Linked Visualisations via Galois Dependencies

Extended paper with additional supporting material

ROLY PERERA[*], The Alan Turing Institute, UK
MINH NGUYEN, University of Bristol, UK
TOMAS PETRICEK[†], University of Kent, UK
MENG WANG, University of Bristol, UK

We present new language-based dynamic analysis techniques for linking visualisations and other structured outputs to data in a fine-grained way, allowing users to explore how data attributes and visual or other output elements are related by selecting (focusing on) substructures of interest. Our approach builds on bidirectional program slicing techiques based on Galois connections, which provide desirable round-tripping properties. Unlike the prior work, our approach allows selections to be negated, equipping the bidirectional analysis with a De Morgan dual which can be used to link different outputs generated from the same input. This offers a principled language-based foundation for a popular view coordination feature called *brushing and linking* where selections in one chart automatically select corresponding elements in another related chart.

CCS Concepts: • **Theory of computation** → **Program semantics**.

Additional Key Words and Phrases: Galois connections; data provenance

ACM Reference Format:
Roly Perera, Minh Nguyen, Tomas Petricek, and Meng Wang. 2022. Linked Visualisations via Galois Dependencies: *Extended paper with additional supporting material. Proc. ACM Program. Lang.* 6, POPL, Article 7 (January 2022), 72 pages. https://doi.org/10.1145/3498668

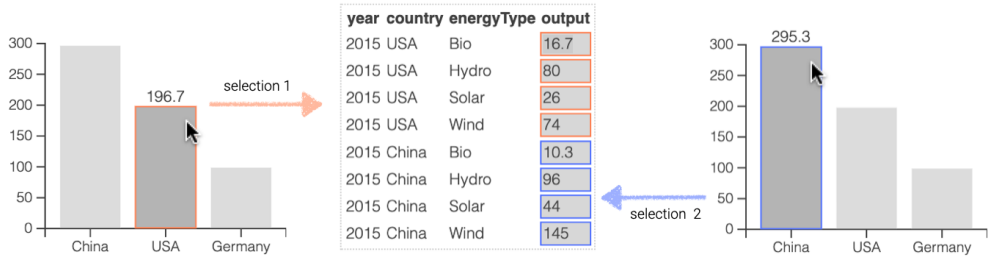
1 INTRODUCTION

Techniques for dynamic dependency analysis have been fruitful, with applications ranging from information-flow security [Sabelfeld and Myers 2003] and optimisation [Kildall 1973] to debugging and program comprehension [De Lucia et al. 1996; Weiser 1981]. There are, however, few methods suitable for fine-grained analysis of richly structured outputs, such as data visualisations and multidimensional arrays. Dataflow analyses [Reps et al. 1995] tend to focus on analysing variables rather than parts of structured values. Where-provenance [Buneman et al. 2001] and related data provenance techniques are fine-grained, but are specific to relational query languages. Taint tracking [Newsome and Song 2005] is also fine-grained, but works forwards from input to output. For many applications, it would be useful to be able to focus on a particular part of a structured output, and have an analysis isolate the input data pertinent only to that substructure.

[*]Also with University of Bristol.
[†]Also with The Alan Turing Institute.

Authors' addresses: Roly Perera, The Alan Turing Institute, London, UK, rperera@turing.ac.uk; Minh Nguyen, min.nguyen@bristol.ac.uk, University of Bristol, Bristol, UK; Tomas Petricek, University of Kent, Canterbury, UK, tpetricek@kent.ac.uk; Meng Wang, meng.wang@bristol.ac.uk, University of Bristol, Bristol, UK.

2475-1421/2022/1-ART7
https://doi.org/10.1145/3498668




```
let totalFor c rows =
   sum [ row.output | row ⟵ rows, row.country == c ];
let data2015 = [ row | row ⟵ data, row.year == 2015 ];
    countryData = [ { x: c, y: totalFor c data2015 }
                  | c ⟵ ["China", "USA", "Germany"] ]
in BarChart { caption: "Total output by country", data: countryData }
```

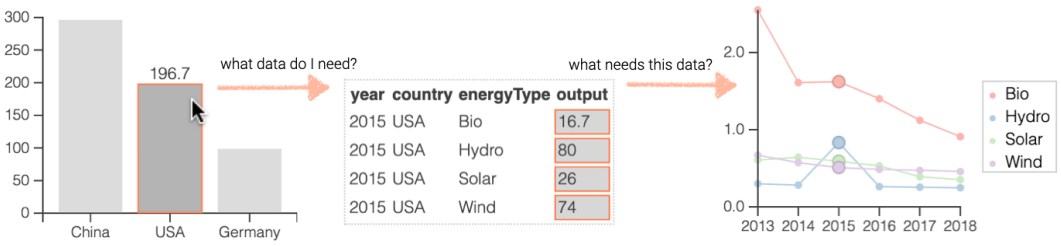
Fig. 1. Fine-grained linking of outputs to inputs, focusing on data for USA (left) and China (right).

This is a need that increasingly arises outside of traditional programming. Journalists and data scientists use programs to compute charts and other visual summaries from data, charts which must be interpreted by colleagues, policy makers and lay readers alike. Interpreting a chart correctly means understanding what the components of the visualisation actually *represent*, i.e. the mapping between data and visual elements. But this is a hard task, requiring time and expertise, even with access to the data and source code used to create the visualisation. It is easy for innocent (but devastating) mistakes such as transposing two columns of data to go unnoticed [Miller 2006]. Since visualisations are simply cases of programs that transform structured inputs (data tables) into structured outputs (charts and other graphics), general-purpose language-based techiques for fine-grained dependency tracking should be able to help with this, by making it possible to reveal these relationships automatically to an interested user.

1.1 Linking Structured Outputs to Structured Inputs

First, interpreting a chart would be much easier if the user were able to explore the relationship between the various parts of the chart and the underlying data interactively, discovering the relevant relationships on a need-to-know basis. For example, selecting a particular bar in a bar chart could highlight the relevant data in a table, perhaps showing only the relevant rows, as illustrated in Figure 1. We could certainly do more and say something about the nature of the relationship (summation, in this case), but even just revealing the relevant data puts a reader in a much better position to fact-check or confirm their own understanding of what they are looking at. (The figure shows how selecting the bar for the USA should highlight different data than selecting the bar for China.) Indeed, this is useful enough that visualisation designers sometimes create "data-linked" artefacts like these by hand, such as Nadieh Bremer's award-winning visualisation of population density growth in Asian cities [Bremer and Ranzijn 2015], at the cost of significant programming effort. Libraries such as Altair [VanderPlas et al. 2018] alleviate some of this work, but require data transformations to be specified using a limited set of combinators provided (and understood) by the library.

What we would like to do is allow data scientists to author analyses and visualisations using an expressive functional language like the one shown in Figure 1, and obtain data linking automatically for the generated artefact, as a baked-in transparency feature. At the core of this is a program




```
let series type country = [
   { x: year, y: row.output }
   | year ⟵ [2013..2018], row ⟵ data,
     row.year == year, row.energyType == type, row.country == country
] in LineChart {
   caption: "Output of USA relative to China",
   plots: [
      LinePlot { name: type, data: plot }
      | type ⟵ ["Bio", "Hydro", "Solar", "Wind"],
        let plot = zipWith (fun p1 p2 ⟶ { x: p1.x, y: p1.y / p2.y })
                           (series type "USA") (series type "China")
   ]
}
```

Fig. 2. Linking visualisations via common data dependencies

analysis problem: we want to be able to focus on a particular visual attribute — say the value of `y` in the record `{x: "USA", y: 196.7}` passed to `BarChart` in the example above — and perform some kind of backwards analysis to determine the relevant inputs, in this case the value of `output` in four of the records that appear in the data source. Framing this as a program analysis problem not only provides a path to automation, but also invites interesting questions that a hand-crafted solution is unlikely to properly address. For example, does the union of two output selections depend on the union of their respective dependencies? Do dependencies "round-trip", in that they identify sufficient resources to reconstruct the selected output? Are they minimal? These questions are important to establishing trust, and a language-based approach offers a chance to address them.

1.2 Linking Structured Outputs to Other Structured Outputs

Second, authors often present distinct but related aspects of data in separate charts. In this situation a reader should be able to focus on (select) a visual element in one chart or other structured output and automatically see elements of a different chart which were computed using related inputs. For example in Figure 2 below, selecting the bar on the left should automatically highlight all the related visual elements on the right. This is a well-recognised use case called *brushing and linking* [Becker and Cleveland 1987], which is supported by geospatial applications like GeoDa [Anselin et al. 2006] and charting libraries like Plotly, but tends to be baked into specific views, or require programmer effort and therefore anticipation in advance by the chart designer. Moreover these applications and libraries provide no direct access to the common data which explains why elements are related.

Again, we would like to enable a more automated (and ubiquitous) version of brushing and linking, without imposing a burden on the programmer. They should be able to express visualisations and other data transformations using standard functional programming features such as those shown in Figure 2, and have brushing and linking enabled automatically between computed artefacts

which depend on common data. At the core of this requirement is a variant of our original program analysis problem: we want to select part of the output and perform a backwards analysis to identify the required inputs, as before, but then also perform a forwards analysis to identify the dependent parts of the other output. In Figure 2, these consist of the value of `y` for the record passed to `LinePlot` where `x` has the value `2015`, for each `LinePlot` in the list passed to `LineChart`. Moreover, we would also like the brushing and linking feature to be able to provide a concise view of the data that explain why the two selections are linked. Note, however, that the intuition behind the forwards analysis here is not the same as the one we appealed to in the context of round-tripping: there the (hypothetical) question was whether the selected data was *sufficient* to reconstruct the selected output, whereas to identify related items in another view, we must determine those parts for which the selected data is *necessary*. As before, a language-based approach offers the prospect of addressing these sorts of question in a robust way.

1.3 Contributions

To make progress towards these challenges, we present a bidirectional analysis which tracks fine-grained data dependencies between input and output selections, with round-tripping properties characterised by Galois connections. Selections have a complement, which we use to adapt the analysis to compute fine-grained dependencies between two outputs which depend on common inputs. Recent program slicing techniques [Perera et al. 2012, 2016; Ricciotti et al. 2017] allow the user to focus on the output by "erasing" parts deemed to be irrelevant; the erased parts, called *holes*, are propagated backwards by a backwards analysis which identifies parts of the program and input which are no longer needed. Although these approaches also enjoy useful round-tripping properties characterised by Galois connections, they only allow focusing on *prefixes* (the portion of the output or program that remains after the irrelevant parts have been erased), a notion which is not closed under complement. Our specific contributions are as follows:

- a new bidirectional dynamic dependency analysis which operates on selections of arbitrary parts of data values, for a core calculus with lists, records and mutual recursion, and a proof that the analysis is a Galois connection (§ 3);
- a second bidirectional dependency analysis, derived from the first by De Morgan duality, which is also a Galois connection and which can be composed with the first analysis to link outputs to outputs, with an extended example based on matrix convolution (§ 4);
- a richer surface language called Fluid[1], implemented in PureScript, with familiar functional programming features such as piecewise definitions and list comprehensions, and a further Galois connection linking selections between the core and surface languages (§ 5).

Proofs and other supplementary materials can be found at https://arxiv.org/abs/2109.00445.

2 CORE LANGUAGE

The core calculus which provides the setting for the rest of the paper is a mostly standard call-by-value functional language with datatypes and records. The main unusual feature is the use of *eliminators*, a trie-like construct that provides a uniform syntax and semantics for pattern-matching; this allows us to assume that incomplete or overlapping patterns and other syntactic considerations have been dealt in the surface language. (In § 5 we show how familiar pattern-matching features like case expressions and piecewise function definitions easily desugar into eliminators.) We give a big-step environment-based semantics, which is easier for the backward and forward dependency analyses in § 3, and introduce a compact (term-like) representation of derivation trees in the

[1]See https://github.com/explorable-viz/fluid/. To generate the figures in this paper, check out tag `v0.4.2` and follow the instructions in artifact-evaluation.md.

	Type	
$A, B ::=$	`Bool`	Booleans
	`Int`	integers
	`Rec` $(\overrightarrow{x\colon A})$	records
	`List` A	lists
	$A \to B$	functions
$\Gamma, \Delta ::=$	$\overrightarrow{x\colon A}$	typing context

	Term	
$e ::=$	`true` | `false`	Boolean
	n	integer
	x	variable
	$\phi(\overrightarrow{e})$	primitive application
	$e\, e'$	application
	`[]` | u `:` v	list
	$(\overrightarrow{x\colon e})$	record
	e`.`x	record projection
	$\lambda\sigma$	anonymous function
	`let` h `in` e	recursive let
$h ::=$	$\overrightarrow{x\colon \sigma}$	recursive functions

	Continuation type	
$K ::=$	A	term
	$A \rightarrowtail K$	eliminator

	Continuation	
$\kappa ::=$	e	term
	σ	eliminator

	Eliminator	
$\sigma, \tau ::=$	$x\colon \kappa$	variable
	$\{$`true`$\colon \kappa$, `false`$\colon \kappa'\}$	Boolean
	$\{(\overrightarrow{x})\colon \kappa\}$	record
	$\{$`[]`$\colon \kappa$, `(:)`$\colon \sigma\}$	list

	Value	
$u, v ::=$	`true` | `false`	Boolean
	n	integer
	`[]` | u `:` v	list
	$(\overrightarrow{x\colon v})$	record
	`cl`(ρ, h, σ)	closure
$\rho ::=$	$\overrightarrow{x\colon v}$	environment

Fig. 3. Syntax of core language

operational semantics, called *traces*, which we will use to define the analyses over a fixed execution. Mutual recursion requires some care for the backwards analysis, so we also treat that as a core language feature.

2.1 Syntax and Typing

Although our implementation is untyped, types help describe the structure of the core language. Figure 3 introduces the types A, B which include `Bool`, `Int` and function types $A \to B$, but also lists `List` A and records `Rec` $(\overrightarrow{x\colon A})$ which exemplify the two kinds of structured data which are of interest: recursive datatypes with varying structure, and tabular data with a fixed shape. As usual the notation $x\colon A$ denotes the binding of x to A (understood formally as a pair); $\overrightarrow{x\colon A}$ denotes the sequence of bindings that results from zipping same-length sequences $\overrightarrow{x}$ and $\overrightarrow{A}$. In a record type `Rec` $(\overrightarrow{x\colon A})$ the field names in $\overrightarrow{x}$ are required to be unique.

The terms e of the language are defined in Figure 3. These include Boolean constants `true` and `false`, integers n, variables x, and applications $e\, e'$. Primitives are not first-class; the expression $\phi(\overrightarrow{e})$ is the fully saturated application of ϕ to a sequence of arguments. (First-class and infix primitives are provided by desugarings in § 5). We also provide list constructors nil `[]` and cons e `:` e', record construction $(\overrightarrow{x\colon e})$ and record projection e`.`x. The final two term forms, anonymous functions $\lambda\sigma$ and recursive let-bindings `let` h `in` e where h is of the form $\overrightarrow{x\colon \sigma}$, are explained below after we introduce the pattern-matching construct σ (*eliminator*). The typing rules for terms are given in Figure 4, and are intended only to help a reader understand the language; therefore the rules are simple and do not include features such as polymorphism. The main typing rules of interest are the ones which involve eliminators.

2.2 Eliminators

Eliminators σ, τ are also defined in Figure 3, and are essentially generalised tries [Connelly and Morris 1995; Hinze 2000] extended with variable binding. An eliminator specifies how to match an initial part of a value and select a continuation κ for further execution; κ may be a term e, or another eliminator σ. The Boolean eliminator $\{\texttt{true}\colon \kappa, \texttt{false}\colon \kappa'\}$ selects either κ or κ' depending on whether a Boolean value is `true` or `false`. The record eliminator $\{(\vec{x})\colon \kappa\}$ matches a record with fields $\vec{x}$ and then selects κ with the variables $\vec{x}$ bound to the components of the record. The list eliminator $\{[]\colon \kappa, (:)\colon \sigma\}$ selects κ if the list is empty and otherwise defers to another eliminator σ which specifies how the head and tail of the list are to be matched. Finally, the variable eliminator $x\colon \kappa$ extends the usual notion of trie, matching any value, and selecting κ with x bound to that value. Eliminators resemble the "case trees" commonly used as an intermediate form when compiling languages with pattern-matching [Graf et al. 2020], and can serve as an elaboration target for more user-oriented features such as the piecewise definitions described in § 5.

The use of nested eliminators to match sub-values will become clearer if we consider the typing judgement $\Gamma \vdash \sigma : A \rightarrowtail K$ given in Figure 4. Eliminators always have a function-like type; the judgement form should be read as a four-place relation, with $\rightarrowtail$ being part of the notation. (The definition delegates to an auxiliary judgement $\Gamma \vdash \kappa : K$ which we define to be the union of the $\Gamma \vdash e : A$ and $\Gamma \vdash \sigma : A \rightarrowtail K$ relations.) The typing rule for variable eliminators reveals the connection between eliminators and functions: it converts a continuation κ which can be assigned type K under the assumption that x is of type A into an eliminator of type $A \rightarrowtail K$. The typing rule for Boolean eliminators says that to make an eliminator of type $\texttt{Bool} \rightarrowtail K$, we simply need continuations κ and κ' of type K. The rule for the empty record states that to make an eliminator of type $\texttt{Rec}\ () \rightarrowtail K$, we simply need a continuation κ of type K. The rule for non-empty records allows us to transform a "curried" eliminator of type $\texttt{Rec}\ (\overrightarrow{x\colon A}) \rightarrowtail B \rightarrowtail K$ into one of type $\texttt{Rec}\ (\overrightarrow{x\colon A} \cdot y\colon B) \rightarrowtail K$, analogous to the isomorphism between $A \to B \to C$ and $A \times B \to C$ [Hinze 2000]. (Formalising eliminators precisely requires nested datatypes [Bird and Meertens 1998] and polymorphic recursion, but these details need not concern us here.)

The typing rule for list eliminators $\{[]\colon \kappa, (:)\colon \sigma\}$ combines some of the flavour of record and Boolean eliminators. To make an eliminator of type $\texttt{List}\ A \rightarrowtail K$, we need a continuation of type K for the empty case, and for the non-empty case, an eliminator of type $A \rightarrowtail \texttt{List}\ A \rightarrowtail K$ which will be used to process the head and tail.

2.2.1 Functions as Eliminators. We can now revisit the term forms $\lambda\sigma$ and $\texttt{let}\ h\ \texttt{in}\ e$. If σ is an eliminator of type $A \rightarrowtail B$, then $\lambda\sigma$ is an anonymous function of type $A \to B$. If h is of the form $\overrightarrow{x\colon \sigma}$, then $\texttt{let}\ h\ \texttt{in}\ e$ introduces a sequence of mutually recursive functions which are in scope in e. The typing rule for $\texttt{let}\ h\ \texttt{in}\ e$ uses an auxiliary typing judgement $\Gamma \vdash h : \Delta$ which assigns to every x in Δ the function type $A \to B$ if the σ to which x is bound in h has the eliminator type $A \rightarrowtail B$.

2.2.2 Values. Values v, u, and environments ρ are also defined in Figure 3, and are standard for call-by-value. (Environments are more convenient than substitution for tracking variable usage.) To support mutual recursion, the closure form $\texttt{cl}(\rho, h, \sigma)$ captures the (possibly empty) sequence h of functions with which the function was mutually defined, in addition to the ambient environment ρ. For the typing judgements $\vdash \rho : \Gamma$ and $\vdash v : A$ for environments and values (Figure 4), only the closure case is worth noting, which delegates to the typing rules for recursive definitions and eliminators.

2.2.3 Evaluation. Figure 6 gives the operational semantics of the core language. In § 3 we will define forward and backward analyses over a single execution; in anticipation of that use case, we treat the operational semantics as an inductive data type, following the "proved transitions"

$\boxed{\Gamma \vdash e : A}$ *e* ***has type*** *A* ***under*** Γ

$$\frac{}{\Gamma \vdash x : A}\ x : A \in \Gamma \qquad \frac{}{\Gamma \vdash n : \texttt{Int}} \qquad \frac{}{\Gamma \vdash \texttt{true} : \texttt{Bool}} \qquad \frac{}{\Gamma \vdash \texttt{false} : \texttt{Bool}}$$

$$\frac{\Gamma \vdash e_i : A_i \quad (\forall i \le |\vec{x}|)}{\Gamma \vdash (\overrightarrow{x\colon e}) : \texttt{Rec}\ (\overrightarrow{x\colon A})} \qquad \frac{\Gamma \vdash e : \texttt{Rec}\ (\overrightarrow{x\colon A})}{\Gamma \vdash e.x_i : A_i}\ i \le |\vec{x}| \qquad \frac{\Gamma \vdash \sigma : A \rightarrowtail B}{\Gamma \vdash \lambda\sigma : A \to B}$$

$$\frac{\Gamma \vdash e_i : \texttt{Int} \quad (\forall i \le j)}{\Gamma \vdash \phi(\vec{e}) : \texttt{Int}}\ \phi \in \mathbb{Z}^j \to \mathbb{Z} \qquad \frac{\Gamma \vdash e : A \to B \qquad \Gamma \vdash e' : A}{\Gamma \vdash e\,e' : B} \qquad \frac{}{\Gamma \vdash [] : \texttt{List}\ A}$$

$$\frac{\Gamma \vdash e : A \qquad \Gamma \vdash e' : \texttt{List}\ A}{\Gamma \vdash (e : e') : \texttt{List}\ A} \qquad \frac{\Gamma \vdash h : \Delta \qquad \Gamma \cdot \Delta \vdash e : A}{\Gamma \vdash \texttt{let}\ h\ \texttt{in}\ e : A}$$

$\boxed{\Gamma \vdash \sigma : A \rightarrowtail K}$ σ ***has type*** $A \rightarrowtail K$ ***under*** Γ

$$\frac{\Gamma \cdot x\colon A \vdash \kappa : K}{\Gamma \vdash (x\colon \kappa) : A \rightarrowtail K} \qquad \frac{\Gamma \vdash \kappa : K \qquad \Gamma \vdash \kappa' : K}{\Gamma \vdash \{\texttt{true}\colon \kappa, \texttt{false}\colon \kappa'\} : \texttt{Bool} \rightarrowtail K} \qquad \frac{\Gamma \vdash \kappa : K}{\Gamma \vdash \{():\kappa\} : \texttt{Rec}\ () \rightarrowtail K}$$

$$\frac{\Gamma \vdash \{(\vec{x}):\sigma\} : \texttt{Rec}\ (\overrightarrow{x\colon A}) \rightarrowtail B \rightarrowtail K}{\Gamma \vdash \{(\vec{x} \cdot y):\sigma\} : \texttt{Rec}\ (\overrightarrow{x\colon A} \cdot y\colon B) \rightarrowtail K} \qquad \frac{\Gamma \vdash \kappa : K \qquad \Gamma \vdash \sigma : A \rightarrowtail \texttt{List}\ A \rightarrowtail K}{\Gamma \vdash \{[]\colon \kappa, (:):\sigma\} : \texttt{List}\ A \rightarrowtail B}$$

$\boxed{\vdash v : A}$ v ***has type*** A

$$\frac{}{\vdash n : \texttt{Int}} \qquad \frac{}{\vdash \texttt{true} : \texttt{Bool}} \qquad \frac{}{\vdash \texttt{false} : \texttt{Bool}} \qquad \frac{\vdash v_i : A_i \quad (\forall i \le |\vec{x}|)}{\vdash (\overrightarrow{x\colon v}) : \texttt{Rec}\ (\overrightarrow{x\colon A})} \qquad \frac{}{\vdash [] : \texttt{List}\ A}$$

$$\frac{\vdash u : A \qquad \vdash v : \texttt{List}\ A}{\vdash (u : v) : \texttt{List}\ A} \qquad \frac{\vdash \rho : \Gamma \qquad \Gamma \vdash h : \Delta \qquad \Gamma \cdot \Delta \vdash \sigma : A \rightarrowtail B}{\vdash \texttt{cl}(\rho, h, \sigma) : A \to B}$$

$\boxed{\vdash \rho : \Gamma}$ ρ ***has type*** Γ $\qquad$ $\boxed{\Gamma \vdash h : \Delta}$ h ***has type*** Δ ***under*** Γ

$$\frac{\vdash v_i : A_i \quad (\forall i \le |\vec{x}|)}{\vdash \overrightarrow{x\colon v} : \overrightarrow{x\colon A}} \qquad \frac{\Gamma \cdot \Delta \vdash \sigma_i : A_i \rightarrowtail B_i \quad (\forall i \le |\vec{x}|)}{\Gamma \vdash \overrightarrow{x\colon \sigma} : \Delta}\ \Delta = \overrightarrow{x\colon A \to B}$$

Fig. 4. Typing rules for core language

approach adopted by Boudol and Castellani [1989] for reversible CCS. The inhabitants of this data type are derivation trees explaining how a result was computed, and the analyses will be defined by structural recursion over these trees. Expressed in terms of inference rules, these trees can become quite cumbersome, so we introduce an equivalent but more term-like syntax for them, called a *trace* (Figure 5), similar to the approach taken by Perera et al. [2016] for π-calculus.

