated type $'A$. Then, $[\![(\!|'A|\!)]\!] = \bigcap_{\vec{\alpha}\in \mathsf{O}^m} [\!['A]\!]^{<\vec{\alpha}}$.

Proof
For "$\subseteq$", assume $r \in [\![(\!|'A|\!)]\!] = [\![\forall \Psi. A]\!]$ and $\vec{\alpha} \in \mathsf{O}^m$ and $\rho \in [\![\Psi]\!]$ and $\vec{b} : \Psi$ and show $r\,\vec{b} \in ([\![\mathfrak{m}]\!]_\rho < \vec{\alpha}) \Rightarrow [\![A]\!]_\rho$. This follows from $r\,\vec{b} \in [\![A]\!]_\rho$, since by definition $\mathscr{A} \subseteq (P \Rightarrow \mathscr{A})$ for all $P, \mathscr{A}$.

For "$\supseteq$", assume $r \in \bigcap_{\vec{\alpha}} \forall_{\rho\in[\![\Psi]\!]}\, ([\![\mathfrak{m}]\!]_\rho < \vec{\alpha}) \Rightarrow [\![A]\!]_\rho$ and $\rho \in [\![\Psi]\!]$ and $\vec{b} : \Psi$ and show $r\,\vec{b} \in [\![A]\!]_\rho$. Choosing some $\vec{\alpha} > [\![\mathfrak{m}]\!]_\rho$ (this is always possible due to the open nature of O), we conclude by instantiation of the first assumption. □

In order to justify a block of mutually recursive functions, we perform an lexicographic induction over a tuple $\vec{\alpha}$ of ordinals. This requires us to interpret the declarations of the mutual block relative to the upper bound $\vec{\alpha}$ on the measure of the recursive calls. *Bounded semantic declaration typing* $\boxed{\vec{'\delta} \models^{\vec{\alpha}} '\delta}$ is defined by

$$\boxed{f_1 : 'A_1 = \vec{D}_1, \ldots, f_n : 'A_n = \vec{D}_n \models^{\vec{\alpha}} f : (\forall \Psi.\, \mathfrak{m} \Rightarrow A) = \vec{D}}$$

$$:\Longleftrightarrow \quad \begin{array}{ll} \text{if} & f_i \in [\!['A_i]\!]^{<\vec{\alpha}} \text{ for } i = 1..n \\ \text{and} & \rho \in [\![\Psi]\!] \text{ with } [\![\mathfrak{m}]\!]_\rho \leqslant \alpha \\ \text{and} & \vec{b} : \Psi \\ \text{then} & f\,\vec{b} \in [\![A]\!]_\rho. \end{array}$$

Corollary 38 (*Soundness of measure erasure in declarations*)
$\models (\!|'\delta|\!)$ iff $\models^{\vec{\alpha}} '\delta$ for all $\alpha \in \mathsf{O}^m$.

Lemma 39 (*Soundness of declaration typing*)
Let m be the length of the measure in block $\vec{'\delta}$ and declaration $'\delta$. If $\vec{'\delta} \vdash '\delta$, then $\vec{'\delta} \models^{\vec{\alpha}} '\delta$ for all $\vec{\alpha} \in \mathsf{O}^m$.

Proof
Declaration typing $\vec{'\delta} \vdash '\delta$ is derived by rule:

$$\frac{\vdash\ \hat{\Psi}\overrightarrow{\mathsf{x}_f}\vec{D}\ \trianglelefteq\ \forall \Psi.\, \vec{'A}^{<\mathfrak{m}} \to A}{\overrightarrow{f : 'A = \mathbf{D}} \vdash f : (\forall \Psi.\, \mathfrak{m} \Rightarrow A) = \hat{\Psi}\vec{D}[\vec{f}/\overrightarrow{\mathsf{x}_f}]}.$$