Trace

$T, U ::=$	x	variable
	`true` | `false`	Boolean
	n	integer
	$(\overrightarrow{x\colon T})$	record
	$T_{\overrightarrow{x\colon v}}.y$	record projection
	`[]` | T `:` U	list
	$\lambda\sigma$	anonymous function
	$T\ U \blacktriangleright w\colon T'$	application
	$\phi(\overrightarrow{U_n})$	primitive application
	`let` h `in` T	recursive let

Match

$w ::=$	x	variable
	`true` | `false`	Boolean
	$(\overrightarrow{x\colon w})$	record
	`[]` | w `:` w'	list

Fig. 5. Syntax of traces and matches

The judgement $T :: \rho, e \Rightarrow v$ defined at the top of Figure 6 states that term e under environment ρ evaluates to value v, and that T is a proof term that witness that fact. (In the figure, the traces appear in grey, to reinforce the idea that they are not part of the definition of $\Rightarrow$ but rather a notation for its inhabitants.) The rules for Booleans, integers and lists are standard and have unsurprising trace forms. For variables, we give an explicit inductive definition of the environment lookup relation $\in$ at the bottom of the figure, again so that later we can perform analysis over a proof that an environment contains a binding. The lambda rule is standard except that we specify ε for the sequence of definitions being simultaneously defined, since a lambda is not recursive. For record construction, the trace form contains a subtrace T_i for each field, and for record projection, which also uses the lookup relation $\in$, the trace form $T_{\overrightarrow{x\colon v}}.y$ records both the record $\overrightarrow{x\colon v}$ and the field name y that was selected.

The rule for (mutually) recursive functions `let` h `in` e, where h is a sequence $\overrightarrow{x\colon \sigma}$ of function definitions, makes use of the auxiliary relation $\rho, h \twoheadrightarrow \rho'$ at the bottom of Figure 6 which turns h into an environment ρ' binding each function name x_i to a closure $\mathtt{cl}(\rho, h, \sigma_i)$ capturing ρ and a copy of h. For primitive applications, the trace records the values of the arguments which were passed to the operation ϕ. The rule for application $e\,e'$ is slightly non-standard, because it must deal with both mutual recursion and pattern-matching. First we unpack the recursive definitions h from the closure $\mathtt{cl}(\rho_1, h, \sigma)$ computed by e, and again use the auxiliary relation $\twoheadrightarrow$ to promote this into an environment ρ_2 of closures. We then use the relation $\rightsquigarrow$ explained below to match v against the eliminator σ, obtaining the branch e'' of the function to be executed and parameter bindings ρ_3. In addition to subtraces T and U for the function and argument, the application trace $T\ U \blacktriangleright w\colon T'$ also has subtraces w for the pattern-match and T' for the selected branch.

2.2.4 Pattern Matching. The judgement $w :: v, \sigma \rightsquigarrow \rho, \kappa$ also defined in Figure 6 states that eliminator σ can match v and produce environment ρ and continuation κ, with ρ containing the variable bindings that arose during the match. *Matches* w are a compact notation for proof terms for the $\rightsquigarrow$ relation, analogous to traces for the $\Rightarrow$ relation, and again appear in grey in the figure.

Variable eliminators $x\colon \kappa$ match any value, returning the singleton environment $x\colon v$ and continuation κ. Boolean eliminators match any Boolean value, returning the appropriate branch and empty environment ε. List eliminators $\{\mathtt{[]}\colon \kappa, (\mathtt{:})\colon \sigma\}$ match any list. The nil case is analogous to the handling of Booleans; the cons case depends on the fact that the nested eliminator σ for the cons branch has the curried type $A \rightarrowtail \mathtt{List}\ A \rightarrowtail K$. First, we recursively match the head v of type A using σ, obtaining bindings ρ and eliminator $\tau : \mathtt{List}\ A \rightarrowtail K$ as the continuation. Then the tail v' is matched using τ to yield additional bindings ρ' and final continuation κ' of type K. As a simple example, which omits the proof terms w, consider the following pattern-match:

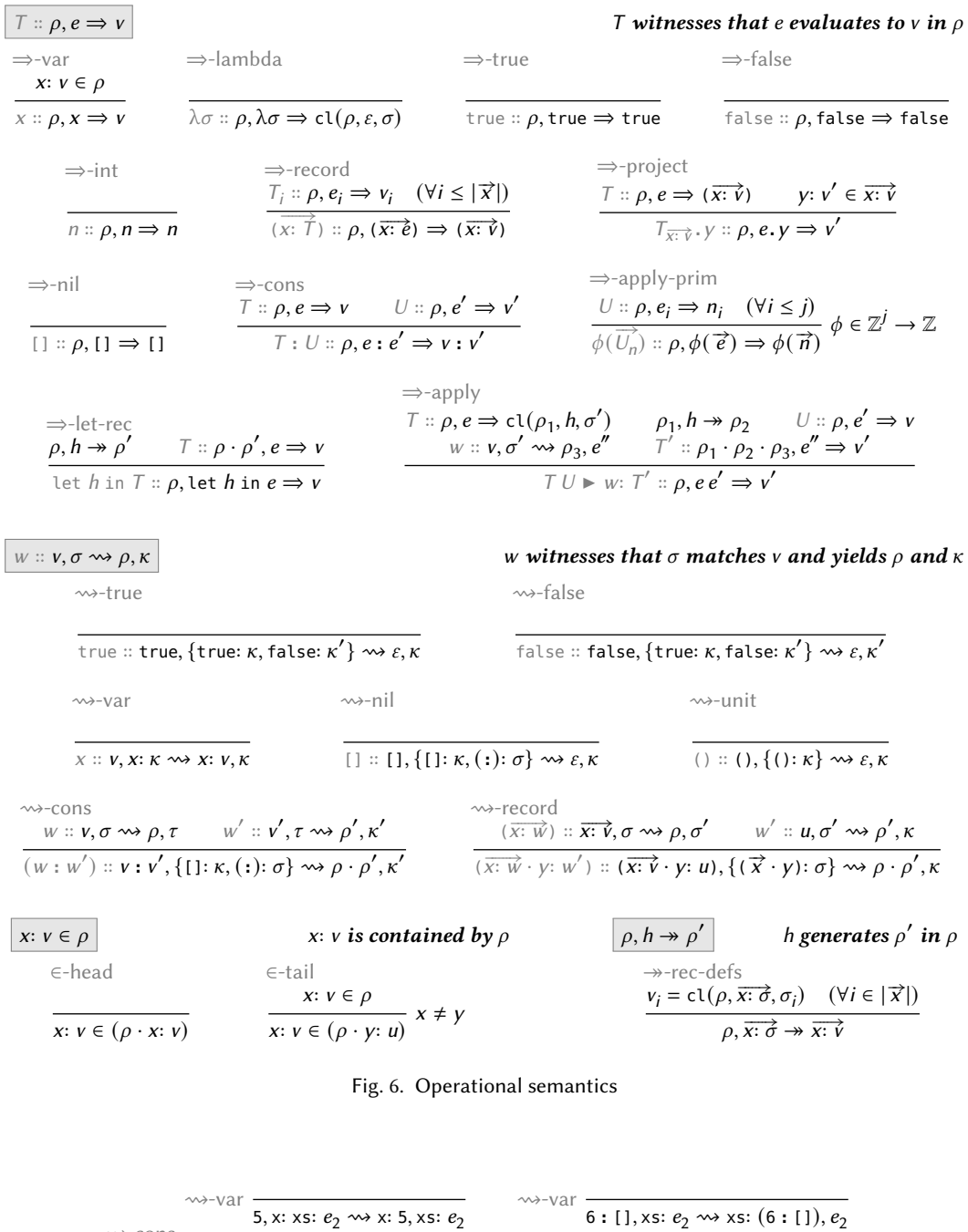
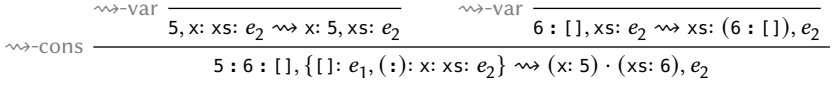


Fig. 6. Operational semantics



Here the eliminator $\{\texttt{[]}\colon e_1, \texttt{(:)}\colon \texttt{x}\colon \texttt{xs}\colon e_2\}$ is used to match `5 : 6 : []`. The `[]` case is disregarded; the `(:)` case is used to retrieve a variable eliminator $\texttt{x}\colon \texttt{xs}\colon e_2$, which is used to match the head `5`. This produces the binding $\texttt{x}\colon 5$ and a further variable eliminator $\texttt{xs}\colon e_2$ as the continuation, which is used to match the tail. This produces the additional binding $\texttt{xs}\colon (6 : [])$ and the expression e_2 as

the continuation. To see how this might generalise to a nested pattern, consider how one could replace the inner variable eliminator `xs`: e_2 by another list eliminator.

Record matching is similar: the empty record case resembles the nil case, and the non-empty case relies on the nested eliminator having curried type $\texttt{Rec}\ (\overrightarrow{x\colon A}) \rightarrowtail B \rightarrowtail K$. The initial part $\overrightarrow{x\colon v}$ of the record is matched using σ, returning another eliminator σ' of type $B \rightarrowtail K$. Then the last field $y\colon u$ is matched using σ' to yield final continuation κ of type K.

3 A BIDIRECTIONAL DYNAMIC DEPENDENCY ANALYSIS

We now extend the core language from § 2 with a bidirectional mechanism for tracking data dependencies. § 3.1 establishes a way of selecting (parts of) values, such as the height of a bar in a bar chart. § 3.2 defines a forward analysis function $\nearrow_T$ which specifies how selections on programs and environments (collectively: *input selections*) become selections on outputs; selections represent *availability*, with the computed output selection indicating the data available to the downstream computation. § 3.3 defines a backward dependency function $\searrow_T$ specifying how output selections are mapped back to inputs; then selections represent demands, with the computed input selection identifying the data needed from the upstream computation. Both functions are monotonic. This will become important in § 3.4, where we show that $\searrow_T$ and $\nearrow_T$ form a *Galois connection*, establishing the round-tripping properties alluded to in § 1.1.

3.1 Lattices of Selections

Our approach to representing selections is shown in Figure 7. The basic idea is to parameterise the type Val of values by a (bounded) lattice $\mathcal{A}$ of *selection states* α. We add selection states to Booleans, integers, records and lists; while it would present no complications to equip closures with selection states too, for present purposes we are only interested in dependencies between first-order data, so closures are not (directly) selectable. Closures do however have selectable parts, and moreover capture the current *argument availability*, explained in § 3.2.2 below, which is also a selection state α. We parameterise the type Term of terms similarly, allowing us to trace data dependencies back to expressions that appear in the source code, but only add selection states to the term constructors corresponding to selectable values. We return to this in § 5.

	Terms selections			***Value selections***	
$e \in \mathsf{Term}\,\mathcal{A} ::=$	...		$u, v \in \mathsf{Val}\,\mathcal{A} ::=$	$\square$	hole
	$\square$	hole		$\texttt{true}_\alpha \mid \texttt{false}_\alpha$	Boolean
	$\texttt{true}_\alpha \mid \texttt{false}_\alpha$	Boolean		n_α	integer
	n_α	integer		$(\overrightarrow{x\colon v})_\alpha$	record
	$(\overrightarrow{x\colon e})_\alpha$	record		$[]_\alpha \mid u :_\alpha v$	list
	$[]_\alpha \mid e :_\alpha e'$	list		$\texttt{cl}(\rho, h, \alpha, \sigma)$	closure
$\alpha, \beta \in \mathcal{A}$		selection state			

Fig. 7. Selection states, term selections and value selections

The top and bottom elements $\top$ and $\bot$ of $\mathcal{A}$ represent fully selected and fully unselected; the meet and join operations $\sqcap$ and $\sqcup$, which have $\top$ and $\bot$ as their respective units, are used to combine selection information. In Figure 1, the `data` field of `BarChart` expects a list of records with fields `x` and `y`, mapping strings representing categorical data to floats determining the height of the corresponding bar; the record computed for China is `(x: "China" · y: 295.3)`. The two-point lattice $2 \stackrel{\text{def}}{=} \langle \{\mathrm{tt}, \mathrm{ff}\}, \mathrm{tt}, \mathrm{ff}, \wedge, \vee \rangle$ can be used to represent the selection of the field `y` within this record as $\texttt{(x: "China"}_{\mathrm{ff}} \cdot \texttt{y: 295.3}_{\mathrm{tt}}\texttt{)}_{\mathrm{ff}}$, indicating that the number `295.3` is selected, but that neither the

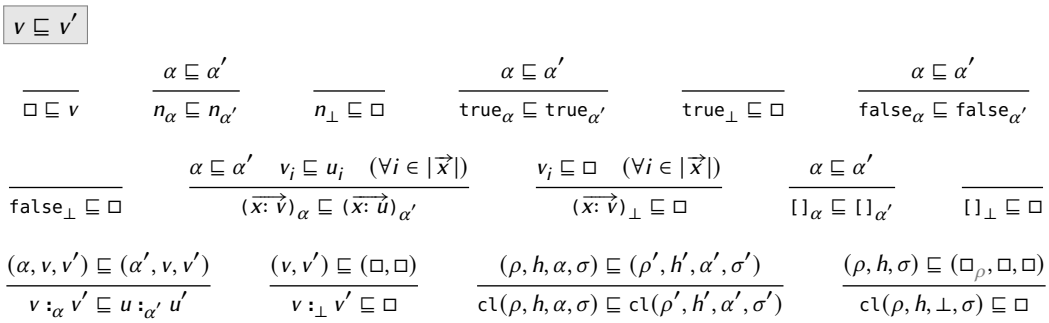


Fig. 8. Preorder on value selections

string `"China"`, nor the record itself, is selected. Because lattices are closed under component-wise products, we sometimes write $(\alpha, \beta) \sqsubseteq (\alpha', \beta')$ to mean that $\alpha \sqsubseteq \alpha'$ and $\beta \sqsubseteq \beta'$. This also suggests more interesting lattices of selections, such as vectors of Booleans to represent multiple selections simultaneously, which might be visualised using different colours (as in Figure 1).

3.1.1 Selections of a Value. The analyses which follow will be defined with respect to a fixed computation, and so we will often need to talk about the selections of a given value. To make this notion precise, consider that the raw (selection-free) syntax described in § 2 can be recovered from a term selection via an erasure operation $\lfloor \cdot \rfloor : \mathrm{Val}\, \mathcal{A} \to \mathrm{Val}\, 1$ which forgets the selection information, where 1 is the trivial one-point lattice. We refer to $\lfloor v \rfloor$ as the *shape* of v. Allowing $\mathbf{u}, \mathbf{v}$ from now on to range over raw values, and reserving u, v for value selections, we can then define:

Definition 3.1 (Selections of $\mathbf{v}$*).* Define $\mathrm{Sel}_{\mathbf{v}}\, \mathcal{A}$ to be the set of all values $v \in \mathrm{Val}\, \mathcal{A}$ with shape $\mathbf{v}$, i.e. that erase to $\mathbf{v}$.

Since its elements have a fixed shape, the pointwise comparison of any $v, v' \in \mathrm{Sel}_{\mathbf{v}}\, \mathcal{A}$ using the partial order $\sqsubseteq$ of $\mathcal{A}$ is well defined, as is the pointwise application (zip) of a binary operation [Gibbons 2017]. It should therefore be clear that if $\mathcal{A}$ is a lattice, then $\mathrm{Sel}_{\mathbf{v}}\, \mathcal{A}$ is also a lattice, with $\top_{\mathbf{v}}$, $\bot_{\mathbf{v}}$, $\sqcap_{\mathbf{v}}$, and $\sqcup_{\mathbf{v}}$ defined pointwise. For example, if u and u' have the same shape and v and v' have the same shape, the join of the lists $(u :_\alpha v)$ and $(u' :_{\alpha'} v')$ is defined and equal to $(u \sqcup u') :_{\alpha \sqcup \alpha'} (v \sqcup v')$. Similarly, the top element of $\mathrm{Sel}_{\mathbf{v}}\, \mathcal{A}$ is the selection of $\mathbf{v}$ which has $\top$ at every selection position. (We omit the $\mathbf{v}$ indices from these lattice operations if it is clear which lattice is being referred to.) The notion of the "selections" of $\mathbf{v}$ extends to the other syntactic forms.

3.1.2 Environment Selections and Hole Equivalence. The notion of the "selections" of $\mathbf{v}$ also extends (pointwise) to environments, so that $\mathrm{Sel}_{\boldsymbol{\rho}}\, \mathcal{A}$ means the set of environment selections ρ' of shape $\boldsymbol{\rho}$, where the variables in ρ' are bound to selections of the corresponding variables in $\boldsymbol{\rho}$. One challenge arises from the pointwise use of $\sqcup$ to combine environment selections. Since environments contain other environments recursively, via closures, a naive implementation of environment join is a very expensive operation. One solution is to employ an efficient representation of values which are fully unselected, which is often the case during the backward analysis.

We therefore augment the set of value selections $\mathrm{Val}\, \mathcal{A}$ with a distinguished element *hole*, written $\square$, which is an alternative notation for $\bot_{\mathbf{v}}$ for any $\mathbf{v}$, i.e. the selection of shape $\mathbf{v}$ which has $\bot$ at every selection position, and generalise this idea to terms and eliminators. The equivalence of $\square$ to any such bottom element is established explicitly by the preorder order defined (for values) in Figure 8: the first rule always allows $\square$ on the left-hand side of $\sqsubseteq$, and other rules allow $\square$ on the

right-hand side of $\sqsubseteq$ as long as all the selections that appear on the left-hand side are $\bot$. (The rules for terms e and eliminators σ are analogous and are omitted.) If we write $\doteq$ for the equivalence relation induced by $\sqsubseteq$ on values selections, which we call *hole-equivalence*, it should be clear that $\Box \sqcup v \doteq v$ and $\Box \sqcap v \doteq \Box$. This means the join of two selections v, v' of $\mathbf{v}$ can be implemented efficiently, whenever one selection is $\Box$, by simply discarding $\Box$ and returning the other selection without further processing.

Definition 3.2 (Hole equivalence). Define $\doteq$ as the intersection of $\sqsubseteq$ and $\sqsupseteq$.

Because $\Box$ is equivalent to $\bot_{\mathbf{v}}$ for any $\mathbf{v}$, all such bottom elements are hole-equivalent. For example, the value selection $\Box :_\top \Box$ is hole-equivalent to $5_\bot :_\top \Box$, but also to $6_\bot :_\top [\,]_\bot$, and so the last two selections, even though they have different shapes, are hole-equivalent by transitivity. In practice we only use the hole ordering to compare selections with the same shape.

3.2 Forward Data Dependency

We now define the core bidirectional data dependency analyses for a fixed computation $T :: \boldsymbol{\rho}, \mathbf{e} \Rightarrow \mathbf{v}$, where T is a trace. In practice one would obtain T by first evaluating $\mathbf{e}$ in $\boldsymbol{\rho}$, and then run multiple forward or backward analyses over T with appropriate lattices. We start with the forward dependency function $\nearrow_T$ which "replays" evaluation, turning input availability into output availability, with T guiding the analysis whenever holes in the input selection would mean the analysis would otherwise get stuck. $\nearrow_T$ uses the auxiliary function $\nearrow_w$ for forward-analysing a pattern-match; we explain this first, as it introduces the key idea of a selection as identifying the data available to a downstream computation.

3.2.1 Forward Match. Figure 9 defines a family of *forward-match* functions $\nearrow_w$ of type $\mathrm{Sel}_{\mathbf{v},\sigma}\,\mathcal{A} \to (\mathrm{Sel}_{\boldsymbol{\rho},\boldsymbol{\kappa}}\,\mathcal{A}) \times \mathcal{A}$ for any $w :: \mathbf{v}, \boldsymbol{\sigma} \rightsquigarrow \boldsymbol{\rho}, \boldsymbol{\kappa}$. (The definition is presented in a relational style for readability, but should be understood as a total function defined by structural recursion on w, which appears in grey to emphasise the connection to Figure 6.) Forward match replays the match witnessed by w, turning availability $(v, \sigma) \in \mathrm{Sel}_{\mathbf{v},\sigma}\,\mathcal{A}$ on the matched value and eliminator into availability $(\rho, \kappa) \in \mathrm{Sel}_{\boldsymbol{\rho},\boldsymbol{\kappa}}\,\mathcal{A}$ on the variable bindings and continuation yielded by the match.

$\nearrow_w$ also returns the *meet* of the selection states associated with the part of $\mathbf{v}$ which was matched by $\boldsymbol{\sigma}$. We call this the *argument availability*, since it represents the availability of the matched part of a function argument. In the variable case, the empty part of $\mathbf{v}$ was matched and so the argument availability in this context is simply $\top$, the unit for $\sqcap$. In the Boolean case, the argument availability is simply the α on $\texttt{true}_\alpha$ or $\texttt{false}_\alpha$; the empty list and empty record cases are similar. In the cons case, we return the meet of the α on the cons node itself with the availabilities β and β' computed for v and v'. Non-empty records are similar, but to process the initial part of the record, we supply the neutral selection state $\top$ on the subrecord in order to use the definition recursively. (Note that these subrecords exist only as intermediate artefacts of the interpreter.)

One might hope to be able to dispense with the match witness w and simply define $\nearrow$ by case analysis on v and σ. However, it is then unclear how to proceed in the event that either v or σ is a hole. In particular, it is not clear how to obtain the $\boldsymbol{\rho}$ associated with the original pattern-match in order to produce an environment selection $\rho' \in \mathrm{Sel}_{\boldsymbol{\rho}}\,\mathcal{A}$. If $\nearrow$ is defined with respect to a known w, this can be achieved via additional rules $\nearrow$-hole-v and $\nearrow$-hole-σ that define the behaviour at hole to be the same as the behaviour at any $\doteq$-equivalent value in $\mathrm{Sel}_{\mathbf{v}}\,\mathcal{A}$ or $\mathrm{Sel}_{\sigma}\,\mathcal{A}$.

Operationally, these hole rules can be interpreted as "expanding" the holes in v or σ, in a shape-preserving way, until another rule of the definition applies. Recall the pattern-matching example from § 2.2.4. This pattern-match has the witness `x : xs`, recording that the list `5 : 6 : []` was matched to the depth of a single cons. Suppose we wish to forward-analyse over the pattern-match using $\Box$

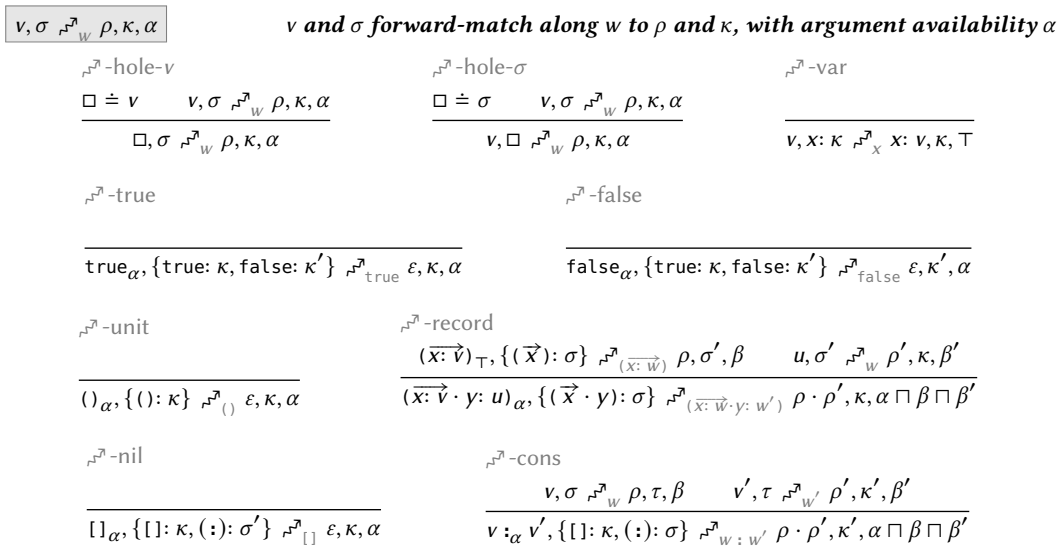


Fig. 9. Forward match

to represent the selection on the matched list. The information in the match witness allows us to expand $\Box$ to $\Box :_\bot \Box$ and then use the $\nearrow$-cons rule to derive the following forward-match:

$$\dfrac{\dfrac{\dfrac{}{\Box, \mathtt{x}\colon \mathtt{xs}\colon e_2 \nearrow_{\mathtt{x}} \mathtt{x}\colon \Box, \mathtt{xs}\colon e_2, \top}\,\nearrow\text{-var} \quad \dfrac{}{\Box, \mathtt{xs}\colon e_2 \nearrow_{\mathtt{xs}} \mathtt{xs}\colon \Box, e_2, \top}\,\nearrow\text{-var}}{\Box :_\bot \Box, \{[]\colon e_1, (:)\colon \mathtt{x}\colon \mathtt{xs}\colon e_2\} \nearrow_{\mathtt{x}\,:\,\mathtt{xs}} (\mathtt{x}\colon \Box) \cdot (\mathtt{xs}\colon \Box), e_2, \bot}\,\nearrow\text{-cons}}{\Box, \{[]\colon e_1, (:)\colon \mathtt{x}\colon \mathtt{xs}\colon e_2\} \nearrow_{\mathtt{x}\,:\,\mathtt{xs}} (\mathtt{x}\colon \Box) \cdot (\mathtt{xs}\colon \Box), e_2, \bot}\,\nearrow\text{-hole-}v$$

Lemma 3.3 below implies that an implementation is free to replace any term by a hole-equivalent one of the same shape, with the result of $\nearrow_w$ being unique up to $\doteq$. This justifies the strategy of expanding holes just enough for a non-hole rule to apply; there will be exactly one such rule, corresponding to the execution path originally taken, and although there may be multiple possible expansions, they will produce hole-equivalent results. This also explains why it is reasonable to think of $\nearrow_w$ not just as a relation, but as a function.

Lemma 3.3 (Monotonicity of $\nearrow_w$). *Suppose* $w :: \mathbf{v}, \boldsymbol{\sigma} \rightsquigarrow \boldsymbol{\rho}, \boldsymbol{\kappa}$, *with* $v, \sigma \nearrow_w \rho, \kappa, \alpha$ *and* $v', \sigma' \nearrow_w \rho', \kappa', \alpha'$. *If* $(v, \sigma) \sqsubseteq (v', \sigma)$ *then* $(\rho, \kappa, \alpha) \sqsubseteq (\rho', \kappa', \alpha')$.

The forward-match function $\nearrow_w$ is a key component of the forward evaluation function $\nearrow_T$ defined in § 3.2.2 below. When forward-analysing a function call, the argument is forward-matched using $\nearrow_w$, and the resulting argument availability α used to upper-bound the availability of any partial values constructed by that function, establishing a forward link from resources consumed and resources produced. Since the dynamic context of a function call extends over multiple evaluation steps, $\nearrow_T$ is threaded with an additional input α which tracks the active argument availability; at the outermost level, before there are any active function calls, this has the value $\top$.

3.2.2 Forward Evaluation. Figure 10 defines a family of *forward-evaluation* functions $\nearrow_T$ of type $(\mathrm{Sel}_{\rho,\mathbf{e}}\,\mathcal{A}) \times \mathcal{A} \to \mathrm{Sel}_{\mathbf{v}}\,\mathcal{A}$ for any $T :: \boldsymbol{\rho}, \mathbf{e} \Rightarrow \mathbf{v}$. (Like forward match, forward evaluation is presented in a relational style, but should be read as a total function defined by structural recursion

$\rho, e, \alpha \nearrow_T v$ — *ρ and e, with argument availability α, forward-evaluate along T to v*

$$\frac{\Box \doteq e \qquad \rho, e, \alpha \nearrow_T v}{\rho, \Box, \alpha \nearrow_T v}\ \nearrow\text{-hole} \qquad \frac{x\colon v \in \rho}{\rho, x, \alpha \nearrow_x v}\ \nearrow\text{-var} \qquad \frac{}{\rho, \lambda\sigma, \alpha \nearrow_{\lambda\sigma'} \mathtt{cl}(\rho, \varepsilon, \alpha, \sigma)}\ \nearrow\text{-lambda}$$

$$\frac{}{\rho, \mathtt{true}_{\alpha'}, \alpha \nearrow_{\mathtt{true}} \mathtt{true}_{\alpha \sqcap \alpha'}}\ \nearrow\text{-true} \qquad \frac{}{\rho, \mathtt{false}_{\alpha'}, \alpha \nearrow_{\mathtt{false}} \mathtt{false}_{\alpha \sqcap \alpha'}}\ \nearrow\text{-false} \qquad \frac{}{\rho, n_{\alpha'}, \alpha \nearrow_n n_{\alpha \sqcap \alpha'}}\ \nearrow\text{-int}$$

$$\frac{\rho, e_i, \alpha \nearrow_{T_i} v_i \quad (\forall i \le |\overrightarrow{x}|)}{\rho, (\overrightarrow{x\colon e})_{\alpha'}, \alpha \nearrow_{(\overrightarrow{x\colon T})} (\overrightarrow{x\colon v})_{\alpha \sqcap \alpha'}}\ \nearrow\text{-record} \qquad \frac{\rho, e, \alpha \nearrow_T \doteq (\overrightarrow{x\colon u})_\beta \qquad y\colon v' \in \overrightarrow{x\colon u}}{\rho, e.y, \alpha \nearrow_{T_{\overrightarrow{x\colon v}}.y} v'}\ \nearrow\text{-project} \qquad \frac{}{\rho, []_{\alpha'}, \alpha \nearrow_{[]} []_{\alpha \sqcap \alpha'}}\ \nearrow\text{-nil}$$

$$\frac{\rho, e, \alpha \nearrow_T v \qquad \rho, e', \alpha \nearrow_U v'}{\rho, e :_{\alpha'} e', \alpha \nearrow_{T:U} v :_{\alpha \sqcap \alpha'} v'}\ \nearrow\text{-cons} \qquad \frac{\rho, e_i, \alpha \nearrow_{U_i} \doteq n_{i\beta_i} \quad (\forall i \le |\overrightarrow{n}|)}{\rho, \phi(\overrightarrow{e}), \alpha \nearrow_{\phi(\overrightarrow{U_n})} \phi(\overrightarrow{n})_{\alpha'}}\ \phi_{\overrightarrow{n}\,*}(\overrightarrow{\beta}) = \alpha'\ \nearrow\text{-apply-prim}$$

$$\frac{\rho, e, \alpha \nearrow_T \doteq \mathtt{cl}(\rho_1, h, \beta, \sigma) \qquad \rho_1, h, \beta \nearrow \rho_2 \qquad \rho, e', \alpha \nearrow_U v \qquad v, \sigma \overset{\nearrow}{\to}_w \rho_3, e'', \beta' \qquad \rho_1 \cdot \rho_2 \cdot \rho_3, e'', \beta \sqcap \beta' \nearrow_{T'} v'}{\rho, e\,e', \alpha \nearrow_{T\,U \blacktriangleright w\colon T'} v'}\ \nearrow\text{-apply} \qquad \frac{\rho, h', \alpha \nearrow \rho' \qquad \rho \cdot \rho', e, \alpha \nearrow_T v}{\rho, \mathtt{let}\ h'\ \mathtt{in}\ e, \alpha \nearrow_{\mathtt{let}\ h\ \mathtt{in}\ T} v}\ \nearrow\text{-let-rec}$$

$\rho, h, \alpha \nearrow \rho'$ — *h forward-generates to ρ' in ρ and α*

$$\frac{v_i = \mathtt{cl}(\rho, \overrightarrow{x\colon \sigma}, \alpha, \sigma_i) \quad (\forall i \in |\overrightarrow{x}|)}{\rho, \overrightarrow{x\colon \sigma}, \alpha \nearrow \overrightarrow{x\colon v}}\ \nearrow\text{-rec-defs}$$

Fig. 10. Forward evaluation

on T.) Forward evaluation replays T, taking a selection $(\rho, e) \in \mathrm{Sel}_{\boldsymbol{\rho},\mathbf{e}}\,\mathcal{A}$ identifying the available parts of the environment and program, and an $\alpha \in \mathcal{A}$ representing the argument availability for the dynamically innermost function call, and returning a selection $v \in \mathrm{Sel}_{\mathbf{v}}\,\mathcal{A}$ identifying the outputs that can be produced using only the available resources. The rules resemble those for the evaluation relation $\Rightarrow$. The general pattern is that each rule takes the active argument availability α, combines it (using $\sqcap$) with any availability supplied on the expression form consumed at that step, and uses the result as the availability of any partial values constructed at that step. The argument availability α is passed down unchanged to any subcomputations, except in the case of function application.

Function application. In the application case, the rule must determine a new argument availability for the function body, because the function context is changing. First, we unpacks the β stored in the closure, representing the argument availability which was active when the closure was constructed. Then we determine an additional selection state β', representing the availability of the matched part of the current argument, by forward-matching v with the eliminator σ from the closure. These are combined using $\sqcap$ to represent the conjoined availability of all arguments that were pattern-matched in order to execute the function body, and the result $\beta \sqcap \beta'$ used to forward-evaluate the function body. The auxiliary function $\nearrow_{\rho,h}\colon (\mathrm{Sel}_{\boldsymbol{\rho},\mathbf{h}}\,\mathcal{A}) \times \mathcal{A} \to \mathrm{Sel}_{\boldsymbol{\rho}'}\,\mathcal{A}$ for any

$\boldsymbol{\rho}, \mathbf{h} \twoheadrightarrow \boldsymbol{\rho}'$ is given at the bottom of Figure 10 and resembles $\twoheadrightarrow$, but captures the active argument availability into each closure.

Primitive application. Since primitive operations are opaque, their input-output dependencies cannot be derived from their execution, but must be supplied by the primitive operation itself. More specifically, every primitive $\phi \in \mathtt{Int}^i \to \mathtt{Int}$ is required to provide a forward-dependency function $\phi_{\vec{n}*} : \mathcal{A}^i \to \mathcal{A}$ for every $\vec{n} \in \mathtt{Int}^i$ which specifies how to turn an input selection $\vec{\alpha} \in \mathcal{A}^i$ for $\vec{n}$ into an output selection α' on $\phi(\vec{n})$. There is one such function per possible input $\vec{n}$ so that the dynamic dependencies for that specific call can depend on the values passed to the operation. For example, in our implementation, the dependency function for multiplication establishes (for non-zero n) that both $n * 0$ and $0 * n$ depend only on 0. However, primitives are free to implement forward-dependency however they choose, with the caveat that § 3.3.2 will also require ϕ to provide a backward-dependency function for any input $\vec{n}$, and § 3.4 will require these to be related in a certain way for the consistency of the whole system to be guaranteed.

Other rules. The remaining rules follow the general pattern. Variable lookup disregards α, simply preserving the selection on the value extracted from the environment. The lambda rule captures α in the closure along with the environment; the letrec rule passes α on to $\nearrow$ so it can be captured by recursive closures as well. Record projection is more interesting, disregarding not only the argument availability α but also the availability β of the record itself. This is because containers are considered to be independent of the values they contain: here, v_i has its own internal availability which is preserved by projection, but there is no implied dependency of the field on the record from which it was projected. Record construction also reflects this principle, preserving the field selections unchanged into the resulting record selection. But since this rule also constructs a partial value — the record itself — it must specify an availability on that output. The availability is set to $\alpha \sqcap \alpha'$, reflecting the dependency of the constructed container on both the constructing expression and the active argument match. The rules for nil, cons, integers and Booleans are similar, since they also construct values.

Hole cases. Environments have no special $\square$ form. However, a hole rule is needed to allow forward evaluation to continue in the event that e is $\square$; this is essential because subsequent steps may result in non-$\square$ outputs (for example by extracting non-$\square$ values from ρ). The rule is similar to the hole rules for $\nearrow_w$ and again can be understood operationally as using the information in T to expand $\square$ sufficiently for another rule to apply, with a result which is unique up to $\doteq$. In addition, application and record projection must accommodate the case where the selection on the closure or record being eliminated is represented by $\square$. In these rules $\nearrow_T \doteq$ is used to denote the relational composition of $\nearrow_T$ and $\doteq$.

Lemma 3.4 (Monotonicity of $\nearrow_T$). *Suppose* $T :: \boldsymbol{\rho}, \mathbf{e} \Rightarrow \mathbf{v}$ *with* $\rho, e, \alpha \nearrow_T v$ *and* $\rho', e', \alpha' \nearrow_T v'$. *If* $(\rho, e, \alpha) \sqsubseteq (\rho', e', \alpha')$ *then* $v \sqsubseteq v'$.

3.3 Backward Data Dependency

The backward dependency function $\searrow_T$ "rewinds" evaluation, turning output demand into input demand, with T guiding the analysis backward. We start with the auxiliary function $\hookleftarrow_w$ which is used for backward-analysing a pattern-match.

3.3.1 Backward Match. Figure 11 defines a family of *backward-match* functions $\hookleftarrow_w$ of type $(\mathrm{Sel}_{\boldsymbol{\rho},\boldsymbol{\kappa}}\,\mathcal{A}) \times \mathcal{A} \to \mathrm{Sel}_{\mathbf{v},\boldsymbol{\sigma}}\,\mathcal{A}$ for any $w :: \mathbf{v}, \boldsymbol{\sigma} \rightsquigarrow \boldsymbol{\rho}, \boldsymbol{\kappa}$. Backward-match rewinds the match witnessed by w, turning demand on the environment and continuation into demand on the value and eliminator that were originally matched. The additional input α represents the downstream demand placed on any resources that were constructed in the context of this match; $\hookleftarrow_w$ transfers this to the matched portion of $\mathbf{v}$, establishing a backwards link from resources produced to resources

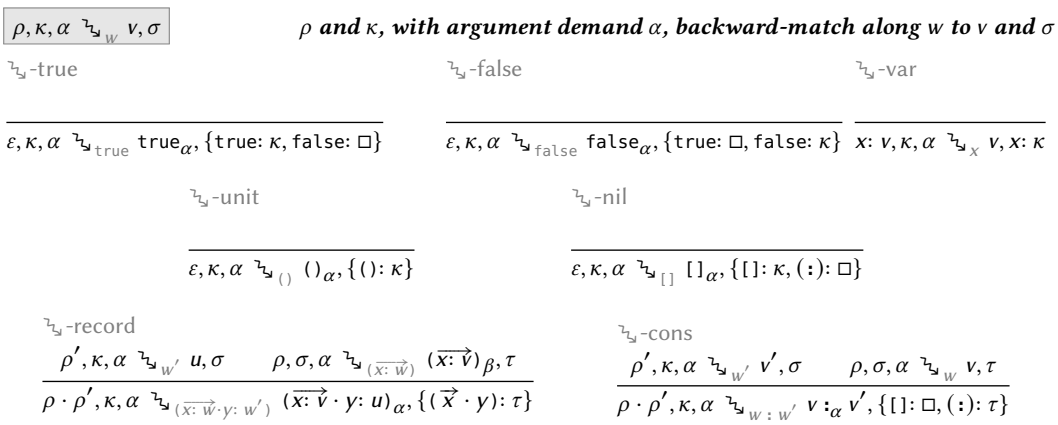


Fig. 11. Backward match

consumed in a given function context. We call α the *argument demand* since it represents the demand to be pushed backwards onto the matched part of a function argument.

In the variable case, the empty part of $\mathbf{v}$ was matched, so α is disregarded. The rule need only ensure that the demand v in the singleton environment $x: v$ is propagated backward. If a Boolean constant was matched, α becomes the demand on that constant, and κ, capturing the demand on the continuation, is used to construct the demand on the original eliminator, with $\square$ used to represent the absence of demand on the non-taken branch. (This use of $\square$ explains why matches w need only retain information about taken branches.) The nil case is similar.

For a cons match $w : w'$, we split the environment into ρ and ρ', using the fact that there is a unique well-typed decomposition. We then backward-match w and w' recursively to obtain v and v', representing the demand on the head and tail of the list. These are combined into the demand on the entire list, using α as the demand on the root cons node. The eliminator selection σ represents the demand on the interim eliminator used to match the tail, and τ the demand on the eliminator used to match the head; these are then combined into a demand on the eliminator used to match the whole list, with $\square$ again used to represent the absence of demand on the nil branch. Records are similar, except that there is only a single branch. The selection state β computed for the initial part of the record is an artefact of processing records recursively, and is disregarded.

Lemma 3.5 (Monotonicity of $\searrow_w$). *Suppose* $w :: \mathbf{v}, \boldsymbol{\sigma} \rightsquigarrow \boldsymbol{\rho}, \boldsymbol{\kappa}$, *with* $\rho, \kappa, \alpha \searrow_w v, \sigma$ *and* $\rho', \kappa', \alpha' \searrow_w v', \sigma'$. *If* $(\rho, \kappa, \alpha) \sqsubseteq (\rho', \kappa', \alpha')$ *then* $(v, \sigma) \sqsubseteq (v', \sigma)$.

3.3.2 Backward Evaluation. Figure 12 defines a family of *backward-evaluation* functions $\searrow_T$ of type $\mathsf{Sel}_{\mathbf{v}}\, \mathcal{A} \to (\mathsf{Sel}_{\boldsymbol{\rho},\mathbf{e}}\, \mathcal{A}) \times \mathcal{A}$ for any $T :: \boldsymbol{\rho}, \mathbf{e} \Rightarrow \mathbf{v}$. Backward evaluation rewinds T, using the output selection $v \in \mathsf{Sel}_{\mathbf{v}}\, \mathcal{A}$ to determine an input selection $(\rho, e) \in \mathsf{Sel}_{\boldsymbol{\rho},\mathbf{e}}\, \mathcal{A}$ and an argument demand $\alpha \in \mathcal{A}$ which will eventually be pushed back onto the argument of the dynamically innermost function call. (At the outermost level, where there are no active function calls, the argument demand is discarded.) The rules resemble those of the evaluation relation $\Rightarrow$ with inputs and outputs flipped. The general pattern is that each backward rule takes the join of the demand attached to any partial values constructed at that step, and the argument demand associated with any subcomputations, and passes it upwards as the new argument demand. The output environment is constructed similarly, by joining the demand flowing back through the environment copies used

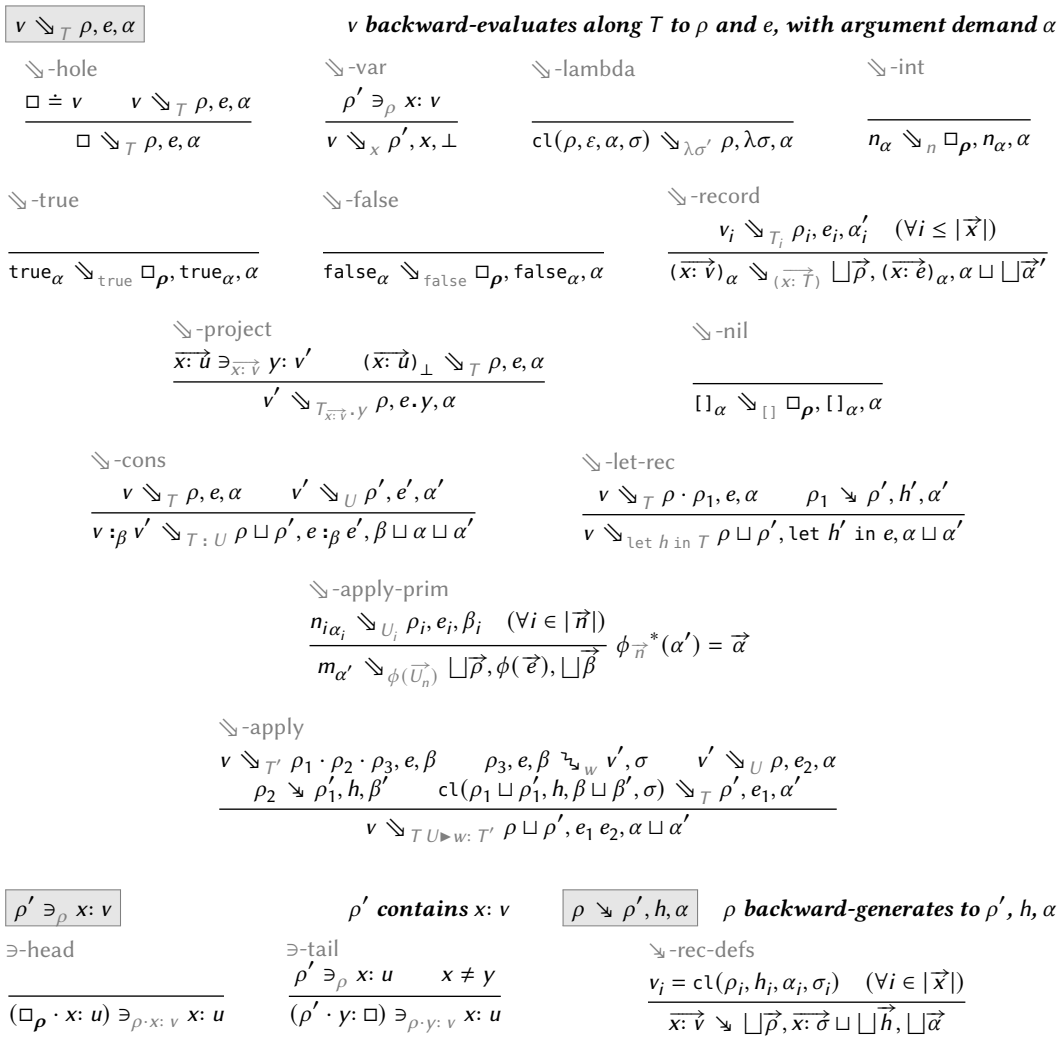


Fig. 12. Backward evaluation

to evaluate subcomputations. Demand is also attached to the source expression when it is the expression form responsible for the construction of a demanded value.

Function application. The application rule is where the argument demand is used and the function context changes, so we start here. The rule essentially runs the forward evaluation rule in reverse, using the trace T' to backward-evaluate the function body. The argument demand β associated with T' is the join of the demand on any resources constructed directly by that function invocation, and is transferred to the matched part of the function argument by the backward-match function $\curvearrowright_w$. The argument demand passed upwards into the enclosing function context is $\alpha \sqcup \alpha'$, representing the resources needed along T and U. The auxiliary function $\searrow_{\rho,h} : \mathrm{Sel}_{\rho'}\,\mathcal{A} \to (\mathrm{Sel}_{\boldsymbol{\rho},\mathbf{h}}\,\mathcal{A}) \times \mathcal{A}$ for any $\boldsymbol{\rho}, \mathbf{h} \twoheadrightarrow \boldsymbol{\rho}'$ defined at the bottom of Figure 12 is used to turn ρ_2, capturing the demand flowing back through any recursive uses of the function and any others with which it was mutually defined,

into information that can be merged back into the demand on the closure. The function $\searrow_{\rho,h}$ is also used in the letrec rule, which otherwise follows the general pattern described above.