We show $\overrightarrow{f : 'A = \mathbf{D}} \models^{\vec{\alpha}} f : (\forall \Psi.\, \mathfrak{m} \Rightarrow A) = \hat{\Psi}\vec{D}[\vec{f}/\overrightarrow{\mathsf{x}_f}]$. By assumption $f_i \in [\!['A_i]\!]^{<\vec{\alpha}}$ for all i. Assume $\rho \in [\![\Psi]\!]$ with $[\![\mathfrak{m}]\!]_\rho \leqslant \vec{\alpha}$ and $\vec{b} : \Psi$, and show $f\,\vec{b} \in [\![A]\!]_\rho$. By soundness of definition typing (Thm. 35), $\lambda\hat{\Psi}\overrightarrow{\mathsf{x}_f}\vec{D} \in \forall_{\rho\in[\![\Psi]\!]}([\![\vec{'A}]\!]^{<[\![\mathfrak{m}]\!]_\rho} \to [\![A]\!]_\rho)$. Since $f_i \in [\!['A_i]\!]^{<\vec{\alpha}} \subseteq [\!['A_i]\!]^{<[\![\mathfrak{m}]\!]_\rho}$ for all i by contravariance, this implies that $(\lambda\hat{\Psi}\overrightarrow{\mathsf{x}_f}\vec{D})\,\vec{b}\,\vec{f} \in [\![A]\!]_\rho$. By the simulation $f\,\vec{b} \rhd (\lambda\hat{\Psi}\overrightarrow{\mathsf{x}_f}\vec{D})\,\vec{b}\,\vec{f}$, we have $f\,\vec{b} \in [\![A]\!]_\rho$. □

Theorem 40 (*Soundness of block typing*)
Let $\models \Sigma$. If $\vdash \beta$ in Σ, then $\models \Sigma, (\!|\beta|\!)$.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

Proof

Case let-declaration.

$$\frac{\vdash A \qquad \vdash \vec{D} \trianglelefteq A \text{ in } \Sigma}{\vdash \mathsf{let}\, f : A = \vec{D} \text{ in } \Sigma}.$$

Let $\mathscr{A} = [\![A]\!]$. We have to show $f \in \mathscr{A}$ relative to signature $\Sigma, f : A = \vec{D}$. Since $f \rhd \lambda\vec{D}$ and $\lambda\vec{D} \in \mathscr{A}$ by Theorem 35, we conclude by Lemma 3.

Case mutual block. Let n the number of mutual declarations and $'\delta_k = (f_k : 'A_k = \vec{D}_k)$ and $'A_k = \forall\Psi_k.\, \mathfrak{m}_k \Rightarrow A_k$ for $k = 1..n$. Note that $(\!|\vec{'\delta}|\!) = (f_k : \forall\Psi_k.\, A_k = \vec{D}_k)_{k=1..n}$ in this case.

$$\frac{\vdash_m 'A_k \text{ for } k = 1..n \qquad \vec{'\delta} \vdash '\delta_k \text{ in } \Sigma \text{ for } k = 1..n}{\vdash \mathsf{mutual}_m\, \vec{'\delta} \text{ in } \Sigma}.$$

By soundness of declaration typing (Lemma 39), we have $\vec{'\delta} \models^{\vec{\alpha}} '\delta_k$ for $\vec{\alpha} \in \mathsf{O}^m$ and $k = 1..n$. By lexicographic induction on $\vec{\alpha} \in \mathsf{O}^m$, this entails $\models^{\vec{\alpha}} '\delta_k$ for $k = 1..n$, using the reduction rules for $f_{1..n}$ in the extended signature $\Sigma, (\!|\vec{'\delta}|\!)$. This entails $\models (\!|'\delta_k|\!)$ by Corollary 38.

We spell out the induction in more detail. Assume $\vec{\alpha} \in \mathsf{O}^m$ and $k \in \{1..n\}$ and show $\models^{\vec{\alpha}} '\delta_k$. By induction hypothesis $\models^{\vec{\beta}} \vec{'\delta}$ for all $\vec{\beta} < \vec{\alpha}$ (lexicographic comparison). Using $\vec{'\delta} \models^{\vec{\alpha}} '\delta_k$ solves the goal, but to apply it we have to show $f_k \in [\!['A_k]\!]^{<\vec{\alpha}}$ for all k. Assume $\rho \in [\![\Psi_k]\!]$ with $[\![\mathfrak{m}_k]\!]_\rho < \vec{\alpha}$ and $\vec{b} : \Psi$ and show $f_k\, \vec{b} \in [\![A_k]\!]_\rho$. We conclude by induction hypothesis for $\vec{\beta} = [\![\mathfrak{m}_k]\!]_\rho$. □

Corollary 41 (*Soundness of program typing*)

1. If $\models \Sigma$ and $\vdash \vec{\beta}$ in Σ, then $\models \Sigma, (\!|\vec{\beta}|\!)$.
2. If $\vdash \vec{\beta}; t$, then $t \in \mathsf{SN}$ in signature $(\!|\vec{\beta}|\!)$.

6 Conclusion

Our work provides a uniform type-based approach to proving termination of (co)inductive definitions. It is centered around patterns and copatterns which allow us to reason about both finite and infinite data by well-founded induction. Proving strong normalization for this language is a significant step towards understanding well-founded corecursion in terms of the depth of observation we can safely make.

As a next step, we plan to extend our work to full dependently typed systems to allow coinductive definitions to be defined and reasoned with by observations. This will put coinduction in these systems on a robust foundation. We have already implemented size-based type checking for patterns and copatterns in MiniAgda (Abel, 2012) and Agda 2.4 which gives us confidence in the approach.

However, some challenges remain on the way to dependent types. As in dependent type theory, we can reason about programs internally, size annotations appearing in programs can get in the way of completing an argument, e. g., showing that two programs are equal which only differ in size annotations. Sacchini (2013) gives an instructive example for this phenomenon. Roughly speaking, we have to internalize the disregard (or erasure) of size (and possibly type) application, which we now do externally when constructing the model. Exactly how to do this in a sound way is unclear at the moment.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

Further, we would like to infer size applications and solve size constraints automatically. Some preliminary algorithm, which has become part of Agda 2.4, can be found in Reihl's bachelor thesis (Reihl, 2013).

Acknowledgments

Big thanks to the reviewers of a previous version of this paper who asked many insightful questions that lead to the present, reworked version. The first author thanks Andrea Vezzosi for many inspiring discussions on sized types that improved their exposition in this paper. He also acknowledges support by Vetenskapsrådet project *Termination Certificates for Dependently-Typed Programs and Proofs via Refinement Types* and a Vetenskapsrådet framework grant to the ProgLog group (Thierry Coquand *et al.*) of the Department of Computer Science and Engineering at Chalmers and Gothenburg University The second author acknowledges support by NSERC (National Science and Engineering Research Council Canada).

References

Abel, A. (2006) *A Polymorphic Lambda-Calculus with Sized Higher-Order Types* . Ph.D. thesis, Ludwig-Maximilians-Universität München.

Abel, A. (2008a) Polarized subtyping for sized types. *Math. Struct. Comput. Sci.* **18**(5), 797–822.

Abel, A. (2008b) Semi-continuous sized types and termination. *Logical Meth. Comput. Sci.* **4**(2:3), 1–33.

Abel, A. (2010) MiniAgda: Integrating sized and dependent types. In (Bove *et al.*, 2010).

Abel, A. (2012) Type-based termination, inflationary fixed-points, and mixed inductive-coinductive types. In *Proceedings of the 8th Wksh. on Fixed Points in Comp. Sci. (FICS 2012)*, Miller, D. & Ésik, Z. (eds), Electr. Proc. in Theor. Comp. Sci., vol. 77 pp. 1–11.

Abel, A., Pientka, B., Thibodeau, D. & Setzer, A. (2013) Copatterns: Programming infinite structures by observations. In *Proceedings of the 40th ACM Symp. on Principles of Programming Languages, POPL 2013*, Giacobazzi, R. & Cousot, R. (eds), ACM Press, pp. 27–38.

AgdaTeam. (2015) *The Agda Wiki.*

Altenkirch, T. & Danielsson, N. A. (2012) Termination checking in the presence of nested inductive and coinductive types. In *Wksh. on Partiality And Recursion in Interactive Theorem Provers, PAR 2010*, Bove, A., Komendantskaya, E. & Niqui, M. (eds), EPiC Series in Comput. Sci., vol. 5. EasyChair, pp. 101–106.

Amadio, R. M. & Coupet-Grimal, S. (1998) Analysis of a guard condition in type theory (extended abstract) In *Proceedings of the 1st International Conference on Foundations of Software Science and Computation Structure, FoSSaCS'98*, Nivat, M. (ed), Lect. Notes in Comput. Sci., vol. 1378. Springer, pp. 48–62.