Primitive application. Each primitive operation $\phi : \texttt{Int}^i \to \texttt{Int}$ must provide a backward-dependency function $\phi_{\vec{n}}{}^* : \mathcal{A} \to \mathcal{A}^i$ for every $\vec{n} \in \texttt{Int}^i$ which specifies how to turn the output selection α' on $\phi(\vec{n})$ into an input selection $\vec{a} \in \mathcal{A}^i$ on $\vec{n}$. The rule for primitive application uses this information to pair each argument n_i with its demand α_i and then backwards-evaluate the argument. The argument demand passed upward is the join of those arising from these subcomputations, and is unrelated to the execution of the primitive itself, similar to a function application. Here $\bigsqcup\vec{\beta}$ means the fold of $\sqcup$ (with unit $\bot$) over the sequence of selection states $\beta_1 \cdot .. \cdot \beta'_{|\vec{x}|}$. Environment demands $\vec{\rho} = \rho_1 \cdot .. \cdot \rho_{|\vec{n}|}$ are joined (pointwise) in a similar fashion.

Other rules. In the variable case, no partial values were constructed during evaluation and there are no subcomputations, so the argument demand is $\bot$, the unit for $\sqcup$. The returned environment selection demands v for the variable x and $\square$ for all other variables, using the family of *backwards lookup* functions $- \ni_\rho x\colon - $ of type $\mathsf{Sel}_{\mathbf{v}}\,\mathcal{A} \to \mathsf{Sel}_{\boldsymbol{\rho}}\,\mathcal{A}$ for any $x\colon \mathbf{v} \in \boldsymbol{\rho}$ also defined in Figure 12. (The output of the function is on the left in the relational notation.) For atomic values such as integers, Booleans and nil, the argument demand is simply the demand α associated with the constructed value, which is also attached to the corresponding expression, and the environment demand has $\square$ for every variable in the original environment $\boldsymbol{\rho}$, written $\square_{\boldsymbol{\rho}}$.

For closures, the argument demand is unpacked along with the other components, preserving any internal selections on ρ and σ. Composite values such as records and cons cells follow the general pattern; thus for records, the argument demands α'_i from the subcomputations are joined with the α on the record itself to produce the argument demand passed upward. Record projection never demands the record constructor itself, but simply promotes the field demand into a record demand, using $\ni_{\overrightarrow{x\colon \mathbf{v}}}$ to demand fields other than y with $\square$.

Hole rule. The hole rule, as elsewhere, ensures that the function is defined when v is $\square$, and it is easy to show that $\searrow_T$ preserves $\sqsubseteq$, and thus $\doteq$.

Lemma 3.6 (Monotonicity of $\searrow_T$). *Suppose* $T :: \boldsymbol{\rho}, \mathbf{e} \Rightarrow \mathbf{v}$ *with* $v \searrow_T \rho, e, \alpha$ *and* $v' \searrow_T \rho', e', \alpha'$. *If* $v \sqsubseteq v'$ *then* $(\rho, e, \alpha) \sqsubseteq (\rho', e', \alpha')$.

3.4 Round-Tripping Properties of $\nearrow_T$ and $\searrow_T$

We now establish more formally the round-tripping properties, alluded at the beginning of the section, that relate $\nearrow_T$ to $\searrow_T$. For the analyses to be coherent, we expect $\nearrow_T(\searrow_T(v))$ to produce a value selection $v' \sqsupseteq v$, and $\searrow_T(\nearrow_T(\rho, e))$ to produce an input selection $(\rho', e') \sqsubseteq (\rho, e)$. Pairs of (monotonic) functions $f : X \to Y$ and $g : Y \to X$ that are related in this way are called *Galois connections*. Galois connections generalise isomorphisms: f and g are not quite mutual inverses, but are the nearest to an inverse each can get to the other. We will present a visual example of some of these round-tripping properties in § 4.2; here we establish the relevant theorems.

Definition 3.7 (Galois connection). Suppose X and Y are sets equipped with partial orders $\leq_X$ and $\leq_Y$. Then monotonic functions $f : X \to Y$ and $g : Y \to X$ form a *Galois connection* $(f, g) : X \to Y$ iff $g(f(x)) \geq_X x$ and $f(g(y)) \leq_Y y$.

Galois connections are also adjoint functors between poset categories, with left and right adjoints f and g usually called the *lower* and *upper* adjoints, because f approximates an inverse of g from below, and g an inverse of f from above. Galois connections compose component-wise, so it is useful to think of them as having a type $X \to Y$, with the direction (by convention) given by the lower adjoint. If $\gamma : X \to Y$ is a Galois connection, we will write γ^* and γ_* for the lower and upper adjoints respectively; an important property we will return to is that γ^* preserves joins and γ_* preserves

meets. We now show that, for any $\mathcal{A}$, $\searrow_T$ and $\nearrow_T$ form a Galois connection (Theorem 3.11), by first establishing that the relevant auxiliary functions also form Galois connections.

Theorem 3.8 (Galois connection for pattern-matching). *Suppose* $w :: \mathbf{v}, \sigma \rightsquigarrow \rho, \kappa$. *Then* $(\searrow_w, \nearrow_w) : (\mathsf{Sel}_{\rho,\kappa}\,\mathcal{A}) \times \mathcal{A} \to \mathsf{Sel}_{\mathbf{v},\sigma}\,\mathcal{A}$ *is a Galois connection.*

Proof. See Appendix B.2. □

Lemma 3.9 (Galois connection for environment lookup). *Suppose* $x\colon \mathbf{v} \in \rho$. *Then* $(- \ni_\rho x\colon , \in_\rho x\colon -) : \mathsf{Sel}_{\mathbf{v}}\,\mathcal{A} \to \mathsf{Sel}_{\rho}\,\mathcal{A}$ *is a Galois connection.*

Proof. See Appendix B.3. □

Theorem 3.10 (Galois connection for recursive bindings). *Suppose* $\rho, \mathbf{h} \twoheadrightarrow \rho'$. *Then* $(\searrow_{\rho,\mathbf{h}}, \nearrow_{\rho,\mathbf{h}}) : \mathsf{Sel}_{\rho'}\,\mathcal{A} \to (\mathsf{Sel}_{\rho,\mathbf{h}}\,\mathcal{A}) \times \mathcal{A}$ *is a Galois connection.*

Proof. See Appendix B.4. □

We assume (rather than prove) that the backward and forward dependency functions ${\phi_{\vec{n}}}^*$ and $\phi_{\vec{n}*}$ provided for every primitive operation $\phi : \mathtt{Int}^i \to \mathtt{Int}$ and every $\vec{n}$ of length i form a Galois connection of type $\mathcal{A} \to \mathcal{A}^i$. Under this assumption the following holds.

Theorem 3.11 (Galois connection for evaluation). *Suppose* $T :: \rho, \mathbf{e} \Rightarrow \mathbf{v}$. *Then* $(\searrow_T, \nearrow_T) : \mathsf{Sel}_{\mathbf{v}}\,\mathcal{A} \to (\mathsf{Sel}_{\rho,\mathbf{e}}\,\mathcal{A}) \times \mathcal{A}$ *is a Galois connection.*

Proof. See Appendix B.5. □

Establishing that $(\searrow_T, \nearrow_T)$ is an adjoint pair might seem rather weak as a correctess property: it merely ensures that the two analyses are related in a sensible way, not that they actually capture any useful information. This is a familiar problem from other approximate analyses like type systems and model checking, where properties like soundness or completeness are essential but do not by themselves guarantee utility. One could certainly define versions of $\searrow_T$ and $\nearrow_T$ that are too coarse grained to be useful, yet still satisfy Theorem 3.11. However Galois connections do at least require that every tightening or tweak to the forward analysis is paired with a corresponding adjustment to the backward analysis, and vice-versa. In § 6 we consider how other ideas from provenance and program slicing might be adapted to provide additional correctness criteria.

4 DE MORGAN DEPENDENCIES FOR BRUSHING AND LINKING

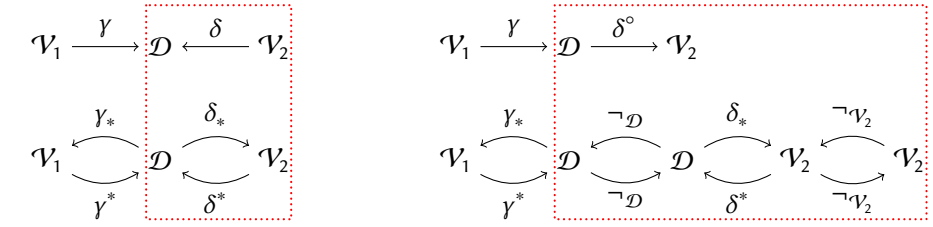
§ 3 addresses the first kind of question we motivated in the introduction (§ 1.1). In particular $\searrow_T$ can answer questions like: "what data is needed to compute this bar in a bar chart?", and indeed we were able to use our implementation to generate Figure 1. The second problem we set ourselves was how to link selections between *cognate* outputs, i.e. outputs computed from the same data (§ 1.2). This is called "brushing and linking" in data visualisation [Becker and Cleveland 1987], and has been extensive studied as an interaction paradigm, but with little emphasis on techniques for automation. Intuitively, the problem has a bidirectional flavour: one must consider how dependencies flow backward from a selection in one output to a selection v in the common data, and then forward from the selected data v to a corresponding selection in the other output. A natural question then is whether the analysis established in § 3 can supply the information required to support an automated solution.

An immediate problem is that the flavour of the forward dependency required here differs from that provided by the forward analysis $\nearrow_T$ defined in § 3.2. That was able to answer the question: what can we compute given only the data selected in v? But to identify the related data in another output, we must determine not what the input selection v is sufficient for, but what it is necessary

for: those parts of the other output that depend on v. In fact the question can be formulated as a kind of dual: what would we *not* be able to compute if the data selected in v were *unavailable*?

4.1 De Morgan Duality

Why $\nearrow_T$ is unsuitable as a forward dependency relation for linking cognate outputs can also be understood in terms of compositionality. Suppose $\mathcal{V}_1$ and $\mathcal{V}_2$ are the lattices of selections for two views computed from a shared input source, and $\mathcal{D}$ is the lattice of selections for the shared input. Using the procedure given in § 3, we can obtain two Galois connections $\gamma : \mathcal{V}_1 \to \mathcal{D}$ and $\delta : \mathcal{V}_2 \to \mathcal{D}$ as shown in Figure 13a. (The reader can ignore Figure 13b for the moment.)



(a) γ and δ cannot be composed

(b) Composing via De Morgan duality

Fig. 13. Dualising $\delta : \mathcal{V}_2 \to \mathcal{D}$ for composition with $\gamma : \mathcal{V}_1 \to \mathcal{D}$

Unfortunately, γ and δ are not composable, as their types makes clear. While the upper adjoint $\delta_* : \mathcal{D} \to \mathcal{V}_2$ has the correct type to compose with the lower adjoint $\gamma^* : \mathcal{V}_1 \to \mathcal{D}$, the result is not a Galois connection: δ_* preserves meets, whereas γ^* preserves joins. However, it turns out that if selections are closed under complement, we can derive an analysis of what is *necessary* for a given input selection from an analysis of what it is *sufficient* for. The effect is to invert δ, yielding a Galois connection δ° with a type that allows it to compose with γ. Then the composite $\delta^\circ \circ \gamma$ is a Galois connection linking $\mathcal{V}_1$ to $\mathcal{V}_2$ via $\mathcal{D}$, as shown in Figure 13b, offering a general mechanism for brushing and linking, with nice round-tripping properties. We now unpack this in more detail.

First we shift settings from the lattices used in § 3 to Boolean lattices (or Boolean algebras) $\mathcal{A} = \langle A, \top, \bot, \sqcap, \sqcup, \neg \rangle$, which are lattices equipped with an involution $\neg : \mathcal{A} \to \mathcal{A}$ called *complement*. Boolean algebras satisfy complementation laws $x \sqcap \neg x = \bot$ and $x \sqcup \neg x = \top$ and De Morgan laws $\neg x \sqcap \neg y = \neg(x \sqcup y)$ and $\neg x \sqcup \neg y = \neg(x \sqcap y)$. If $\mathcal{A}$ is a Boolean algebra, then $\mathsf{Sel}_{\mathsf{v}}\, \mathcal{A}$ is also a Boolean algebra, with the Boolean operations, and in particular $\neg_{\mathsf{v}} : \mathsf{Sel}_{\mathsf{v}}\, \mathcal{A} \to \mathsf{Sel}_{\mathsf{v}}\, \mathcal{A}$, defined pointwise. An additional distinguished value selection $\blacksquare$ serves as the negation of $\square$. The two-point lattice 2 we used to illustrate § 3 is also a Boolean algebra $\langle \{\mathsf{tt}, \mathsf{ff}\}, \mathsf{tt}, \mathsf{ff}, \wedge, \vee, \neg \rangle$ with $\neg$ corresponding to logical negation.

It is an easy consequence of the complementation and De Morgan laws that any meet-preserving operation $g : \mathcal{A} \to \mathcal{B}$ on Boolean algebras has a join-preserving De Morgan dual $g^\circ : \mathcal{A} \to \mathcal{B}$ given by $\neg_{\mathcal{B}} \circ g \circ \neg_{\mathcal{A}}$, and any join-preserving operation h has a meet-preserving De Morgan dual h° defined similarly. Moreover if h is the lower adjoint of g, then g° is the lower adjoint of h°. Thus Galois connections on Boolean algebras also admit a (contravariant) notion of De Morgan duality, defined component-wise.

Definition 4.1 (De Morgan dual of a Galois connection). Suppose $\mathcal{A}$ and $\mathcal{B}$ are Boolean algebras and $\gamma : \mathcal{A} \to \mathcal{B}$ is a Galois connection (γ^*, γ_*). Define the *De Morgan dual* γ° of γ to be the Galois connection $({\gamma_*}^\circ, {\gamma^*}^\circ) : \mathcal{B} \to \mathcal{A}$.

```
let zero n = const n;
    wrap n n_max = ((n - 1) `mod` n_max) + 1;
    extend n = min (max n 1);
    nth2 i j xss = nth (j - 1) (nth (i - 1) xss);

let convolve image kernel method =
    let ((m, n), (i, j)) = (dims image, dims kernel);
        (half_i, half_j) = (i `quot` 2, j `quot` 2);
        area = i * j
    in  ⟨ let weightedSum = sum [
            image!(x, y) * kernel!(i' + 1, j' + 1)
          | (i', j') ← range (0, 0) (i - 1, j - 1),
            let x = method (m' + i' - half_i) m,
            let y = method (n' + j' - half_j) n,
            x ≥ 1, x ≤ m, y ≥ 1, y ≤ n
        ] in weightedSum `quot` area
        | (m', n') in (m, n) ⟩;
```

```
let emboss = [[-2, -1, 0],
              [-1,  1, 1],
              [ 0,  1, 2]];
    filter = ⟨ nth2 i j emboss
             | (i, j) in (3, 3) ⟩;
    image' = [[15, 13,  6, 9, 16],
              [12,  5, 15, 4, 13],
              [14,  9, 20, 8,  1],
              [ 4, 10,  3, 7, 19],
              [ 3, 11, 15, 2,  9]];
    image = ⟨ nth2 i j image'
            | (i, j) in (5, 5) ⟩
in convolve image filter zero
```

Fig. 14. Matrix convolution example, with methods `zero`, `wrap` and `extend` for dealing with boundaries

Dualising a Galois connection flips the direction of the arrow by swapping the roles of the upper and lower adjoints. So while $\gamma : \mathcal{A} \to \mathcal{B}$ and $\delta : \mathcal{C} \to \mathcal{B}$ are not composable, γ and $\delta^\circ : \mathcal{B} \to \mathcal{C}$ are, and the composition is achieved by transforming δ_* from something which determines what we can compute with v into something which determines what we cannot compute without v. This offers a principled basis for an automated brushing and linking feature between cognate computations T and U. When the user selects part of the output of T, we can use $\searrow_T$ to compute the needed data v, and then use $\nearrow_U{}^\circ$ to compute the parts of the output of U that depend on v. This is the approach implemented in Fluid, and we used this to generate Figure 2 in § 1.2.

4.2 Example: Matrix Convolution

We now illustrate the $(\nearrow_T{}^\circ, \searrow_T{}^\circ)$ Galois connection, contrasting it with $(\searrow_T, \nearrow_T)$, using an example which computes the convolution of a 5×5 matrix with a 3×3 kernel. Convolution has an intuitive dependency structure and the values involved have an easy visual presentation, making it useful for conveying the flavour of the four distinct (but connected) dependency relations that arise in the framework. The source code for the example is given in Figure 14, and shows the `convolve` function, plus `zero`, `wrap` and `extend` which provide different methods for handling the boundaries of the input matrix. The angle-bracket notation is used to construct matrices, which were omitted from § 2. (The formal treatment is similar to records.)

Fluid was used to generate the diagrams in Figure 15, which show the four dependency relations and two of their four possible round-trips. Figure 15a shows the $(\searrow_T, \nearrow_T)$ Galois connection defined in § 3.4. In the upper figure, the user selects (in green) the output cell at position $(2, 2)$ (counting rows downwards from 1). This induces a demand (via the lower adjoint $\searrow_T$) on the input matrix `image` and the kernel `filter`, revealing (in blue) that the entire kernel was needed to compute the value 1, but only some of the input matrix. In particular the elements at $(1, 3)$ and $(3, 1)$ in `image` were not needed, because of zeros present in `filter`. If we then "round-trip" that input selection, computing the corresponding availability on the output using the upper adjoint $\nearrow_T$, the green selection grows: it turns out that the data needed to make $(2, 2)$ available are sufficient to make $(1, 1)$ available as well.

(a) Galois dependency ($\searrow_T, \nearrow_T$) (b) De Morgan dual ($\nearrow_T{}^\circ, \searrow_T{}^\circ$)

Fig. 15. Upper and lower pairs are dual; left and right pairs are adjoint

Figure 15b shows the De Morgan dual ($\nearrow_T{}^\circ, \searrow_T{}^\circ$). In the upper part of the figure, the user selects (green) kernel cell $(1, 2)$ to see the output cells that depend on it. This is computed using the De Morgan dual $\nearrow_T{}^\circ$. First we negate the input selection, marking $(1, 2)$ as unavailable, and all other inputs as available. Then we forward-analyse with $\nearrow_T$ to determine that with this data selection, we can only compute the top row of the output. (If it seems odd that we can compute even the top row, notice that the example uses the method `zero` for dealing with boundaries; `wrap` or `extend` would give a different behaviour.) Then we negate that top row selection to produce the (blue) output selection shown in the figure. These are exactly the output cells which depend on kernel cell $(1, 2)$ in the sense that they cannot be computed if that input is unavailable.

We can then round-trip this output selection using the De Morgan dual $\searrow_T{}^\circ$. We first negate the blue output selection (selecting the top row of the output again), and then use $\searrow_T$ to determine the needed inputs, which turn out to be the top two rows of `image`, and the top row of `filter`. Negating again produces the green output selection shown in the lower figure. Thus the backwards De Morgan dual computes the inputs that would *not* be needed if the selected outputs were not needed: more economically, the inputs that are *only* needed for the selected output. Here the round-trip reveals that if kernel cell $(1, 2)$ is unavailable, then the entire top row of the kernel might as well have been unavailable too, and similarly for the bottom 3 rows of the input.

4.3 Relationship to Galois Slicing

The De Morgan dual puts us in a better position to consider the relationship between the present system and earlier work on *Galois slicing*, a program slicing technique that has been explored for pure functional programs [Perera 2013; Perera et al. 2012], functional programs with effects [Ricciotti et al. 2017], and π-calculus [Perera et al. 2016]. We consider other related work in § 6.1.

Galois slicing operates on lattices of *slices*, which are programs (or values) where parts deemed irrelevant are replaced by a hole $\square$. (If we think of the notion of selection defined in § 3.1.1 as picking out a subset of the paths in a term, then slices resembles selections which are prefix-closed, meaning that if a given path in a term is selected, then so are all of its prefixes.) For a fixed computation, a meet-preserving *forward-slicing* function is defined which takes input slices to output slices,

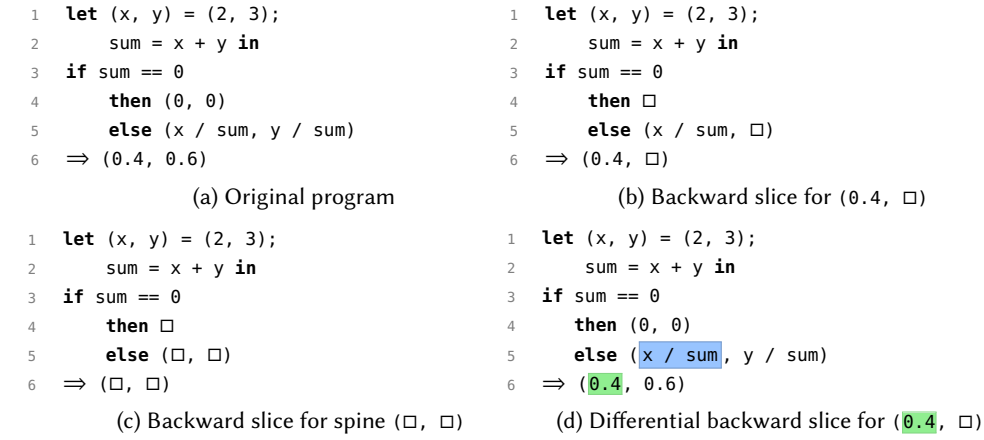


Fig. 16. Differential Galois slicing selects input (blue) needed *only* for selected output (green)

discarding parts which cannot be computed because the needed input is not present, plus a join-preserving *backward-slicing* function taking output slices to input slices, retaining the parts needed for the output slice. For example Figure 16a shows a computation with output `(0.4, 0.6)`, and Figure 16b gives the backward slice for output slice `(0.4, □)`. Forward and backward slicing, for a given computation, form a Galois connection, giving the analyses the nice round-tripping properties we motivated in § 3.4.

Unfortunately, the notion of slice does not lend itself to computing dependencies where the needed input or output is a proper part of a value, such as a component of a tuple. *Differential* slicing [Perera et al. 2012] improves on this by using Galois slicing to compute a pair of input slices (e, e') for a pair of output slices (v, v') where $v \sqsubseteq v'$. By monotonicity, $e \sqsubseteq e'$. This can be used to compute a (differential) slice for an arbitrary subtree, by setting v to be the "spine" of the original output up to the location of the subtree, and v' to be v with the subtree of interest plugged back in. Here we could focus on the value `0.4` in the output by computing the backward slice for `(□, □)` (Figure 16c) and then comparing it with the backward slice for `(0.4, □)`, generating a differential slice where the parts that are different are highlighted (Figure 16d). But although it supports a notion of selection which is closer to what we need, the differential slice highlights only the program parts that are needed *exclusively* by the selected output, and as such underapproximates the dependency information needed for data linking. (In fact differential slicing is similar to the De Morgan dual $\searrow_T{}^{\circ}$.) Because is this example `2` and `3` are needed to compute the spine as well (in order to decide which conditional branch to execute), they are excluded from the differential slice, whereas our backward analysis $\searrow_T$ is able to directly determine that both `2` and `3` are needed to compute `0.4`.

5 GALOIS CONNECTIONS FOR DESUGARING

Elaborating a richer surface language into a simpler core is a common pattern with well known benefits. It can, however, make it harder to express certain information to the programmer in terms of the surface language. We face this problem with the analysis in § 3, which links outputs not only to inputs, but also to expressions responsible for introducing data. We could use this information in an IDE to link structured outputs to relevant code fragments, but only if we are able to map term selections back to the surface program. We now sketch a bidirectional desugaring procedure which addresses this, and which composes with the Galois dependency analysis defined in § 3.

	Identifier	
$x, y ::=$	...	
	$\oplus$	operator name
	Surface term	
$s, t ::=$	...	
	$(\oplus)$	first-class operator
	$s \oplus s'$	binary application
	$\texttt{let}\ \overrightarrow{g}\ \texttt{in}\ s$	recursive functions
	$\texttt{if}\ s\ \texttt{then}\ s\ \texttt{else}\ s$	if
	$\texttt{match}\ s\ \texttt{as}\ \overrightarrow{p = s}$	match
	$\texttt{let}\ p = s\ \texttt{in}\ s$	structured let
	$[_\alpha\ s\ r$	non-empty list
	$[\ s\ ..\ s\ ]$	list enum
	$[\ s \mid \overrightarrow{q}\ ]_\alpha$	list comprehension
	List rest term	
$r ::=$	$]_\alpha$	end
	$,_\alpha\ s\ r$	cons

	Recursive function	
$g ::=$	$x\texttt{:}\ \overrightarrow{c}$	
	Clause	
$c ::=$	$\overrightarrow{p}\ \texttt{=}\ s$	
	Pattern	
$p ::=$	x	variable
	$(x\texttt{:}\ \overrightarrow{p})$	record
	$[\,]$	nil
	$p\ \texttt{:}\ p$	cons
	$[\ p\ o$	non-empty list
	List rest pattern	
$o ::=$	$]$	end
	$,\ p\ o$	cons
	Qualifier	
$q ::=$	s	guard
	$\texttt{let}\ p = s$	declaration
	$p \leftarrow s$	generator

Fig. 17. Syntax for surface language, with selection states

5.1 Surface Language Syntax

The surface language, Fluid, extends the core syntax with list notation $[s,\ldots,s']$, Haskell 98-style list comprehensions [Jones 2003], list enumerations, first-class primitives and piecewise function definitions and pattern-matching, as shown in Figure 17. Typing rules are given in Appendix A, Figures 20 and 21. We attach selection states α to surface terms s, t that desugar to core terms with selections, and let $\mathbf{s}$, $\mathbf{t}$ range over "raw" surface terms, which are isomorphic to the term selections where the type of selection states is the unit lattice 1.

Figure 18 shows how the end-to-end mapping would appear to a user. (For illustrative purposes the library function `map` and some raw data are included in the same source file.) On the left, the user selects a cons cell (green) in the output; by backwards evaluating and then backwards desugaring, we are able to highlight the list comprehension, the cons in the second clause of `map`, and both occurrences of the constant `"Hydro"`. These last two are highlighted because the selected cons cell was constructed by eliminating a Boolean that was in turn constructed by the primitive == operator, which consumed the two strings. The user might then conjecture that the two occurrences of `"Geo"` were somehow responsible for the inclusion of the third cons cell in the output; they can confirm this by making the green selection on the right. (Highlighting == too would clearly be helpful here; we discuss this possibility in § 6.1.) The grey selection is included to contrast the cons highlighting with the data demanded by the list elements themselves, which is quite different.

5.2 Forward Desugaring

To define the forward evaluation function $\nearrow_T$ in § 3.2, we performed a regular evaluation using $\Rightarrow$ to obtain a trace T, and then defined $\nearrow_T$ by recursion over T, with T guiding the analysis in the presence of $\Box$. There are no holes in the surface language, so we can take a simpler approach, defining a single *forward desugaring* relation $\nearrow$, and then showing that for every raw surface term $\mathbf{t} \nearrow \mathbf{e}$, there is a monotonic function $\nearrow_t : \mathsf{Sel}_\mathbf{t}\,\mathcal{A} \to \mathsf{Sel}_\mathbf{e}\,\mathcal{A}$, which is simply $\nearrow$ domain-restricted to $\mathsf{Sel}_\mathbf{t}\,\mathcal{A}$. The full definition of $\nearrow$ is given in Appendix A ; Figure 19 gives a representative selection of the rules.

The definition follows a similar pattern to $\nearrow_T$. At each step, we take the meet of the availability on any parts of s being consumed at that step, and use that as the availability of any parts of e being generated at that step. Thus the rules for list notation simply transfer the selection state α on the opening and closing brackets $[_\alpha$ and $]_\alpha$ to the corresponding cons and nil of the resulting list, and those on intervening delimiters $,_\alpha$ to the corresponding cons. List comprehensions $[\, s \mid \overrightarrow{q} \,]_\alpha$ have a rule for each kind of qualifier q at the head of $\overrightarrow{q}$, plus a rule for when $\overrightarrow{q}$ is ε. The general pattern is to push the α on the comprehension itself through recursively, so it ends up on all core terms generated during its elaboration: in particular the `false` branch when q is a guard, and the singleton list when $\overrightarrow{q}$ is empty. Auxiliary relations $\nearrow$ and $\nearrow_p$ (defined in Appendix A, Figures 24 and 25) transfer availability on guards and generators onto the eliminators they elaborate into.

5.3 Backward Desugaring

The backwards analysis is then defined as a family of *backward desugaring* functions $\searrow_t : \mathsf{Sel}_\mathbf{e}\,\mathcal{A} \to \mathsf{Sel}_\mathbf{t}\,\mathcal{A}$ for any $\mathbf{t} \nearrow \mathbf{e}$, with the raw surface term $\mathbf{t}$ guiding the analysis backwards. (The role of $\mathbf{t}$ in disambiguating the backwards rules should be clear if you consider that e typically matches multiple rules but only one for a given $\mathbf{t}$.) Figure 19 gives some representative rules; the full definition is given in Appendix A To reverse a desugaring step, we take the join of the demand on any parts of e which were constructed at this step, and use that as the demand on the parts of s which were consumed at this step, turning demand on the core term into (minimal) demand on the surface term. Thus the effect of the list comprehension rules and auxiliary judgements is to set the demand on the comprehension itself to be the join of the demand of all the syntax generated during the elaboration of the comprehension, using auxiliary judgments $\searrow_p$ and $\searrow_p$ (Appendix A, Figures 28 and 27) to transfer demand from eliminators back onto the guards and generators.

5.4 Round-Tripping Properties and Compositionality

It is easy to verify that $\nearrow_t$ and $\searrow_t$ are monotonic. Moreover they form an adjoint pair.

Theorem 5.1 (Galois connection for desugaring). *Suppose $t \nearrow e$. Then $(\searrow_t, \nearrow_t) : \mathsf{Sel}_\mathbf{e}\,\mathcal{A} \to \mathsf{Sel}_\mathbf{t}\,\mathcal{A}$ is a Galois connection.*

Proof. See Appendix C.2. □

```
let map f [] = [];
    map f (x : xs) = f x : map f xs;
let data = [
   { energyType: "Bio", output: 6.2 },
   { energyType: "Hydro", output: 260 },
   { energyType: "Solar", output: 19.9 },
   { energyType: "Wind", output: 91 },
   { energyType: "Geo", output: 14.4 }
];
let xs = [ row.output
   | type ⟵ ["Hydro", "Solar", "Geo"],
     row ⟵ data, row.energyType == type
] in
map (fun x ⟶ floor (x / sum xs * 100)) xs
⟹ (88 : (6 : (4 : [])))
```

```
let map f [] = [];
    map f (x : xs) = f x : map f xs;
let data = [
   { energyType: "Bio", output: 6.2 },
   { energyType: "Hydro", output: 260 },
   { energyType: "Solar", output: 19.9 },
   { energyType: "Wind", output: 91 },
   { energyType: "Geo", output: 14.4 }
];
let xs = [ row.output
   | type ⟵ ["Hydro", "Solar", "Geo"],
     row ⟵ data, row.energyType == type
] in
map (fun x ⟶ floor (x / sum xs * 100)) xs
⟹ (88 : (6 : (4 : [])))
```

Fig. 18. Source selections (blue) resulting from selecting different list cells (green)

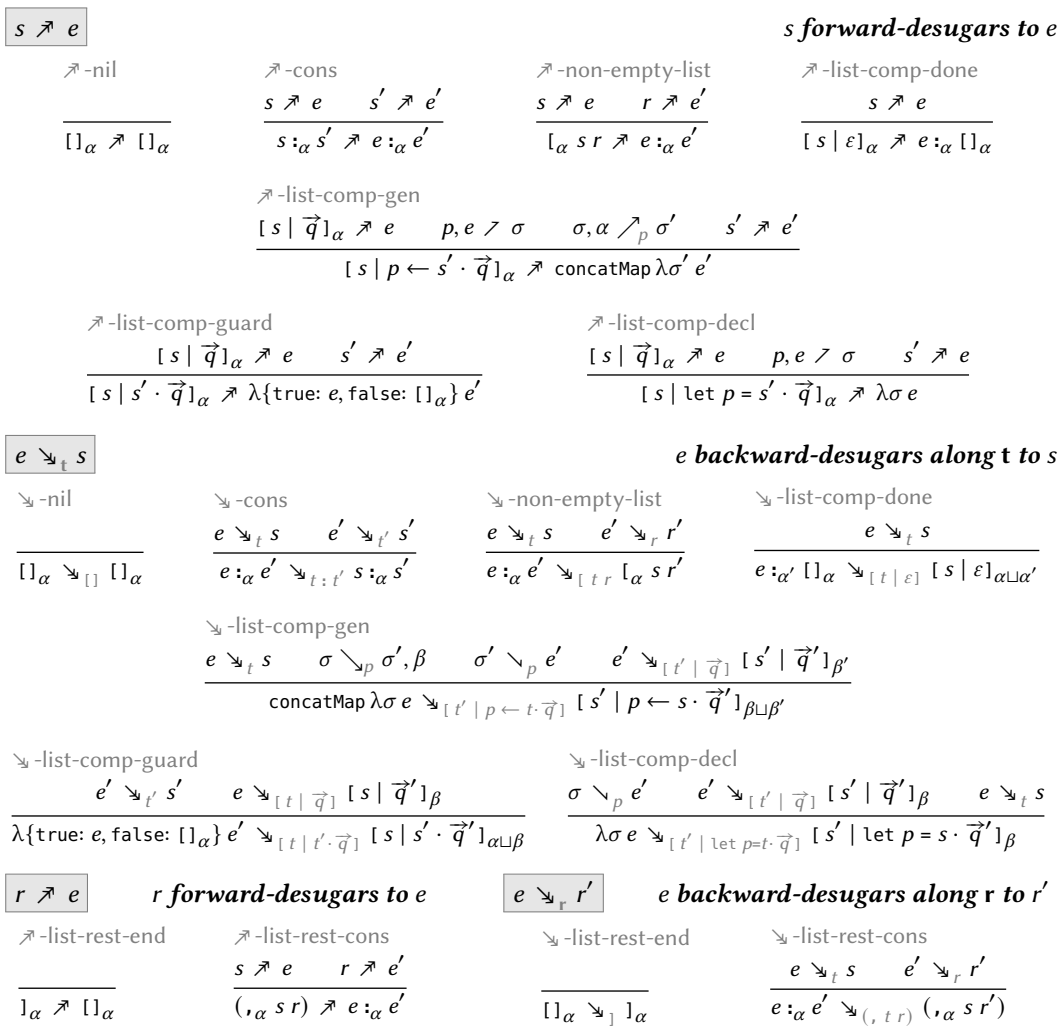


Fig. 19. Forwards and backwards desugaring (selected rules only)

The $(\searrow_t, \nearrow_t)$ Galois connection readily composes with $(\searrow_t, \not\nearrow_t)$ to produce surface-language selections like the ones shown in Figure 18. This is useful, although somewhat monolithic. In future work we will investigate techniques for backwards desugaring at arbitrary steps in the computation, perhaps by interleaving desugaring with execution in the style of Pombrio and Krishnamurthi [2014], as well as presenting selections on intermediate values (such as lists) in the surface language, even though they were not obtained via desugaring.

6 CONCLUSION

Our research was motived by the goal of making computational outputs which are automatically able to reveal how they relate to data in a fine-grained way. A casual reader who wants to understand or fact-check a chart, or a scientist evaluating another's work, should be able to do so by interacting directly with an output. Recent work by Walny et al. [2019] suggests that developers would also

benefit from such a feature while implementing visualisations, for example to check whether a quantity is represented by diameter or area in a bubble chart.

Galois connections provide an appealing setting for this problem because of their elegant round-tripping properties. However, existing dynamic analysis techniques based on Galois connections do not lend themselves to richly structured outputs like visualisations and matrices. We presented an approach that allows focusing on arbitrary substructures, which also means data selections can be inverted. This enables linking not just of outputs to data, but of outputs to other outputs, providing a mathematical basis for a widely used (but so far ad hoc) feature in data visualisation. We implemented our approach in Fluid, a realistic high-level functional programming language.

6.1 Other Related Work and Future Directions

We close by considering some limitations and opportunities in the context of other related work. Galois slicing [Perera et al. 2012, 2016; Ricciotti et al. 2017] was considered in § 4.3.

Executable slicing. Executable slices [Hall 1995] are programs with some parts removed, but which are still executable. Our approach computes data selections, not executable slices, but such a notion has obvious relevance in data science: "explaining" part of a result should (arguably) entail being able to recompute it. *Expression provenance* [Acar et al. 2012] explains how primitive values are computed using only primitive operations; however, this still omits crucial information, and does not obviously generalise to structured outputs. Work on executable slicing in term rewriting [Field and Tip 1998] could perhaps be adapted to structured data and combined with dependency tracking for higher-order data (§ 3.1).

Dynamic program analysis. Dynamic analysis techniques like dataflow analysis [Chen and Poole 1988] and taint tracking [Reps et al. 1995] tend to focus on variables, rather than parts of structured values, and lack round-tripping properties; Galois dependencies have a clear advantage here. A limitation of dynamic techniques which is shared by our approach is that they can usually only reveal *that* certain dependencies arise, not *why*, which requires analysing path conditions [Hammer et al. 2006]. In a data science setting this would clearly be valuable too, and it would be interesting to see if the benefits of the Galois framework can be extended to techniques for computing dynamic path conditions.

Brushing and linking. Brushing and linking has been extensive studied in the data visualisation community [Becker and Cleveland 1987; McDonald 1982], but although Roberts and Wright [2006] argued it should be ubiquitous, no automated method of implementation has been proposed to date. Geospatial applications like GeoDa [Anselin et al. 2006] hard-code view coordination features into specific views, and libraries like d3.js and Plotly support ad hoc linking mechanisms, with varying degrees of programmer effort required. No existing approach provides automation or round-tripping guarantees, or is able to provide data selections explaining why visual selections are linked.

Data provenance in data visualisation. A recent vision paper by Psallidas and Wu [2018] is the only work we are aware of that proposes that brushing and linking, and related view cooordination features like cross-filtering, can be understood in terms of data provenance. In a relational (query processing) setting, where the relevant notion of provenance is lineage, they propose backward-analysing to data, and then forward-analysing to another view, although again without the round-tripping features of Galois connections. Moreover theirs is primarily a concept paper, proposing a research programme, rather than solving a specific problem.

Acknowledgements. Perera and Petricek were supported by The UKRI Strategic Priorities Fund under EPSRC Grant EP/T001569/1, particularly the *Tools, Practices and Systems* theme within that

grant, and by The Alan Turing Institute under EPSRC grant EP/N510129/1. Wang was supported by *Expressive High-Level Languages for Bidirectional Transformations*, EPSRC Grant EP/T008911/1.

REFERENCES

Umut A. Acar, Amal Ahmed, James Cheney, and Roly Perera. 2012. A Core Calculus for Provenance. In *Proceedings of the First International Conference on Principles of Security and Trust* (Tallinn, Estonia) *(POST '12)*. Springer-Verlag, Berlin, Heidelberg, 410–429. https://doi.org/10.1007/978-3-642-28641-4_22

Luc Anselin, Ibnu Syabri, and Youngihn Kho. 2006. GeoDa: An Introduction to Spatial Data Analysis. *Geographical Analysis* 38, 1 (2006), 5–22. https://doi.org/10.1111/j.0016-7363.2005.00671.x

Richard A. Becker and William S. Cleveland. 1987. Brushing Scatterplots. *Technometrics* 29, 2 (May 1987), 127–142. https://doi.org/10.1080/00401706.1987.10488204

Richard Bird and Lambert Meertens. 1998. Nested datatypes. In *Mathematics of Program Construction*, Johan Jeuring (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 52–67.

Gérard Boudol and Ilaria Castellani. 1989. Permutation of transitions: An event structure semantics for CCS and SCCS. In *Linear Time, Branching Time and Partial Order in Logics and Models for Concurrency*, J.W. Bakker, W.-P. Roever, and G. Rozenberg (Eds.). Lecture Notes in Computer Science, Vol. 354. Springer, 411–427. https://doi.org/10.1007/BFb0013028

Nadieh Bremer and Marlieke Ranzijn. 2015. Urbanization in East Asia between 2000 and 2010. http://nbremer.github.io/urbanization/.

Peter Buneman, Sanjeev Khanna, and Wang-Chiew Tan. 2001. Why and Where: A Characterization of Data Provenance. In *Proceedings of the 8th International Conference on Database Theory (ICDT '01)*. Springer-Verlag, London, UK, 316–330.

TY Chen and PC Poole. 1988. Dynamic dataflow analysis. *Information and Software Technology* 30, 8 (1988), 497–505. https://doi.org/10.1016/0950-5849(88)90146-2

Richard H. Connelly and F. Lockwood Morris. 1995. A generalization of the trie data structure. *Mathematical Structures in Computer Science* 5, 3 (1995), 381–418. https://doi.org/10.1017/S0960129500000803

A. De Lucia, A.R. Fasolino, and M. Munro. 1996. Understanding function behaviors through program slicing. In *WPC '96. 4th Workshop on Program Comprehension*. 9–18. https://doi.org/10.1109/WPC.1996.501116

John Field and Frank Tip. 1998. Dynamic Dependence in Term Rewriting Systems and its Application to Program Slicing. *Information and Software Technology* 40, 11–12 (November/December 1998), 609–636.

Jeremy Gibbons. 2017. APLicative Programming with Naperian Functors. In *European Symposium on Programming (Lecture Notes in Computer Science, Vol. 10201)*, Hongseok Yang (Ed.). 568–583. https://doi.org/10.1007/978-3-662-54434-1_21

Sebastian Graf, Simon Peyton Jones, and Ryan G Scott. 2020. Lower your guards: a compositional pattern-match coverage checker. *Proceedings of the ACM on Programming Languages* 4, ICFP (2020), 1–30.

Robert J. Hall. 1995. Automatic extraction of executable program subsets by simultaneous dynamic program slicing. *Automated Software Engineering* 2 (1995), 33–53. https://doi.org/10.1007/BF00873408

Christian Hammer, Martin Grimme, and Jens Krinke. 2006. Dynamic path conditions in dependence graphs. *Proceedings of the ACM SIGPLAN Symposium on Partial Evaluation and Semantics-Based Program Manipulation*, 58–67. https://doi.org/10.1145/1111542.1111552

Ralf Hinze. 2000. Generalizing generalized tries. *Journal of Functional Programming* 10, 4 (2000), 327–351. https://doi.org/10.1017/S0956796800003713

Simon L. Peyton Jones. 2003. Haskell 98: Introduction. *Journal of Functional Programming* 13, 1 (2003), 0–6.

Gary A. Kildall. 1973. A Unified Approach to Global Program Optimization. In *Proceedings of the 1st Annual ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages* (Boston, Massachusetts) *(POPL '73)*. Association for Computing Machinery, New York, NY, USA, 194–206. https://doi.org/10.1145/512927.512945

John Alan McDonald. 1982. *Interactive graphics for data analysis*. Ph.D. Dissertation.

Greg Miller. 2006. A Scientist's Nightmare: Software Problem Leads to Five Retractions. *Science* 314, 5807 (2006), 1856–1857. https://doi.org/10.1126/science.314.5807.1856

James Newsome and Dawn Song. 2005. Dynamic taint analysis for automatic detection, analysis, and signature generation of exploits on commodity software. In *Network and Distributed Systems Security Symposium*.

Roland Perera. 2013. *Interactive Functional Programming*. Ph.D. Dissertation. University of Birmingham, Birmingham, UK. http://etheses.bham.ac.uk/4209/.

Roly Perera, Umut A. Acar, James Cheney, and Paul Blain Levy. 2012. Functional Programs That Explain Their Work. In *Proceedings of the 17th ACM SIGPLAN International Conference on Functional Programming* (Copenhagen, Denmark) *(ICFP '12)*. ACM, New York, NY, USA, 365–376. https://doi.org/10.1145/2364527.2364579

Roly Perera, Deepak Garg, and James Cheney. 2016. Causally Consistent Dynamic Slicing. In *Concurrency Theory, 27th International Conference, CONCUR '16 (Leibniz International Proceedings in Informatics (LIPIcs))*, Josée Desharnais and Radha Jagadeesan (Eds.). Schloss Dagstuhl–Leibniz-Zentrum für Informatik, Dagstuhl, Germany. https://doi.org/10.

4230/LIPIcs.CONCUR.2016.18

Justin Pombrio and Shriram Krishnamurthi. 2014. Resugaring: Lifting Evaluation Sequences through Syntactic Sugar. *SIGPLAN Notices* 49, 6 (Jun 2014), 361–371. https://doi.org/10.1145/2666356.2594319

Fotis Psallidas and Eugene Wu. 2018. Provenance for Interactive Visualizations. In *Workshop on Human-In-the-Loop Data Analytics (HILDA 2018)*. ACM.

Thomas Reps, Susan Horwitz, and Mooly Sagiv. 1995. Precise Interprocedural Dataflow Analysis via Graph Reachability. In *Proceedings of the 22nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages* (San Francisco, California, USA) *(POPL '95)*. Association for Computing Machinery, New York, NY, USA, 49–61. https://doi.org/10.1145/199448.199462

Wilmer Ricciotti, Jan Stolarek, Roly Perera, and James Cheney. 2017. Imperative Functional Programs That Explain Their Work. *Proceedings of the ACM on Programming Languages* 1, ICFP, Article 14 (2017), 28 pages. https://doi.org/10.1145/3110258

J. C. Roberts and M. A. E. Wright. 2006. Towards Ubiquitous Brushing for Information Visualization. In *Tenth International Conference on Information Visualisation (IV'06)*. 151–156. https://doi.org/10.1109/IV.2006.113

A. Sabelfeld and A. C. Myers. 2003. Language-Based Information-Flow Security. *IEEE Journal on Selected Areas in Communications* 21, 1 (Jan 2003), 5–19. https://doi.org/10.1109/JSAC.2002.806121

Jacob VanderPlas, Brian E. Granger, Jeffrey Heer, Dominik Moritz, Kanit Wongsuphasawat, Arvind Satyanarayan, Eitan Lees, Ilia Timofeev, Ben Welsh, and Scott Sievert. 2018. Altair: Interactive Statistical Visualizations for Python. *The Journal of Open Source Software* 3, 32 (2018). https://doi.org/10.21105/joss.01057

Jagoda Walny, Christian Frisson, Mieka West, Doris Kosminsky, Søren Knudsen, Sheelagh Carpendale, and Wesley Willett. 2019. Data Changes Everything: Challenges and Opportunities in Data Visualization Design Handoff. *IEEE Transactions on Visualization and Computer Graphics* PP (08 2019), 1–1. https://doi.org/10.1109/TVCG.2019.2934538

Mark Weiser. 1981. Program slicing. In *Proceedings of the 5th International Conference on Software Engineering* (San Diego, California, USA) *(ICSE '81)*. IEEE Press, Piscataway, NJ, USA, 439–449. https://doi.org/10.5555/800078.802557

$\boxed{\Gamma \vdash \overrightarrow{g} : \Delta}$

$$\frac{\Gamma \cdot \Delta \vdash \overrightarrow{c_i} : A_i \to B_i \quad (\forall i \le j)}{\Gamma \vdash x_1 \colon \overrightarrow{c_1} \cdot \ldots \cdot x_j \colon \overrightarrow{c_j} : \Delta} \; \Delta = \overrightarrow{x \colon A \to B}$$

$\boxed{\Gamma \vdash s : A}$

$$\frac{}{\Gamma \vdash (\oplus) : A} \; \oplus : A \in \Gamma \qquad \frac{\Gamma \vdash s : \mathtt{Int} \qquad \Gamma \vdash s' : \mathtt{Int}}{\Gamma \vdash s \oplus s' : \mathtt{Int}} \; \oplus : \mathtt{Int} \times \mathtt{Int} \to \mathtt{Int} \in \Gamma$$

$$\frac{\Gamma \vdash \overrightarrow{g} : \Delta \qquad \Gamma \cdot \Delta \vdash s : A}{\Gamma \vdash \mathtt{let}\ \overrightarrow{g}\ \mathtt{in}\ s : A} \qquad \frac{\Gamma \vdash s : \mathtt{Bool} \qquad \Gamma \vdash s_1 : A \qquad \Gamma \vdash s_2 : A}{\Gamma \vdash \mathtt{if}\ s\ \mathtt{then}\ s_1\ \mathtt{else}\ s_2 : A}$$

$$\frac{\Gamma \vdash s : A \qquad \Gamma \vdash \overrightarrow{c} : A \to B}{\Gamma \vdash \mathtt{match}\ s\ \mathtt{as}\ \overrightarrow{c} : B} \qquad \frac{p : A \dashv \Gamma' \qquad \Gamma \vdash s : A \qquad \Gamma \cdot \Gamma' \vdash s' : B}{\Gamma \vdash \mathtt{let}\ p = s\ \mathtt{in}\ s' : B}$$

$$\frac{\Gamma \vdash s : A \qquad \Gamma \vdash r : \mathtt{List}\ A}{\Gamma \vdash [\ s\ r : \mathtt{List}\ A} \qquad \frac{\Gamma \vdash s : \mathtt{Int} \qquad \Gamma \vdash s' : \mathtt{Int}}{\Gamma \vdash [\ s\ ..\ s'\ ] : \mathtt{List\ Int}} \qquad \frac{\Gamma \vdash \overrightarrow{q} \dashv \Delta \qquad \Gamma \cdot \Delta \vdash s : A}{\Gamma \vdash [\ s \mid \overrightarrow{q}\ ] : \mathtt{List}\ A}$$

$\boxed{\Gamma \vdash r : \mathtt{List}\ A}$

$$\frac{}{\Gamma \vdash\ ] : \mathtt{List}\ A} \qquad \frac{\Gamma \vdash s : A \qquad \Gamma \vdash r : \mathtt{List}\ A}{\Gamma \vdash\ ,\ s\ r : \mathtt{List}\ A}$$

$\boxed{\Gamma \vdash \overrightarrow{q} \dashv \Delta}$

$$\frac{}{\Gamma \vdash \varepsilon \dashv \varepsilon} \qquad \frac{\Gamma \vdash s : \mathtt{Bool}}{\Gamma \vdash s \dashv \varepsilon} \qquad \frac{\Gamma \vdash s : \mathtt{List}\ A \qquad p : A \dashv \Delta}{\Gamma \vdash p \leftarrow s \dashv \Delta} \qquad \frac{\Gamma \vdash s : A \qquad p : A \dashv \Delta}{\Gamma \vdash \mathtt{let}\ p = s \dashv \Delta}$$

$$\frac{\Gamma \vdash q \dashv \Gamma' \qquad \Gamma \cdot \Gamma' \vdash \overrightarrow{q} \dashv \Delta}{\Gamma \vdash q \cdot \overrightarrow{q} \dashv \Delta} \; \overrightarrow{q} \neq \varepsilon$$

Fig. 20. Typing rules for surface terms (additional forms only) and qualifiers

A SURFACE LANGUAGE: TYPING AND FORWARDS AND BACKWARDS DESUGARING

Definition A.1 (Disjoint join of partial continuations). Define $\boxplus$ to be the smallest partial symmetric function satisfying the equations in Figure 22.