Barthe, G., Frade, M. J., Giménez, E., Pinto, L. & Uustalu, T. (2004) Type-based termination of recursive definitions. *Math. Struct. Comput. Sci.* **14**(1), 97–141.

Barthe, G., Grégoire, B. & Pastawski, F. (2005) Practical inference for type-based termination in a polymorphic setting. In *Proceedings of the 7th International Conference on Typed Lambda Calculi and Applications, TLCA 2005*, Urzyczyn, P. (ed), Lect. Notes in Comput. Sci., vol. 3461. Springer, pp. 71–85.

Barthe, G., Grégoire, B. & Riba, C. (2008) Type-based termination with sized products. In *Computer Science Logic, 22nd Int. Wksh., CSL 2008, 17th Annual Conf. of the EACSL*,

Kaminski, M. & Martini, S. (eds), Lect. Notes in Comput. Sci., vol. 5213. Springer, pp. 493–507.

Blanqui, F. (2004) A type-based termination criterion for dependently-typed higher-order rewrite systems. In *Rewriting Techniques and Applications, RTA 2004, Aachen, Germany*, van Oostrom, V. (ed), Lect. Notes in Comput. Sci., vol. 3091. Springer, pp. 24–39.

Blanqui, F. & Riba, C. (2006) Combining typing and size constraints for checking the termination of higher-order conditional rewrite systems. In *Proceedings of the 13th Int. Conf. on Logic for Programming, Artificial Intelligence, and Reasoning, LPAR 2006*, Hermann, M. & Voronkov, A. (eds), Lect. Notes in Comput. Sci., vol. 4246. Springer, pp. 105–119.

Bove, A., Komendantskaya, E. & Niqui, M. (eds). (2010) *Wksh. on Partiality and Recursion in Interactive Theorem Provers, PAR 2010*. Electr. Proc. in Theor. Comp. Sci., vol. 43.

Coquand, T. (1994) Infinite objects in type theory. In *Types for Proofs and Programs, Int. Wksh., TYPES'93*, Barendregt, H. & Nipkow, T. (eds), Lect. Notes in Comput. Sci., vol. 806. Springer, pp. 62–78.

Danielsson, N. A. (2010) Beating the productivity checker using embedded languages. In (Bove *et al*., 2010).

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

Ghani, N., Hancock, P. & Pattinson, D. (2009) Representations of stream processors using nested fixed points. *Logical Meth. Comput. Sci.* **5**(3:9)

Giménez, E. (1996) *Un calcul de constructions infinies et son application a la vérification de systèmes communicants*. Ph.D. thesis, Ecole Normale Supérieure de Lyon.

Girard, J.-Y., Lafont, Y. & Taylor, P. (1989) *Proofs and Types*. Cambridge Tracts in Theoret. Comput. Sci., vol. 7. Cambridge University Press.

Hughes, J., Pareto, L. & Sabry, A. (1996) Proving the correctness of reactive systems using sized types. In Proceedings of the 23rd ACM Symposium on Principles of Programming Languages, POPL'96, pp. 410–423.

INRIA. (2012) *The Coq Proof Assistant Reference Manual*. Version 8.4 edn. INRIA.

Jones, G. & Gibbons, J. (1993) *Linear-Time Breadth-fFrst Tree Algorithms: An Exercise in the Arithmetic of Folds and Zips*. Technical Report, University of Auckland.

Mendler, N. P. (1987) Recursive types and type constraints in second-order lambda calculus. In Proceedings of the 2nd IEEE Symp. on Logic in Computer Science (LICS'87). IEEE Computer Soc. Press, pp. 30–36.

Oury, N. (2008) *Coinductive Types and Type Preservation*. Message on the Coq-club mailing list on 6 June 2008.

Pareto, L. (2000) *Types for Crash Prevention*. PhD Thesis, Chalmers University of Technology.

Reihl, F. (2013) *Solving Size Constraints using Graph Representation*. Bachelor's Thesis, Institut für Informatik, Ludwig-Maximilians-Universität München.

Sacchini, J. L. (2011) *On Type-Based Termination and Pattern Matching in the Calculus of Inductive Constructions*. PhD Thesis, INRIA Sophia-Antipolis and École des Mines de Paris.