$p : A \dashv \Gamma$

$$\frac{}{x : A \dashv \varepsilon, x : A} \qquad \frac{p_i : A_i \dashv \Gamma_i \quad (\forall i \le j)}{(\overrightarrow{x : p}) : \mathtt{Rec}\ (\overrightarrow{x : A}) \dashv \Gamma_1 \cdot .. \cdot \Gamma_j}\ |\vec{x}| = j \qquad \frac{}{[\,] : \mathtt{List}\ A \dashv \varepsilon}$$

$$\frac{p : A \dashv \Gamma \qquad p' : \mathtt{List}\ A \dashv \Gamma'}{p : p' : \mathtt{List}\ A \dashv \Gamma \cdot \Gamma'} \qquad \frac{p : A \dashv \Gamma \qquad o : \mathtt{List}\ A \dashv \Gamma'}{[\ p\ o : \mathtt{List}\ A \dashv \Gamma \cdot \Gamma'}$$

$o : \mathtt{List}\ A \dashv \Gamma$

$$\frac{}{\,] : \mathtt{List}\ A \dashv \varepsilon} \qquad \frac{p : A \dashv \Gamma \qquad o : \mathtt{List}\ A \dashv \Gamma'}{(\ ,\ p\ o) : \mathtt{List}\ A \dashv \Gamma \cdot \Gamma'}$$

$\Gamma \vdash \vec{c} : A \to B$

$$\frac{p : A \dashv \Gamma' \qquad \Gamma \cdot \Gamma' \vdash s : B}{\Gamma \vdash p = s : A \to B} \qquad \frac{p : A \dashv \Gamma' \qquad \Gamma \cdot \Gamma' \vdash \vec{p} = s : B}{\Gamma \vdash (p \cdot \vec{p}) = s : A \to B}\ \vec{p} \neq \varepsilon \qquad \frac{\Gamma \vdash c_i : A \to B \quad (\forall i \le j)}{\Gamma \vdash c_1 \cdot .. \cdot c_{j+1} : A \to B}$$

Fig. 21. Typing rules for patterns and clauses

$$
\begin{array}{lll}
\text{Eliminator} \quad \sigma ::= & \ldots & \\
& \{\texttt{true}\colon \kappa\} & \text{true} \\
& \{\texttt{false}\colon \kappa\} & \text{false} \\
& \{[\,]\colon \kappa\} & \text{nil} \\
& \{(\texttt{:})\colon \sigma\} & \text{cons}
\end{array}
$$

$\kappa \uplus \kappa'$

$$
\begin{aligned}
\lambda\sigma \uplus \lambda\sigma' &= \lambda(\sigma \uplus \sigma') \\
\\
(x\colon \sigma) \uplus (x\colon \sigma') &= x\colon \sigma \uplus \sigma' \\
\{\texttt{true}\colon \sigma\} \uplus \{\texttt{true}\colon \sigma'\} &= \{\texttt{true}\colon \sigma \uplus \sigma'\} \\
\{\texttt{false}\colon \tau\} \uplus \{\texttt{false}\colon \tau'\} &= \{\texttt{false}\colon \tau \uplus \tau'\} \\
\{\texttt{true}\colon \kappa\} \uplus \{\texttt{false}\colon \kappa'\} &= \{\texttt{true}\colon \kappa, \texttt{false}\colon \kappa'\} \\
\{\texttt{true}\colon \sigma\} \uplus \{\texttt{true}\colon \sigma', \texttt{false}\colon \kappa\} &= \{\texttt{true}\colon \sigma \uplus \sigma', \texttt{false}\colon \kappa\} \\
\{\texttt{false}\colon \tau\} \uplus \{\texttt{true}\colon \kappa, \texttt{false}\colon \tau'\} &= \{\texttt{true}\colon \kappa, \texttt{false}\colon \tau \uplus \tau'\} \\
\{\texttt{true}\colon \sigma, \texttt{false}\colon \tau\} \uplus \{\texttt{true}\colon \sigma', \texttt{false}\colon \tau'\} &= \{\texttt{true}\colon \sigma \uplus \sigma', \texttt{false}\colon \tau \uplus \tau'\} \\
\{[\,]\colon \sigma\} \uplus \{[\,]\colon \sigma'\} &= \{[\,]\colon \sigma \uplus \sigma'\} \\
\{(\texttt{:})\colon \tau\} \uplus \{(\texttt{:})\colon \tau'\} &= \{(\texttt{:})\colon \tau \uplus \tau'\} \\
\{[\,]\colon \kappa\} \uplus \{(\texttt{:})\colon \kappa'\} &= \{[\,]\colon \kappa, (\texttt{:})\colon \kappa'\} \\
\{[\,]\colon \sigma\} \uplus \{[\,]\colon \sigma', (\texttt{:})\colon \kappa\} &= \{\texttt{true}\colon \sigma \uplus \sigma', \texttt{false}\colon \kappa\} \\
\{(\texttt{:})\colon \tau\} \uplus \{[\,]\colon \kappa, (\texttt{:})\colon \tau'\} &= \{[\,]\colon \kappa, (\texttt{:})\colon \tau \uplus \tau'\} \\
\{[\,]\colon \sigma, (\texttt{:})\colon \tau\} \uplus \{[\,]\colon \sigma', (\texttt{:})\colon \tau'\} &= \{[\,]\colon \sigma \uplus \sigma', (\texttt{:})\colon \tau \uplus \tau'\} \\
\{(\vec{x})\colon \sigma\} \uplus \{(\vec{x})\colon \sigma'\} &= \{(\vec{x})\colon \sigma \uplus \sigma'\}
\end{aligned}
$$

Fig. 22. Partial eliminators and disjoint join of partial continuations

$s \nearrow e$

↗-op
$$\frac{}{(\oplus) \nearrow \oplus}$$

↗-binary-apply
$$\frac{s \nearrow e \qquad s' \nearrow e'}{s \oplus s' \nearrow \oplus\, e\, e'}$$

↗-nil
$$\frac{}{[]_\alpha \nearrow []_\alpha}$$

↗-non-empty-list
$$\frac{s \nearrow e \qquad r \nearrow e'}{[_\alpha\, s\, r \nearrow e :_\alpha e'}$$

↗-cons
$$\frac{s \nearrow e \qquad s' \nearrow e'}{s :_\alpha s' \nearrow e :_\alpha e'}$$

↗-let-rec
$$\frac{\overrightarrow{c_i} \nearrow \sigma_i \quad (\forall i \le j) \qquad s \nearrow e}{\texttt{let}\ x_1 \texttt{:}\ \overrightarrow{c_1} \cdot .. \cdot x_j \texttt{:}\ \overrightarrow{c_j}\ \texttt{in}\ s \nearrow \texttt{let}\ \overrightarrow{x \texttt{:}\ \sigma}\ \texttt{in}\ e}$$

↗-apply
$$\frac{s \nearrow e \qquad s' \nearrow e'}{s\, s' \nearrow e\, e'}$$

↗-match
$$\frac{s \nearrow e \qquad \overrightarrow{c} \nearrow \sigma}{\texttt{match}\ s\ \texttt{as}\ \overrightarrow{c} \nearrow \lambda\sigma\, e}$$

↗-let
$$\frac{s \nearrow e \qquad s' \nearrow e' \qquad p, e' \nearrow \sigma}{\texttt{let}\ p = s\ \texttt{in}\ s' \nearrow \lambda\sigma\, e}$$

↗-if
$$\frac{s \nearrow e \qquad s_1 \nearrow e_1 \qquad s_2 \nearrow e_2}{\texttt{if}\ s\ \texttt{then}\ s_1\ \texttt{else}\ s_2 \nearrow \lambda\{\texttt{true:}\ e_1, \texttt{false:}\ e_2\}\, e}$$

↗-list-enum
$$\frac{s \nearrow e \qquad s' \nearrow e'}{[\, s\ ..\ s'\,] \nearrow \texttt{enumFromTo}\, e\, e'}$$

↗-list-comp-done
$$\frac{s \nearrow e}{[\, s \mid \varepsilon]_\alpha \nearrow e :_\alpha []_\alpha}$$

↗-list-comp-guard
$$\frac{[\, s \mid \overrightarrow{q}]_\alpha \nearrow e \qquad s' \nearrow e'}{[\, s \mid s' \cdot \overrightarrow{q}]_\alpha \nearrow \lambda\{\texttt{true:}\ e, \texttt{false:}\ []_\alpha\}\, e'}$$

↗-list-comp-decl
$$\frac{[\, s \mid \overrightarrow{q}]_\alpha \nearrow e \qquad p, e \nearrow \sigma \qquad s' \nearrow e}{[\, s \mid \texttt{let}\ p = s' \cdot \overrightarrow{q}]_\alpha \nearrow \lambda\sigma\, e}$$

↗-list-comp-gen
$$\frac{[\, s \mid \overrightarrow{q}]_\alpha \nearrow e \qquad p, e \nearrow \sigma \qquad \sigma, \alpha \nearrow_p \sigma' \qquad s' \nearrow e'}{[\, s \mid p \leftarrow s' \cdot \overrightarrow{q}]_\alpha \nearrow \texttt{concatMap}\, \lambda\sigma'\, e'}$$

$r \nearrow e$

↗-list-rest-end
$$\frac{}{]_\alpha \nearrow []_\alpha}$$

↗-list-rest-cons
$$\frac{s \nearrow e \qquad r \nearrow e'}{(,_\alpha\, s\, r) \nearrow e :_\alpha e'}$$

Fig. 23. Desugaring – forward slicing (selected rules)

$\boxed{\vec{p}, \kappa \nearrow \sigma}$

↗-var

$$\frac{}{x, \kappa \nearrow x\colon \kappa}$$

↗-true

$$\frac{}{\texttt{true}, \kappa \nearrow \{\texttt{true}\colon \kappa\}}$$

↗-false

$$\frac{}{\texttt{false}, \kappa \nearrow \{\texttt{false}\colon \kappa\}}$$

↗-nil

$$\frac{}{[\,], \kappa \nearrow \{[\,]\colon \kappa\}}$$

↗-cons

$$\frac{p', \kappa \nearrow \sigma \qquad p, \sigma \nearrow \sigma'}{p : p', \kappa \nearrow \{(:)\colon \sigma'\}}$$

↗-non-empty-list

$$\frac{o, \kappa \nearrow \sigma \qquad p, \sigma \nearrow \sigma'}{[\ p\ o, \kappa \nearrow \{(:)\colon \sigma'\}}$$

↗-unit

$$\frac{}{(), \kappa \nearrow \{()\colon \kappa\}}$$

↗-record

$$\frac{p', \kappa \nearrow \sigma \qquad (\overrightarrow{x\colon p}), \sigma \nearrow \{(\vec{x})\colon \sigma'\}}{(\overrightarrow{x\colon p} \cdot y\colon p'), \kappa \nearrow \{(\vec{x} \cdot y)\colon \sigma'\}}$$

↗-seq

$$\frac{\vec{p}, e \nearrow \sigma \qquad p, \lambda\sigma \nearrow \sigma'}{p \cdot \vec{p}, e \nearrow \sigma'}\ \vec{p} \neq \varepsilon$$

$\boxed{o, \kappa \nearrow \sigma}$

↗-list-rest-end

$$\frac{}{], \kappa \nearrow \{[\,]\colon \kappa\}}$$

↗-list-rest-cons

$$\frac{o, \kappa \nearrow \sigma \qquad p, \sigma \nearrow \sigma'}{(\texttt{,}\ p\ o), \kappa \nearrow \{(:)\colon \sigma'\}}$$

$\boxed{\vec{c} \nearrow\!\!\nearrow \sigma}$

↗↗-clause

$$\frac{s \nearrow e \qquad \vec{p}, e \nearrow \sigma}{\vec{p} = s \nearrow\!\!\nearrow \sigma}$$

↗↗-clause-seq

$$\frac{c \nearrow\!\!\nearrow \sigma \qquad \vec{c} \nearrow\!\!\nearrow \sigma' \qquad \sigma \uplus \sigma' = \tau}{c \cdot \vec{c} \nearrow\!\!\nearrow \tau}\ \vec{c} \neq \varepsilon$$

Fig. 24. Desugaring clauses – forward slicing

$\kappa, \alpha \nearrow_{\vec{\pi}} \kappa'$

↗-empty

$$\frac{}{e, \alpha \nearrow_{\varepsilon} e}$$

↗-var

$$\frac{\kappa, \alpha \nearrow_{\vec{\pi}} \kappa'}{x\colon \kappa, \alpha \nearrow_{x \cdot \vec{\pi}} x\colon \kappa'}$$

↗-true

$$\frac{\kappa, \alpha \nearrow_{\vec{\pi}} \kappa'}{\{\texttt{true}\colon \kappa\}, \alpha \nearrow_{\texttt{true} \cdot \vec{\pi}} \{\texttt{true}\colon \kappa', \texttt{false}\colon []_{\alpha}\}}$$

↗-false

$$\frac{\kappa, \alpha \nearrow_{\vec{\pi}} \kappa'}{\{\texttt{false}\colon \kappa\}, \alpha \nearrow_{\texttt{false} \cdot \vec{\pi}} \{\texttt{true}\colon []_{\alpha}, \texttt{false}\colon \kappa'\}}$$

↗-unit

$$\frac{\kappa, \alpha \nearrow_{\vec{\pi}} \kappa'}{\{():\kappa\}, \alpha \nearrow_{() \cdot \vec{\pi}} \{():\kappa'\}}$$

↗-record

$$\frac{\{(\vec{x}):\sigma\}, \alpha \nearrow_{(\overrightarrow{x:p}) \cdot p' \cdot \vec{\pi}} \{(\vec{x}):\sigma'\}}{\{(\vec{x} \cdot y):\sigma\}, \alpha \nearrow_{(\overrightarrow{x:p} \cdot y:p') \cdot \vec{\pi}} \{(\vec{x} \cdot y):\sigma'\}}$$

↗-nil

$$\frac{\kappa, \alpha \nearrow_{\vec{\pi}} \kappa'}{\{[]:\kappa\}, \alpha \nearrow_{[] \cdot \vec{\pi}} \{[]:\kappa', (:):x:y:[]_{\alpha}\}}$$

↗-cons

$$\frac{\sigma, \alpha \nearrow_{p \cdot p' \cdot \vec{\pi}} \sigma'}{\{(:):\sigma\}, \alpha \nearrow_{(p\,:\,p') \cdot \vec{\pi}} \{[]:[]_{\alpha}, (:):\sigma'\}}$$

↗-non-empty-list

$$\frac{\sigma, \alpha \nearrow_{p \cdot o \cdot \vec{\pi}} \sigma'}{\{(:):\sigma\}, \alpha \nearrow_{([\ p\ o) \cdot \vec{\pi}} \{[]:[]_{\alpha}, (:):\sigma'\}}$$

↗-list-rest-end

$$\frac{\kappa, \alpha \nearrow_{\vec{\pi}} \kappa'}{\{[]:\kappa\}, \alpha \nearrow_{] \cdot \vec{\pi}} \{[]:\kappa', (:):x:y:[]_{\alpha}\}}$$

↗-list-rest-cons

$$\frac{\sigma, \alpha \nearrow_{p \cdot o \cdot \vec{\pi}} \sigma'}{\{(:):\sigma\}, \alpha \nearrow_{(,\ p\ o) \cdot \vec{\pi}} \{[]:[]_{\alpha}, (:):\sigma'\}}$$

Fig. 25. Totalise – forward slicing

$e \searrow_t s$

↘-eq
$$\frac{e \doteq \searrow_t s}{e \searrow_t s}$$

↘-binary-apply
$$\frac{e \searrow_t s \qquad e' \searrow_{t'} s'}{(\oplus)\, e\, e' \searrow_{t \oplus t'} s \oplus s'}$$

↘-nil
$$\frac{}{[]_\alpha \searrow_{[]} []_\alpha}$$

↘-non-empty-list
$$\frac{e \searrow_t s \qquad e' \searrow_r r'}{e :_\alpha e' \searrow_{[\ t\ r} [_\alpha\, s\, r'}$$

↘-cons
$$\frac{e \searrow_t s \qquad e' \searrow_{t'} s'}{e :_\alpha e' \searrow_{t\, :\, t'} s :_\alpha s'}$$

↘-let-rec
$$\frac{\sigma_i \searrow_{\overrightarrow{c_i}} \overrightarrow{c_i'} \quad (\forall i \le j) \qquad e \searrow_t s}{\texttt{let}\ \overrightarrow{x\colon \sigma}\ \texttt{in}\ e \searrow_{\texttt{let}\ x_1\colon \overrightarrow{c_1} \cdot \ldots \cdot x_j\colon \overrightarrow{c_j}\ \texttt{in}\ t} \texttt{let}\ x_1\colon \overrightarrow{c_1'} \cdot \ldots \cdot x_j\colon \overrightarrow{c_j'}\ \texttt{in}\ s}$$

↘-apply
$$\frac{e \searrow_t s \qquad e' \searrow_{t'} s'}{e\, e' \searrow_{t\, t'} s\, s'}$$

↘-if
$$\frac{e \searrow_t s \qquad e_1 \searrow_{t_1} s_1 \qquad e_2 \searrow_{t_2} s_2}{\lambda\{\texttt{true}\colon e_1, \texttt{false}\colon e_2\}\, e \searrow_{\texttt{if}\ t\ \texttt{then}\ t_1\ \texttt{else}\ t_2} \texttt{if}\ s\ \texttt{then}\ s_1\ \texttt{else}\ s_2}$$

↘-match
$$\frac{\sigma \searrow_{\overrightarrow{c}} \overrightarrow{c'} \qquad e \searrow_t s}{\lambda\sigma\, e \searrow_{\texttt{match}\ t\ \texttt{as}\ \overrightarrow{c}} \texttt{match}\ s\ \texttt{as}\ \overrightarrow{c'}}$$

↘-let
$$\frac{\sigma \searrow_p e' \qquad e' \searrow_{t'} s' \qquad e \searrow_t s}{\lambda\sigma\, e \searrow_{\texttt{let}\ p=t\ \texttt{in}\ t'} \texttt{let}\ p = s\ \texttt{in}\ s'}$$

↘-list-enum
$$\frac{e \searrow_t s \qquad e' \searrow_{t'} s'}{\texttt{enumFromTo}\, e\, e' \searrow_{[\ t\ ..\ t'\ ]} [\ s\ ..\ s'\ ]}$$

↘-list-comp-done
$$\frac{e \searrow_t s}{e :_{\alpha'} []_\alpha \searrow_{[\ t\ |\ \varepsilon]} [\ s \mid \varepsilon]_{\alpha \sqcup \alpha'}}$$

↘-list-comp-guard
$$\frac{e' \searrow_{t'} s' \qquad e \searrow_{[\ t\ |\ \overrightarrow{q}\ ]} [\ s \mid \overrightarrow{q'}]_\beta}{\lambda\{\texttt{true}\colon e, \texttt{false}\colon []_\alpha\}\, e' \searrow_{[\ t\ |\ t' \cdot \overrightarrow{q}\ ]} [\ s \mid s' \cdot \overrightarrow{q'}]_{\alpha \sqcup \beta}}$$

↘-list-comp-decl
$$\frac{\sigma \searrow_p e' \qquad e' \searrow_{[\ t'\ |\ \overrightarrow{q}\ ]} [\ s' \mid \overrightarrow{q'}]_\beta \qquad e \searrow_t s}{\lambda\sigma\, e \searrow_{[\ t'\ |\ \texttt{let}\ p=t \cdot \overrightarrow{q}\ ]} [\ s' \mid \texttt{let}\ p = s \cdot \overrightarrow{q'}]_\beta}$$

↘-list-comp-gen
$$\frac{e \searrow_t s \qquad \sigma \searrow_p \sigma', \beta \qquad \sigma' \searrow_p e' \qquad e' \searrow_{[\ t'\ |\ \overrightarrow{q}\ ]} [\ s' \mid \overrightarrow{q'}]_{\beta'}}{\texttt{concatMap}\, \lambda\sigma\, e \searrow_{[\ t'\ |\ p \leftarrow t \cdot \overrightarrow{q}\ ]} [\ s' \mid p \leftarrow s \cdot \overrightarrow{q'}]_{\beta \sqcup \beta'}}$$

$e \searrow_r r'$

↘-list-rest-end
$$\frac{}{[]_\alpha \searrow_{]}]_\alpha}$$

↘-list-rest-cons
$$\frac{e \searrow_t s \qquad e' \searrow_r r'}{e :_\alpha e' \searrow_{(\ ,\ t\ r)} (,_\alpha\, s\, r')}$$

Fig. 26. Desugaring – backward slicing (selected rules)

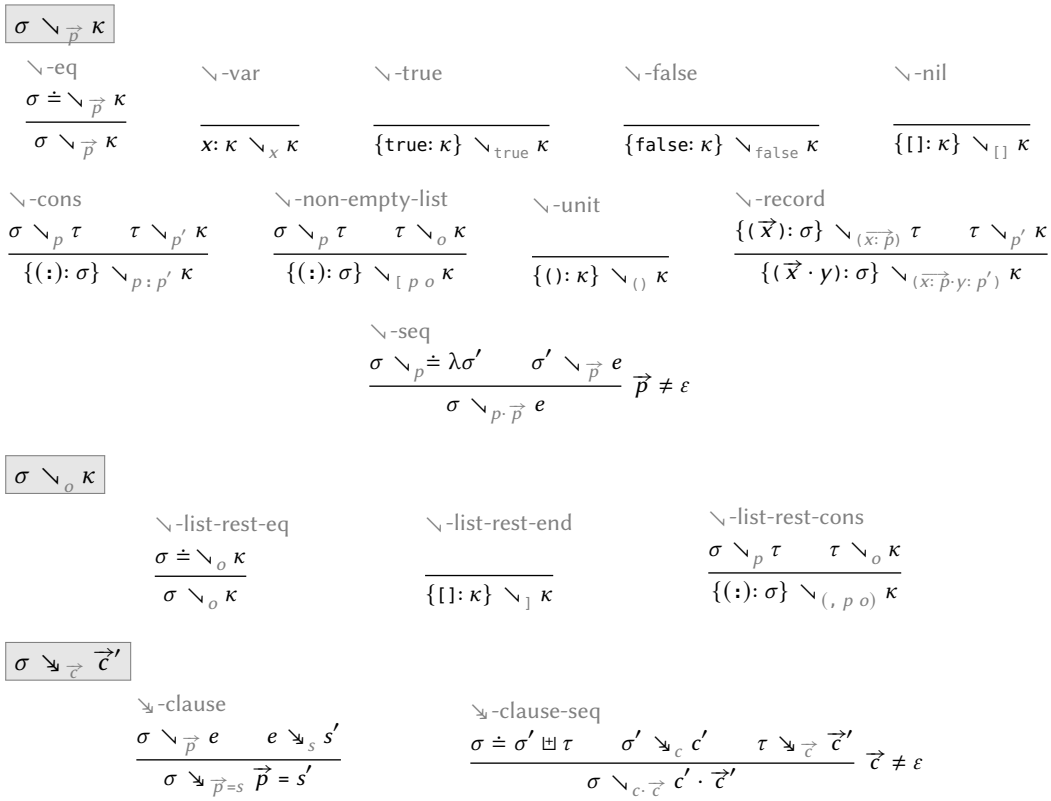


Fig. 27. Desugaring clauses – backward slicing

$\kappa \searrow_{\vec{\pi}} \kappa', \alpha$

$$\frac{}{e \searrow_{\varepsilon} e, \mathsf{ff}}\ \searrow\text{-empty}$$

$$\frac{\sigma \doteq x\colon \kappa \qquad \kappa \searrow_{\vec{\pi}} \kappa', \alpha}{\sigma \searrow_{x \cdot \vec{\pi}} x\colon \kappa', \alpha}\ \searrow\text{-var}$$

$$\frac{\sigma \doteq \{\mathtt{true}\colon \kappa, \mathtt{false}\colon []_{\alpha}\} \qquad \kappa \searrow_{\vec{\pi}} \kappa', \beta}{\sigma \searrow_{\mathtt{true} \cdot \vec{\pi}} \{\mathtt{true}\colon \kappa'\}, \alpha \sqcup \beta}\ \searrow\text{-true}$$

$$\frac{\sigma \doteq \{\mathtt{true}\colon []_{\alpha}, \mathtt{false}\colon \kappa\} \qquad \kappa \searrow_{\vec{\pi}} \kappa', \beta}{\sigma \searrow_{\mathtt{false} \cdot \vec{\pi}} \{\mathtt{false}\colon \kappa'\}, \alpha \sqcup \beta}\ \searrow\text{-false}$$

$$\frac{\sigma \doteq \{()\colon \kappa\} \qquad \kappa \searrow_{\vec{\pi}} \kappa', \alpha}{\sigma \searrow_{() \cdot \vec{\pi}} \{()\colon \kappa'\}, \alpha}\ \searrow\text{-unit}$$

$$\frac{\sigma \doteq \{(\overrightarrow{x} \cdot y)\colon \sigma'\} \qquad \sigma' \searrow_{(\overrightarrow{x\colon p}) \cdot p' \cdot \vec{\pi}} \tau, \beta}{\sigma \searrow_{(\overrightarrow{x\colon p} \cdot y\colon p') \cdot \vec{\pi}} \{(\overrightarrow{x} \cdot y)\colon \tau\}, \beta}\ \searrow\text{-record}$$

$$\frac{\sigma \doteq \{[]\colon \kappa, (\mathbf{:})\colon x\colon y\colon []_{\alpha}\} \qquad \kappa \searrow_{\vec{\pi}} \kappa', \beta}{\sigma \searrow_{[] \cdot \vec{\pi}} \{[]\colon \kappa'\}, \alpha \sqcup \beta}\ \searrow\text{-nil}$$

$$\frac{\sigma \doteq \{[]\colon []_{\alpha}, (\mathbf{:})\colon \sigma'\} \qquad \sigma' \searrow_{p \cdot p' \cdot \vec{\pi}} \tau, \beta}{\sigma \searrow_{(p\,:\,p') \cdot \vec{\pi}} \{(\mathbf{:})\colon \tau\}, \alpha \sqcup \beta}\ \searrow\text{-cons}$$

$$\frac{\sigma \doteq \{[]\colon []_{\alpha}, (\mathbf{:})\colon \sigma'\} \qquad \sigma' \searrow_{p \cdot o \cdot \vec{\pi}} \tau, \beta}{\sigma \searrow_{([\ p\ o) \cdot \vec{\pi}} \{(\mathbf{:})\colon \tau\}, \alpha \sqcup \beta}\ \searrow\text{-non-empty-list}$$

$$\frac{\sigma \doteq \{[]\colon \kappa, (\mathbf{:})\colon x\colon y\colon []_{\alpha}\} \qquad \kappa \searrow_{\vec{\pi}} \kappa', \beta}{\sigma \searrow_{] \cdot \vec{\pi}} \{[]\colon \kappa'\}, \alpha \sqcup \beta}\ \searrow\text{-list-rest-end}$$

$$\frac{\sigma \doteq \{[]\colon []_{\alpha}, (\mathbf{:})\colon \sigma'\} \qquad \sigma' \searrow_{p \cdot o \cdot \vec{\pi}} \tau, \beta}{\sigma \searrow_{(,\ p\ o) \cdot \vec{\pi}} \{(\mathbf{:})\colon \tau\}, \alpha \sqcup \beta}\ \searrow\text{-list-rest-cons}$$

Fig. 28. Totalise — backward slicing

B PROOFS: CORE LANGUAGE

B.1 Conventions

The symbol ➪ indicates that a proof obligation is being discharged, and IH stands for "inductive hypothesis". We make free use of the totality of the forward and backward slicing functions, and the fact that all term constructors preserve and reflect $\sqsubseteq$, for example that $u : u' \sqsubseteq v : v'$ if and only if $u \sqsubseteq v$ and $u' \sqsubseteq v'$.

B.2 Theorem 3.8

B.2.1 Forward after backward direction. Induction on the $\searrow$ derivation.

Proof.

Case $\dfrac{}{x\colon v, \kappa, \alpha \searrow_x v, x\colon \kappa}\ \searrow\text{-var}$

➪ $\dfrac{}{v, x\colon \kappa \nearrow_x x\colon v, \kappa, \mathsf{tt}}\ \nearrow\text{-var}$

➪ $\mathsf{tt} \sqsupseteq \alpha$

Case $\dfrac{}{\varepsilon, \kappa, \alpha \searrow_{\mathtt{true}} \mathtt{true}_\alpha, \{\mathtt{true}\colon \kappa, \mathtt{false}\colon \square\}}\ \searrow\text{-true}$

➪ $\dfrac{}{\mathtt{true}_\alpha, \{\mathtt{true}\colon \kappa, \mathtt{false}\colon \square\} \nearrow_{\mathtt{true}} \varepsilon, \kappa, \alpha}\ \nearrow\text{-true}$

Case $\dfrac{}{\varepsilon, \kappa, \alpha \searrow_{\mathtt{false}} \mathtt{false}_\alpha, \{\mathtt{true}\colon \square, \mathtt{false}\colon \kappa\}}\ \searrow\text{-false}$

➪ $\dfrac{}{\mathtt{false}_\alpha, \{\mathtt{true}\colon \square, \mathtt{false}\colon \kappa\} \nearrow_{\mathtt{false}} \varepsilon, \kappa, \alpha}\ \nearrow\text{-false}$

Case $\dfrac{\rho_2, \kappa, \alpha \searrow_{w'} v', \sigma \qquad \rho_1, \sigma, \alpha \searrow_w v, \tau}{\rho_1 \cdot \rho_2, \kappa, \alpha \searrow_{(w,w')} (v, v')_\alpha, \{(,)\colon \tau\}}\ \searrow\text{-pair}$

$v, \tau \nearrow_w \rho_1', \tau', \beta \sqsupseteq \rho_1, \sigma, \alpha \quad (\exists \rho_1', \tau', \beta)$ IH (1)

$v', \sigma \nearrow_{w'} \sqsupseteq \rho_2, \kappa, \alpha$ IH

$v', \tau' \nearrow_{w'} \rho_2', \kappa', \beta' \sqsupseteq \rho_2, \kappa, \alpha \quad (\exists \rho_2', \kappa', \beta)$ monotonicity (2)

$\nearrow$-pair

$$\dfrac{v, \tau \nearrow_{w} \rho_1', \tau', \beta \qquad v', \tau' \nearrow_{w'} \rho_2', \kappa', \beta'}{(v, v')_{\alpha}, \{(,): \tau\} \nearrow_{(w, w')} \rho_1' \cdot \rho_2', \kappa', \alpha \sqcap \beta \sqcap \beta'} \quad (1, 2)$$

$\Rightarrow (\rho_1' \cdot \rho_2', \kappa', \alpha \sqcap \beta \sqcap \beta') \sqsupseteq (\rho_1 \cdot \rho_2, \kappa, \alpha)$

Case $\searrow$-nil

$$\dfrac{}{\varepsilon, \kappa, \alpha \searrow_{[]} []_{\alpha}, \{[]: \kappa, (:): \square\}}$$

$\Rightarrow$ $\nearrow$-nil

$$\dfrac{}{[]_{\alpha}, \{[]: \kappa, (:): \square\} \nearrow_{[]} \varepsilon, \kappa, \alpha}$$

Case $\searrow$-cons

$$\dfrac{\rho_2, \kappa, \alpha \searrow_{w'} v', \sigma \qquad \rho_1, \sigma, \alpha \searrow_{w} v, \tau}{\rho_1 \cdot \rho_2, \kappa, \alpha \searrow_{w : w'} v :_{\alpha} v', \{[]: \square, (:): \tau\}}$$

$v, \tau \nearrow_{w} \rho_1', \tau', \beta \sqsupseteq \rho_1, \sigma, \alpha \quad (\exists \rho_1', \tau', \beta)$ IH (3)

$v', \sigma \nearrow_{w'} \sqsupseteq \rho_2, \kappa, \alpha$ IH

$v', \tau' \nearrow_{w'} \rho_2', \kappa', \beta' \sqsupseteq \rho_2, \kappa, \alpha \quad (\exists \rho_2', \kappa', \beta')$ monotonicity (4)

$\nearrow$-cons

$$\dfrac{v, \tau \nearrow_{w} \rho_1', \tau', \beta \qquad v', \tau' \nearrow_{w'} \rho_2', \kappa', \beta'}{v :_{\alpha} v', \{[]: \square, (:): \tau\} \nearrow_{w : w'} \rho_1' \cdot \rho_2', \kappa', \alpha \sqcap \beta \sqcap \beta'} \quad (3, 4)$$

$\Rightarrow (\rho_1' \cdot \rho_2', \kappa', \alpha \sqcap \beta \sqcap \beta') \sqsupseteq (\rho_1 \cdot \rho_2, \kappa, \alpha)$

□

B.2.2 Backward after forward direction. Induction on the $\nearrow$ derivation.

Proof.

Case $\nearrow$-var

$$\dfrac{\sigma \doteq x: \kappa}{v, \sigma \nearrow_{x} x: v, \kappa, \mathsf{tt}}$$

$\Rightarrow$ $\searrow$-var

$$\dfrac{}{x: v, \kappa, \mathsf{tt} \searrow_{x} v, x: \kappa}$$

$\Rightarrow (v, x: \kappa) \doteq (v, \sigma)$

Case $\nearrow$-true

$$\dfrac{v \doteq \mathtt{true}_{\alpha} \qquad \sigma \doteq \{\mathtt{true}: \kappa, \mathtt{false}: \kappa'\}}{v, \sigma \nearrow_{\mathtt{true}} \varepsilon, \kappa, \alpha}$$

$\twoheadrightarrow$ $\twoheadrightarrow$-true

$$\frac{}{\varepsilon, \kappa, \alpha \twoheadrightarrow_{\texttt{true}} \texttt{true}_\alpha, \{\texttt{true}\colon \kappa, \texttt{false}\colon \square\}}$$

$\twoheadrightarrow$ $(\texttt{true}_\alpha, \{\texttt{true}\colon \kappa, \texttt{false}\colon \square\}) \sqsubseteq (\texttt{true}_\alpha, \{\texttt{true}\colon \kappa, \texttt{false}\colon \kappa'\}) \doteq (v, \sigma)$

Case $\nearrow$-false

$$\frac{v \doteq \texttt{false}_\alpha \qquad \sigma \doteq \{\texttt{true}\colon \kappa, \texttt{false}\colon \kappa'\}}{v, \sigma \nearrow_{\texttt{false}} \varepsilon, \kappa', \alpha}$$

$\twoheadrightarrow$ $\twoheadrightarrow$-false

$$\frac{}{\varepsilon, \kappa', \alpha \twoheadrightarrow_{\texttt{false}} \texttt{false}_\alpha, \{\texttt{true}\colon \square, \texttt{false}\colon \kappa'\}}$$

$\twoheadrightarrow$ $(\texttt{false}_\alpha, \{\texttt{true}\colon \square, \texttt{false}\colon \kappa'\}) \sqsubseteq (\texttt{false}_\alpha, \{\texttt{true}\colon \kappa, \texttt{false}\colon \kappa'\}) \doteq (v, \sigma)$

Case $\nearrow$-pair

$$\frac{\sigma \doteq \{(,)\colon \sigma'\} \qquad v \doteq (v_1, v_2)_\alpha \qquad v_1, \sigma' \nearrow_{w_1} \rho_1, \tau, \beta \qquad v_2, \tau \nearrow_{w_2} \rho_2, \kappa, \beta'}{v, \sigma' \nearrow_{(w_1, w_2)} \rho_1 \cdot \rho_2, \kappa, \alpha \sqcap \beta \sqcap \beta'}$$

$\rho_2, \kappa, \beta' \twoheadrightarrow_{w_2} \sqsubseteq v_2, \tau$ IH

$\rho_2, \kappa, \alpha \sqcap \beta \sqcap \beta' \twoheadrightarrow_{w_2} u_2, \tau' \sqsubseteq v_2, \tau \quad (\exists u_2, \tau')$ monotonicity (1)

$\rho_1, \tau, \beta \twoheadrightarrow_{w_1} \sqsubseteq v_1, \sigma'$ IH

$\rho_1, \tau', \alpha \sqcap \beta \sqcap \beta' \twoheadrightarrow_{w_1} u_1, \tau'' \sqsubseteq v_1, \sigma' \quad (\exists u_1, \tau'')$ monotonicity (2)

$\twoheadrightarrow$ $\twoheadrightarrow$-pair

$$\frac{\rho_2, \kappa, \alpha \sqcap \beta \sqcap \beta' \twoheadrightarrow_{w_2} u_2, \tau' \qquad \rho_1, \tau', \alpha \sqcap \beta \sqcap \beta' \twoheadrightarrow_{w_1} u_1, \tau''}{\rho_1 \cdot \rho_2, \kappa, \alpha \sqcap \beta \sqcap \beta' \twoheadrightarrow_{(w_1, w_2)} (u_1, u_2)_{\alpha \sqcap \beta \sqcap \beta'}, \{(,)\colon \tau''\}} \quad (1, 2)$$

$\twoheadrightarrow$ $((u_1, u_2)_{\alpha \sqcap \beta \sqcap \beta'}, \{(,)\colon \tau''\}) \sqsubseteq ((v_1, v_2)_\alpha, \{(,)\colon \sigma'\}) \doteq (v, \sigma)$

Case $\nearrow$-nil

$$\frac{v \doteq []_\alpha \qquad \sigma \doteq \{[]\colon \kappa, (:)\colon \sigma'\}}{v, \sigma \nearrow_{[]} \varepsilon, \kappa, \alpha}$$

$\twoheadrightarrow$ $\twoheadrightarrow$-nil

$$\frac{}{\varepsilon, \kappa, \alpha \twoheadrightarrow_{[]} []_\alpha, \{[]\colon \kappa, (:)\colon \square\}}$$

$\twoheadrightarrow$ $([]_\alpha, \{[]\colon \kappa, (:)\colon \square\}) \sqsubseteq ([]_\alpha, \{[]\colon \kappa, (:)\colon \sigma'\}) \doteq (v, \sigma)$

Case $\nearrow$-cons

$$\frac{v \doteq v_1 :_\alpha v_2 \qquad \sigma \doteq \{[]\colon \kappa, (:)\colon \sigma'\} \qquad v_1, \sigma' \nearrow_{w_1} \rho_1, \tau, \beta \qquad v_2, \tau \nearrow_{w_2} \rho_2, \kappa, \beta'}{v, \sigma \nearrow_{w_1 \,:\, w_2} \rho_1 \cdot \rho_2, \kappa, \alpha \sqcap \beta \sqcap \beta'}$$

$\rho_2, \kappa, \beta' \ \curlywedge_{w_2} \sqsubseteq v_2, \tau$ IH

$\rho_2, \kappa, \alpha \sqcap \beta \sqcap \beta' \ \curlywedge_{w_2} \ u_2, \tau' \sqsubseteq v_2, \tau \quad (\exists u_2, \tau')$ monotonicity (3)

$\rho_1, \tau, \beta \ \curlywedge_{w_1} \sqsubseteq v_1, \sigma'$ IH

$\rho_1, \tau', \alpha \sqcap \beta \sqcap \beta' \ \curlywedge_{w_1} \ u_1, \tau'' \sqsubseteq v_1, \sigma' \quad (\exists u_1, \tau'')$ monotonicity (4)

$\curlywedge$-cons

$$\Rightarrow \frac{\rho_2, \kappa, \alpha \sqcap \beta \sqcap \beta' \ \curlywedge_{w_2} \ u_2, \tau' \qquad \rho_1, \tau', \alpha \sqcap \beta \sqcap \beta' \ \curlywedge_{w_1} \ u_1, \tau''}{\rho_1 \cdot \rho_2, \kappa, \alpha \sqcap \beta \sqcap \beta' \ \curlywedge_{w_1 \,:\, w_2} \ u_1 :_{\alpha \sqcap \beta \sqcap \beta'} u_2, \{[\,]\colon \square, (:)\colon \tau''\}} \quad (3, 4)$$

$\Rightarrow (u_1 :_{\alpha \sqcap \beta \sqcap \beta'} u_2, \{[\,]\colon \square, (:)\colon \tau''\}) \sqsubseteq (v_1 :_\alpha v_2, \{[\,]\colon \kappa, (:)\colon \sigma'\}) \doteq (v, \sigma)$

□

B.3 Lemma 3.9

If $\rho \ni_{\rho'} x\colon v$ then $x\colon v \in \rho$.

Proof. By induction on the proof that $\rho \ni_{\rho'} x\colon v$:

Case ∋-head

$$\frac{}{(\square_{\rho'} \cdot x\colon v) \ni_{\rho' \cdot x\colon u} x\colon v}$$

$\Rightarrow$ ∈-head

$$\frac{}{x\colon v \in \square_{\rho'} \cdot x\colon v}$$

Case ∋-tail

$$\frac{\rho \ni_{\rho'} x\colon v}{(\rho \cdot x'\colon \square) \ni_{\rho' \cdot x'\colon u} x\colon v} \ x \neq x'$$

$x\colon v \in \rho$ IH (1)

$\Rightarrow$ ∈-tail

$$\frac{x\colon v \in \rho}{x\colon v \in (\rho \cdot x'\colon \square)} \ x' \neq x \quad (1)$$

□

If $x\colon v \in \rho$ then $\exists \rho'$ such that $\rho' \ni_\rho x\colon v$ and $\rho' \sqsubseteq \rho$.

Proof. By induction on the proof that $x\colon v \in \rho$.

Case ∈-head

$$\frac{}{x\colon v \in (\rho \cdot x\colon v)}$$

$\Rightarrow$ ∋-head

$$\frac{}{(\square_{\boldsymbol{\rho}} \cdot x\colon v) \ni_{\rho \cdot x\colon u} x\colon v}$$

$\Rightarrow (\square_{\boldsymbol{\rho}} \cdot x\colon v) \sqsubseteq (\rho \cdot x\colon v)$

Case $\dfrac{x\colon v \in \rho}{x\colon v \in (\rho \cdot x'\colon u)}\ \in\text{-tail}\ \ x' \neq x$

$\rho \sqsupseteq \rho' \ni_\rho x\colon v \quad (\exists \rho')$ (IH)

$\Rightarrow \dfrac{\rho' \ni_\rho x\colon v}{(\rho' \cdot x'\colon \square) \ni_{\rho \cdot x'\colon u} x\colon v}\ \ni\text{-tail}\ \ x' \neq x$

$\Rightarrow (\rho' \cdot x'\colon \square) \sqsubseteq (\rho \cdot x'\colon u)$

□

B.4 Theorem 3.10

B.4.1 Forward afer backward direction. Suppose $\rho, h \twoheadrightarrow \rho'$. Then $\nearrow_{\rho,h} (\searrow_{\rho,h} (\rho')) \sqsupseteq \rho'$.

Proof.

$\overrightarrow{x\colon \mathtt{cl}(\rho, h, \sigma)} \searrow (\bigsqcup \overrightarrow{\rho}, \overrightarrow{x\colon \sigma} \sqcup \bigsqcup \overrightarrow{h}) \quad \text{where } \overrightarrow{h} = \overrightarrow{x_1\colon \sigma'_1} \cdot .. \cdot \overrightarrow{x_j\colon \sigma'_j}$ (Suppose)

$\overrightarrow{x\colon \tau} = \overrightarrow{x\colon \sigma} \sqcup \bigsqcup \overrightarrow{h} \quad (\exists \overrightarrow{\tau})$

$(\bigsqcup \overrightarrow{\rho}, \overrightarrow{x\colon \tau}) \twoheadrightarrow x_1\colon \mathtt{cl}(\bigsqcup \overrightarrow{\rho}, \overrightarrow{x\colon \tau}, \tau_1) \cdot .. \cdot x_j\colon \mathtt{cl}(\bigsqcup \overrightarrow{\rho}, \overrightarrow{x\colon \tau}, \tau_j)$ (Def. ↠, Figure 6)

$\bigsqcup \overrightarrow{\rho} \sqsupseteq \rho_i \quad (\forall i \leq j)$ (1)

$\overrightarrow{x\colon \tau} \sqsupseteq h_i \quad (\forall i \leq j)$ (2)

$\tau_i = \sigma_i \sqcup \sigma'_{1,i} \sqcup .. \sqcup \sigma'_{j,i} \quad (\forall i \leq j)$

$\tau_i \sqsupseteq \sigma_i$ (3)

$\Rightarrow x_1\colon \mathtt{cl}(\bigsqcup \overrightarrow{\rho}, \overrightarrow{x\colon \tau}, \tau_1) \cdot .. \cdot x_j\colon \mathtt{cl}(\bigsqcup \overrightarrow{\rho}, \overrightarrow{x\colon \tau}, \tau_j) \sqsupseteq \overrightarrow{x\colon \mathtt{cl}(\rho, h, \sigma)}$ (1, 2, 3)

□

B.4.2 Backward after forward direction. Suppose $\rho, h \twoheadrightarrow \rho'$. Then $\searrow_{\rho,h} (\nearrow_{\rho,h} (\rho, h)) \sqsubseteq (\rho, h)$.

Proof.

$\rho, h \twoheadrightarrow x_1\colon \mathtt{cl}(\rho, h, \sigma_1) \cdot .. \cdot x_j\colon \mathtt{cl}(\rho, h, \sigma_j) \ \text{ where } h = \overrightarrow{x\colon \sigma}$ (Suppose)

$x_1\colon \mathtt{cl}(\rho, h, \sigma_1) \cdot .. \cdot x_j\colon \mathtt{cl}(\rho, h, \sigma_j) \searrow (\rho, \overrightarrow{x\colon \sigma} \sqcup h) = (\rho, h)$ (Def. ↘, Figure 12)

$\Rightarrow (\rho, h) \sqsubseteq (\rho, h)$

□

B.5 Theorem 3.11

B.5.1 Forward after backward direction. Induction on the ⇘ derivation.