Sacchini, J. L. (2013) Type-based productivity of stream definitions in the calculus of constructions. In *Proceedings of the 28th IEEE Symposium on Logic in Computer Science (LICS'13)*. IEEE Computer Soc. Press, pp. 233–242.

Sijtsma, B. A. (1989) On the productivity of recursive list definitions. *ACM Trans. Program. Lang. Syst.* **11**(4), 633–649.

Sprenger, C. & Dam, M. (2003) On the structure of inductive reasoning: Circular and tree-shaped proofs in the μ-calculus. In *Proceedings of the 6th International Conference*

on Foundations of Software Science and Computational Structures, FoSSaCS 2003, Gordon, A. D. (ed), Lect. Notes in Comput. Sci., vol. 2620. Springer, pp. 425–440.

Steffen, M. (1998) *Polarized Higher-Order Subtyping*. PhD Thesis, Technische Fakultät, Universität Erlangen.

Taylor, P. (1996) Intuitionistic sets and ordinals. *J. Symb. Logic* **61**(3), 705–744.

Vouillon, J. & Melliès, P.-A. (2004) Semantic types: A fresh look at the ideal model for types. In *Proceedings of the 31st ACM Symp. on Principles of Programming Languages, POPL 2004*. ACM Press, pp. 52–63.

Watkins, K., Cervesato, I., Pfenning, F. & Walker, D. (2003) *A Concurrent Logical Framework I: Judgements and Properties*. Technical Report. School of Computer Science, Carnegie Mellon University, Pittsburgh.

Xi, H. (2002) Dependent types for program termination verification. *J. Higher-Order and Symb. Comput.* **15**(1), 91–131.

Appendix

The appendix contains a recapitulation of syntax and notational definitions of $\mathsf{F}^{\mathsf{cop}}_{\omega}$.

$\kappa \xrightarrow{\pi} \kappa'$	for	$\pi\kappa \to \kappa'$	function kind
$\kappa \to \kappa'$	for	$\kappa \xrightarrow{\circ} \kappa'$	default variance
$\leq a$	for	$<(a+1)$	weak bound
size	for	$\leq\infty$	
λXF	for	$\lambda X{:}\iota.F$	if ι inferable
$A \times B$	for	$(\times)AB$	product type
$A \to B$	for	$(\to)AB$	function type
$\forall X{:}\kappa.A$	for	$\forall_\kappa(\lambda X{:}\lvert\kappa\rvert.A)$	universal type
$\exists X{:}\kappa.A$	for	$\exists_\kappa(\lambda X{:}\lvert\kappa\rvert.A)$	existential type
$\forall j{<}a.A$	for	$\forall_{<a}(\lambda j{:}o.A)$	bounded universal
$\exists j{<}a.A$	for	$\exists_{<a}(\lambda j{:}o.A)$	bounded existential
S_c	for	F where $(c{:}F) \in S$	type of constructor
R_d	for	F where $(d{:}F) \in R$	type of destructor
$\Delta, X{:}\kappa$	for	$\Delta, X{:}\circ\kappa$	default variance
$\Delta, i{<}a$	for	$\Delta, i{:}\circ(<a)$	default variance
$\cdot \to A$	for	A	context abstraction
$\forall\Delta, X{:}\kappa.A$	for	$\forall\Delta.\forall X{:}\kappa.A$	$\forall\Delta.A$
$\widehat{\cdot}$	for	$\cdot$	context domain
$\widehat{\Delta, X{:}\pi\kappa}$	for	$\hat{\Delta}, X$	$\hat{\Delta}$ (variable list)
$(t_1, t_2, \ldots, t_n)$	for	$(t_1, (t_2, \ldots, t_n))$	n-ary tuples
$\lambda x.t$	for	$\lambda\{x \to t\}$	lambda abstraction
$\lambda\vec{q}.t$	for	$\lambda\{\vec{q} \to t\}$	single-clause object
$\vec{q}\{\vec{q}' \to t\}$	for	$\{\vec{q}\vec{q}' \to t\}$	copattern prefix for clause
$\vec{q}\vec{D}$	for	$\{\vec{q}D_1; \ldots; \vec{q}D_n\}$	copattern prefix for clauses

Fig. 19. Notational definitions.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press

SizeVar	$\ni i, j$		size variable
SizeExp	$\ni a, b$	$::= i+n \mid \infty+n$	size expression $(n \geq 0)$
SizeExp$^+$	$\ni a^+, b^+$	$::= a \mid n$	extended size expr. $(n \geq 0)$
Measure	$\ni \mathfrak{m}$	$::= a^+ \mid a^+, \mathfrak{m}$	measure expression
Cond	$\ni \mathfrak{c}$	$::= \mathfrak{m} < \mathfrak{m}'$	condition
Pol	$\ni \pi$	$::= \circ \mid + \mid - \mid \top$	variance
SKind	$\ni \iota$	$::= * \mid o \mid \iota \to \iota'$	simple kinds
Kind	$\ni \kappa$	$::= * \mid <a \mid \pi\kappa \to \kappa'$	kinds (w/ variance)
TyVar	$\ni X, Y, Z, i, j$		type and size variables
TyAtom	$\ni K$	$::= X \mid a \mid 1 \mid \times \mid \to$	type atoms
Type	$\ni F, G, A, B, C$	$::= K \mid \lambda X{:}\iota.\, F \mid F\, G$	type-level lambda-calculus
		$\mid \forall_\kappa \mid \exists_\kappa$	quantifiers
		$\mid \mu^a S \mid \nu^a R$	variant and record types
MType	$\ni {}'A, {}'B$	$::= \forall \Psi.\, \mathfrak{m} \Rightarrow C$	type with measure
CType	$\ni {}^?A, {}^?B$	$::= \forall \Psi.\, \mathfrak{c} \Rightarrow C$	constrained type
Variant	$\ni S$	$::= \langle c_1{:}F_1; \ldots; c_n{:}F_n \rangle$	variant row $(n \geq 0)$
Record	$\ni R$	$::= \{d_1{:}F_1; \ldots; d_n{:}F_n\}$	record row $(n \geq 0)$
Cons	$\ni c$		constructor (variant label)
Proj	$\ni d$		destructor (record label)
Var	$\ni x, y, z$		term variable
Pat	$\ni p$	$::= x \mid () \mid (p_1, p_2) \mid c\, p \mid {}^X p$	pattern
Copat	$\ni q$	$::= p \mid X \mid .d$	copattern
PatSp	$\ni \mathbf{q}$	$::= \vec{q}$	pattern spine
Fun	$\ni f, g, h$		defined function symbol
Elim	$\ni e$	$::= t \mid G \mid .d$	eliminations
App	$\ni u$	$::= x \mid f \mid r\, e$	applicative expressions
Intro	$\ni v$	$::= () \mid (t_1, t_2) \mid c\, t \mid {}^G t$	introductions (checkable)
Exp	$\ni r, s, t$	$::= u \mid (t : A)$	applicative, annotated expr.s
		$\mid v \mid \lambda \vec{D}$	intros, anonymous object
DCl	$\ni D$	$::= \{\vec{q} \to t\}$	definition clause
Def	$\ni \vec{D}, \mathbf{D}$	$::= \{D_1; \ldots; D_n\}$	definition
Decl	$\ni \delta$	$::= f : A = \vec{D}$	declaration
MDecl	$\ni {}'\delta$	$::= f : {}'A = \vec{D}$	declaration with measure
Block	$\ni \beta$	$::= \mathsf{mutual}_m\ {}'\vec{\delta}$	mutual block $(m \geq 1)$
Prg	$\ni P$	$::= \vec{\beta}; t$	program
Sig	$\ni \Sigma$	$::= \vec{\delta}$	signature
SizeCxt	$\ni \Psi$	$::= \cdot \mid \Psi, i{:}\pi(<a)$	size variable context
TyCxt	$\ni \Delta$	$::= \cdot \mid \Delta, X{:}\pi\kappa$	type/size variable context
SCxt	$\ni \lvert\Delta\rvert$	$::= \cdot \mid \lvert\Delta\rvert, X{:}\iota$	simple kinding context
Cxt	$\ni \Gamma$	$::= \cdot \mid \Gamma, x{:}A \mid \Gamma, x{:}{}^?A$	term variable context

Fig. 20. Syntax.

https://doi.org/10.1017/S0956796816000022 Published online by Cambridge University Press