Proof.

Case $\dfrac{\rho \ni_\Gamma x\colon v}{v \searrow_x \rho, x, \mathsf{ff}}\ \searrow\text{-var}$

$x\colon v \in \rho$ (Lemma 3.9)

➪ $\nearrow$-var
$$\frac{x\colon v \in \rho}{\rho, x, \mathsf{ff} \nearrow_x v}$$

Case $\searrow$-op
$$\frac{v \doteq \phi \qquad \rho \ni_\Gamma \oplus\colon v}{v \searrow_{(\oplus)_\Gamma} \rho, (\oplus), \mathsf{ff}}$$

$\oplus : v \in \rho$ (Lemma 3.9)

➪ $\nearrow$-op
$$\frac{\oplus\colon v \in \rho}{\rho, (\oplus), \mathsf{ff} \nearrow_{(\oplus)_\Gamma} v}$$

Case $\searrow$-lambda
$$\frac{v \doteq \mathtt{cl}(\rho, \varepsilon, \sigma)}{v \searrow_{\lambda\sigma'} \rho, \lambda\sigma, \mathsf{ff}}$$

➪ $\nearrow$-lambda
$$\frac{}{\rho, \lambda\sigma, \mathsf{ff} \nearrow_{\lambda\sigma'} \mathtt{cl}(\rho, \varepsilon, \sigma)}$$

➪ $\mathtt{cl}(\rho, \varepsilon, \sigma) \doteq v$

Case $\searrow$-int
$$\frac{v \doteq n_\alpha}{v \searrow_n \square_\Gamma, n_\alpha, \alpha}$$

➪ $\nearrow$-int
$$\frac{}{\square_\Gamma, n_\alpha, \alpha \nearrow_n n_{\alpha\sqcap\alpha}}$$

➪ $n_{\alpha\sqcap\alpha} \sqsupseteq n_\alpha \doteq v$

Case $\searrow$-nil
$$\frac{v \doteq [\,]_\alpha}{v \searrow_{[\,]} \square_\Gamma, [\,]_\alpha, \alpha}$$

➪ $\nearrow$-nil
$$\frac{}{\square_\Gamma, [\,]_\alpha, \alpha \nearrow_{[\,]} [\,]_{\alpha\sqcap\alpha}}$$

➪ $[\,]_{\alpha\sqcap\alpha} \sqsupseteq [\,]_\alpha \doteq v$

Case $\dfrac{v \doteq v_1 :_\beta v_2 \qquad v_1 \searrow_T \rho, e_1, \alpha \qquad v_2 \searrow_U \rho', e_2, \alpha'}{v \searrow_{T:U} \rho \sqcup \rho', e_1 :_\beta e_2, \beta \sqcup \alpha \sqcup \alpha'}$ ↘-cons

$\rho, e_1, \alpha \nearrow_T \sqsupseteq v_1$ IH

$\rho \sqcup \rho', e_1, \beta \sqcup \alpha \sqcup \alpha' \nearrow_T u_1 \sqsupseteq v_1 \quad (\exists u_1)$ monotonicity (1)

$\rho', e_2, \alpha' \nearrow_U \sqsupseteq v_2$ IH

$\rho \sqcup \rho', e_2, \beta \sqcup \alpha \sqcup \alpha' \nearrow_U u_2 \sqsupseteq v_2 \quad (\exists u_2)$ monotonicity (2)

➪ $\dfrac{\rho \sqcup \rho', e_1, \beta \sqcup \alpha \sqcup \alpha' \nearrow_T u_1 \qquad \rho \sqcup \rho', e_2, \beta \sqcup \alpha \sqcup \alpha' \nearrow_U u_2}{\rho \sqcup \rho', e_1 :_\beta e_2, \beta \sqcup \alpha \sqcup \alpha' \nearrow_{T:U} u_1 :_{\beta \sqcap (\beta \sqcup \alpha \sqcup \alpha')} u_2}$ ↗-cons (1, 2)

$\beta \sqcap (\beta \sqcup \alpha \sqcup \alpha') = \beta$

➪ $(u_1 :_{\beta \sqcap (\beta \sqcup \alpha \sqcup \alpha')} u_2) \sqsupseteq (v_1 :_\beta v_2) \doteq v$

Case $\dfrac{\begin{array}{c} v \doteq \langle \vec{u} \mid j_\beta \rangle_\alpha \\ u_i \searrow_{U_i} \rho_i \cdot x\colon i_{\beta_i'}, e_i, \alpha_i' \quad (\forall i \le j) \qquad j_{\beta \sqcup \bigsqcup \vec{\beta}'} \searrow_T \rho', e', \alpha'' \end{array}}{v \searrow_{\langle \vec{U} \mid x \text{ in } T_j \rangle} \bigsqcup \vec{\rho} \sqcup \rho', \langle \bigsqcup \vec{e} \mid x \text{ in } e' \rangle_\alpha, \alpha \sqcup \bigsqcup \vec{\alpha}' \sqcup \alpha''}$ ↘-vector

$\alpha^\dagger = \alpha \sqcup \bigsqcup \vec{\alpha}' \sqcup \alpha''$ define

$\rho', e', \alpha'' \nearrow_T \sqsupseteq j_{\beta \sqcup \bigsqcup \vec{\beta}'}$ IH (3)

$(\bigsqcup \vec{\rho} \sqcup \rho', \alpha^\dagger) \sqsupseteq (\rho', \alpha'')$

$\bigsqcup \vec{\rho} \sqcup \rho', e', \alpha^\dagger \nearrow_T \doteq j_{\beta^\dagger} \sqsupseteq j_{\beta \sqcup \bigsqcup \vec{\beta}'} \quad (\exists j_{\beta^\dagger})$ (3); monotonicity (4)

$\rho_i \cdot x\colon i_{\beta_i'}, e_i, \alpha_i' \nearrow_{U_i} \sqsupseteq u_i \quad (\forall i \le j)$ IH (5)

$(\bigsqcup \vec{\rho} \sqcup \rho', \beta^\dagger, \bigsqcup \vec{e}, \alpha^\dagger) \sqsupseteq (\rho_i, \beta_i', e_i, \alpha_i') \quad (\forall i \le j)$

$(\bigsqcup \vec{\rho} \sqcup \rho') \cdot x\colon i_{\beta^\dagger}, \bigsqcup \vec{e}, \alpha^\dagger \nearrow_{U_i} v_i \sqsupseteq u_i \quad (\forall i \le j) \quad (\exists \vec{v})$ (5); monotonicity (6)

➪ $\dfrac{\begin{array}{c} \bigsqcup \vec{\rho} \sqcup \rho', e', \alpha^\dagger \nearrow_T \doteq j_{\beta^\dagger} \\ (\bigsqcup \vec{\rho} \sqcup \rho') \cdot x\colon i_{\beta^\dagger}, \bigsqcup \vec{e}, \alpha^\dagger \nearrow_{U_i} v_i \quad (\forall i \le j) \end{array}}{\bigsqcup \rho \sqcup \rho', \langle \bigsqcup e \mid x \text{ in } e' \rangle_\alpha, \alpha^\dagger \nearrow_{\langle \vec{U} \mid x \text{ in } T_j \rangle} \langle \vec{v} \mid j_{\beta^\dagger} \rangle_{\alpha \sqcap \alpha^\dagger}}$ ↗-vector (4, 6)

➪ $\langle \vec{v} \mid j_{\beta^\dagger} \rangle_{\alpha \sqcap \alpha^\dagger} \sqsupseteq \langle \vec{u} \mid j_\beta \rangle_\alpha$

Case $\dfrac{\langle \vec{\square} \mid j_{\mathrm{ff}} \rangle_{\mathrm{ff}} \lhd i\colon v \searrow_T \rho, e_1, \alpha \qquad i_{\mathrm{ff}} \searrow_U \rho', e_2, \alpha'}{v \searrow_{T_j \,!\, U_i} \rho \sqcup \rho', e_1 \,!\, e_2, \alpha \sqcup \alpha'}$ ↘-vector-lookup

$\rho, e_1, \alpha \nearrow_T \sqsupseteq \langle \vec{\square} \mid j_{\mathrm{ff}} \rangle_{\mathrm{ff}} \lhd i\colon v$ IH

$\rho \sqcup \rho', e_1, \alpha \sqcup \alpha' \nearrow_T \doteq \langle \vec{u} \mid j_{\beta'} \rangle_\beta \sqsupseteq \langle \vec{\square} \mid j_{\mathrm{ff}} \rangle_{\mathrm{ff}} \lhd i\colon v \quad (\exists \vec{u}, \beta', \beta)$ monotonicity (7)

$$\Rightarrow \quad \frac{\rho \sqcup \rho', e_1, \alpha \sqcup \alpha' \ \nearrow_T \doteq \langle \vec{u} \mid j_{\beta'} \rangle_\beta}{\rho \sqcup \rho', e_1 \,!\, e_2, \alpha \sqcup \alpha' \ \nearrow_{T_j \,!\, U_i} u_i} \ i \leq j \qquad (7)$$

(nearrow-vector-lookup)

$\Rightarrow u_i \sqsupseteq v$

Case $\dfrac{v \doteq j_\beta \qquad \langle \vec{\square} \mid j_\beta \rangle_{\mathsf{ff}} \searrow_T \rho, e, \alpha}{v \searrow_{\mathtt{len}\ T_j} \rho, \mathtt{len}\ e, \alpha}$ (searrow-vector-length)

$\rho, e, \alpha \ \nearrow_T \doteq \langle \vec{v} \mid j_{\beta'} \rangle_{\alpha'} \sqsupseteq \langle \vec{\square} \mid j_\beta \rangle_{\mathsf{ff}} \quad (\exists \vec{v}, \beta', \alpha')$ IH

$$\Rightarrow \quad \frac{\rho, e, \alpha \ \nearrow_T \doteq \langle \vec{v} \mid j_{\beta'} \rangle_{\alpha'}}{\rho, \mathtt{len}\ e, \alpha \ \nearrow_{\mathtt{len}\ T_j} j_{\beta'}}$$

(nearrow-vector-length)

$\Rightarrow j_{\beta'} \sqsupseteq j_\beta \doteq v$

Case $\dfrac{v \doteq \phi(\vec{u} \cdot u') \qquad \phi(\vec{u}) \searrow_T \rho, e_1, \alpha \qquad u' \searrow_U \rho', e_2, \alpha'}{v \searrow_{T_{(\phi, \vec{n})}\ U_m} \rho \sqcup \rho', e_1\ e_2, \alpha \sqcup \alpha'}$ (searrow-apply-prim-unsat)

$\rho, e_1, \alpha \ \nearrow_T \sqsupseteq \phi(\vec{u})$ IH

$\rho \sqcup \rho', e_1, \alpha \sqcup \alpha' \ \nearrow_T \doteq \phi(\vec{v}) \sqsupseteq \vec{u} \quad (\exists \vec{v})$ monotonicity (8)

$\rho, e_2, \alpha \ \nearrow_U \sqsupseteq u'$ IH

$\rho \sqcup \rho', e_2, \alpha \sqcup \alpha' \ \nearrow_U \doteq v' \sqsupseteq u' \quad (\exists v')$ monotonicity (9)

$$\Rightarrow \quad \frac{\begin{array}{c}\rho \sqcup \rho', e_1, \alpha \sqcup \alpha' \ \nearrow_T \doteq \phi(\vec{v}) \\ \rho \sqcup \rho', e_2, \alpha \sqcup \alpha' \ \nearrow_U v'\end{array}}{\rho \sqcup \rho', e_1\ e_2, \alpha \sqcup \alpha' \ \nearrow_{T_{(\phi, \vec{n})}\ U_m} \phi(\vec{v} \cdot v')} \ \mathsf{arity}(\phi) > |\vec{n}| + 1 \qquad (8, 9)$$

(nearrow-apply-prim-unsat)

$\Rightarrow \phi(\vec{v} \cdot v') \sqsupseteq \phi(\vec{u} \cdot u') \doteq v$

Case $\dfrac{\begin{array}{c}v \doteq n'_\beta \qquad \phi\text{–bwd}_{\vec{n} \cdot m}(n'_\beta) = \vec{u} \cdot u' \\ \phi(\vec{u}) \searrow_T \rho, e_1, \alpha \qquad u' \searrow_U \rho', e_2, \alpha'\end{array}}{v \searrow_{T_{(\phi, \vec{n})}\ U_m} \rho \sqcup \rho', e_1\ e_2, \alpha \sqcup \alpha'}$ (searrow-apply-prim-sat)

$\rho, e_1, \alpha \ \nearrow_T \sqsupseteq \phi(\vec{u})$ IH

$\rho \sqcup \rho', e_1, \alpha \sqcup \alpha' \ \nearrow_T \doteq \phi(\vec{v}) \sqsupseteq \phi(\vec{u}) \quad (\exists \vec{v})$ monotonicity (10)

$\rho, e_2, \alpha \ \nearrow_U \sqsupseteq u'$ IH

$\rho \sqcup \rho', e_2, \alpha \sqcup \alpha' \ \nearrow_U \doteq v' \sqsupseteq u' \quad (\exists v')$ monotonicity (11)

$\nearrow$-apply-prim-sat

$$\dfrac{\begin{array}{c}\rho \sqcup \rho', e_1, \alpha \sqcup \alpha' \nearrow_T \doteq \phi(\vec{v}) \\ \rho \sqcup \rho', e_2, \alpha \sqcup \alpha' \nearrow_U v'\end{array}}{\rho \sqcup \rho', e_1\ e_2, \alpha \sqcup \alpha' \nearrow_{T_{(\phi,\vec{n})}\ U_m} \phi\text{–fwd}_{\vec{n}\cdot m}(\vec{v} \cdot v')}\ \text{arity}(\phi) = |\vec{n}| + 1 \quad (10, 11)$$

$\Rightarrow \phi\text{–fwd}_{\vec{n}\cdot m}(\vec{v} \cdot v') \sqsupseteq \phi\text{–fwd}_{\vec{n}\cdot m}(\vec{u} \cdot u') \sqsupseteq n'_\beta \doteq v$ monotonicity

---

Case $\searrow$-apply

$$\dfrac{v \searrow_{T'} \rho_1 \cdot \rho_2 \cdot \rho_3, e, \beta \qquad \rho_3, e, \beta \rightsquigarrow_w v', \sigma \qquad v' \searrow_U \rho, e_2, \alpha \qquad \rho_2 \searrow \rho'_1, h \qquad \mathtt{cl}(\rho_1 \sqcup \rho'_1, h, \sigma) \searrow_T \rho', e_1, \alpha'}{v \searrow_{T\ U \blacktriangleright w:\ T'} \rho \sqcup \rho', e_1\ e_2, \alpha \sqcup \alpha'}$$

$\rho', e_1, \alpha' \nearrow_T \sqsupseteq \mathtt{cl}(\rho_1 \sqcup \rho'_1, h, \sigma)$ IH

$\rho \sqcup \rho', e_1, \alpha \sqcup \alpha' \nearrow_T \doteq \mathtt{cl}(\rho^\dagger, h', \sigma') \sqsupseteq \mathtt{cl}(\rho_1 \sqcup \rho'_1, h, \sigma) \quad (\exists \rho^\dagger, h', \sigma')$ monotonicity (12)

$\rho'_1, h \twoheadrightarrow \sqsupseteq \rho_2$ Theorem 3.10

$\rho^\dagger, h' \twoheadrightarrow \rho'_2 \sqsupseteq \rho_2 \quad (\exists \rho'_2)$ monotonicity (13)

$\rho, e_2, \alpha \nearrow_U \sqsupseteq v'$ IH

$\rho \sqcup \rho', e_2, \alpha \sqcup \alpha' \nearrow_U u' \sqsupseteq v' \quad (\exists u')$ monotonicity (14)

$v', \sigma \nrightarrow_w \sqsupseteq \rho_3, e, \beta$ Theorem 3.8

$u', \sigma' \nrightarrow_w \rho'_3, e', \beta' \sqsupseteq \rho_3, e, \beta \quad (\exists \rho'_3, e', \beta')$ monotonicity (15)

$\rho_1 \cdot \rho_2 \cdot \rho_3, e, \beta \nearrow_{T'} \sqsupseteq v$ IH

$\rho^\dagger \cdot \rho'_2 \cdot \rho'_3, e', \beta' \nearrow_{T'} u \sqsupseteq v \quad (\exists u)$ monotonicity (16)

$\nearrow$-apply

$$\Rightarrow \dfrac{\begin{array}{c}\rho \sqcup \rho', e_1, \alpha \sqcup \alpha' \nearrow_T \doteq \mathtt{cl}(\rho^\dagger, h', \sigma') \\ \rho^\dagger, h' \twoheadrightarrow \rho'_2 \qquad \rho \sqcup \rho', e_2, \alpha \sqcup \alpha' \nearrow_U u' \\ u', \sigma' \nrightarrow_w \rho'_3, e', \beta' \qquad \rho^\dagger \cdot \rho'_2 \cdot \rho'_3, e', \beta' \nearrow_{T'} u\end{array}}{\rho \sqcup \rho', e_1\ e_2, \alpha \sqcup \alpha' \nearrow_{T\ U \blacktriangleright w:\ T'} u} \quad (12, 13, 14, 15, 16)$$

Case $\searrow$-let-rec

$$\dfrac{v \searrow_T \rho \cdot \rho_1, e, \alpha \qquad \rho_1 \searrow \rho', h'}{v \searrow_{\mathtt{let}\ h\ \mathtt{in}\ T} \rho \sqcup \rho', \mathtt{let}\ h'\ \mathtt{in}\ e, \alpha}$$

$\rho \cdot \rho_1, e, \alpha \nearrow_T \sqsupseteq v$ IH

$(\rho \sqcup \rho') \cdot \rho_1, e, \alpha \nearrow_T u \sqsupseteq v \quad (\exists u)$ monotonicity (17)

$\rho', h' \searrow \sqsupseteq \rho_1$ Theorem 3.10

$\rho \sqcup \rho', h' \searrow \rho'_1 \sqsupseteq \rho_1 \quad (\exists \rho'_1)$ monotonicity (18)

$\nearrow$-let-rec

$$\Rightarrow \dfrac{\rho \sqcup \rho', h' \twoheadrightarrow \rho_1 \qquad (\rho \sqcup \rho') \cdot \rho_1, e, \alpha \nearrow_T u}{\rho \sqcup \rho', \mathtt{let}\ h'\ \mathtt{in}\ e, \alpha \nearrow_{\mathtt{let}\ h\ \mathtt{in}\ T} u} \quad (17, 18)$$

$\Rightarrow u \sqsupseteq v$

□

B.5.2 Backward after forward direction. Induction on the $\nearrow$ derivation.

Proof.

Case $\dfrac{e \doteq x \qquad x\colon v \in \rho}{\rho, e, \alpha \nearrow_x v}\ \nearrow\text{-var}$

$\rho \sqsupseteq \rho' \ni_\Gamma x\colon v \quad (\exists \rho')$ (totality; Lemma 3.9)

$\Rightarrow$ $\dfrac{\rho' \ni_\Gamma x\colon v}{v \searrow_x \rho', x, \mathsf{ff}}\ \searrow\text{-var}$

$\Rightarrow (\rho', x, \mathsf{ff}) \sqsubseteq (\rho, x, \alpha)$

Case $\dfrac{e \doteq (\oplus) \qquad \oplus\colon v \in \rho}{\rho, e, \alpha \nearrow_{(\oplus)_\Gamma} v}\ \nearrow\text{-op}$

$\rho \sqsupseteq \rho' \ni_\Gamma \oplus\colon v \quad (\exists \rho')$ (totality; Lemma 3.9)

$\Rightarrow$ $\dfrac{\rho' \ni_\Gamma \oplus\colon v}{v \searrow_{(\oplus)_\Gamma} \rho', (\oplus), \mathsf{ff}}\ \searrow\text{-op}$

$\Rightarrow (\rho', (\oplus), \mathsf{ff}) \sqsubseteq (\rho, (\oplus), \alpha)$

Case $\dfrac{e \doteq \lambda\sigma}{\rho, e, \alpha \nearrow_{\lambda\sigma'} \mathtt{cl}(\rho, \varepsilon, \sigma)}\ \nearrow\text{-lambda}$

$\Rightarrow$ $\dfrac{}{\mathtt{cl}(\rho, \varepsilon, \sigma) \searrow_{\lambda\sigma'} \rho, \lambda\sigma, \mathsf{ff}}\ \searrow\text{-lambda}$

$\Rightarrow (\rho, \lambda\sigma, \mathsf{ff}) \sqsubseteq (\rho, \lambda\sigma, \alpha)$

Case $\dfrac{e \doteq n_\alpha}{\rho, e, \alpha' \nearrow_n n_{\alpha \sqcap \alpha'}}\ \nearrow\text{-int}$

$\Rightarrow$ $\dfrac{}{n_{\alpha \sqcap \alpha'} \searrow_n \square_\Gamma, n_{\alpha \sqcap \alpha'}, \alpha \sqcap \alpha'}\ \searrow\text{-int}$

$\Rightarrow (\square_\Gamma, n_{\alpha \sqcap \alpha'}, \alpha \sqcap \alpha') \sqsubseteq (\rho, n_\alpha, \alpha)$

Case $\dfrac{e \doteq [\,]_\alpha}{\rho, e, \alpha' \nearrow_{[\,]} [\,]_{\alpha \sqcap \alpha'}}$ $\nearrow$-nil

$\Rightarrow$ $\dfrac{}{[\,]_{\alpha \sqcap \alpha'} \searrow_{[\,]} \square_\Gamma, [\,]_{\alpha \sqcap \alpha'}, \alpha \sqcap \alpha'}$ $\searrow$-nil

$\Rightarrow (\square_\Gamma, [\,]_{\alpha \sqcap \alpha'}, \alpha \sqcap \alpha') \sqsubseteq (\rho, [\,]_\alpha, \alpha)$

Case $\dfrac{e \doteq e_1 :_\alpha e_2 \qquad \rho, e_1, \alpha' \nearrow_T v_1 \qquad \rho, e_2, \alpha' \nearrow_U v_2}{\rho, e, \alpha' \nearrow_{T:U} v_1 :_{\alpha \sqcap \alpha'} v_2}$ $\nearrow$-cons

$v_1 \searrow_T \rho_1, e_1', \beta \sqsubseteq \rho, e_1, \alpha' \quad (\exists \rho_1, e_1', \beta)$ IH (1)

$v_2 \searrow_U \rho_2, e_2', \beta' \sqsubseteq \rho, e_2, \alpha' \quad (\exists \rho_2, e_2', \beta')$ IH (2)

$\Rightarrow$ $\dfrac{v_1 \searrow_T \rho_1, e_1', \beta \qquad v_2 \searrow_U \rho_2, e_2', \beta'}{v_1 :_{\alpha \sqcap \alpha'} v_2 \searrow_{T:U} \rho_1 \sqcup \rho_2, e_1' :_{\alpha \sqcap \alpha'} e_2', (\alpha \sqcap \alpha') \sqcup \beta \sqcup \beta'}$ $\searrow$-cons (1, 2)

$\Rightarrow (\rho_1 \sqcup \rho_2, e_1' :_{\alpha \sqcap \alpha'} e_2', (\alpha \sqcap \alpha') \sqcup \beta \sqcup \beta') \sqsubseteq (\rho, e_1 :_\alpha e_2, \alpha')$

Case $\dfrac{e \doteq \langle e_1 \mid x \texttt{ in } e_2 \rangle_\alpha \qquad \rho, e_2, \alpha' \nearrow_T \doteq j_\beta \qquad \rho \cdot x{:}\, i_\beta, e_1, \alpha' \nearrow_{U_i} v_i \quad (\forall i \le j)}{\rho, e, \alpha' \nearrow_{\langle \vec{U} \mid x \texttt{ in } T_j \rangle} \langle \vec{v} \mid j_\beta \rangle_{\alpha \sqcap \alpha'}}$ $\nearrow$-vector

$v_i \searrow_{U_i} \rho_i' \cdot x{:}\, i_{\beta_i''}, e_i', \beta_i' \sqsubseteq \rho \cdot x{:}\, i_\beta, e_1, \alpha' \quad (\forall i \le j) \quad (\exists \vec{\rho}', \vec{\beta}'', \vec{e}', \vec{\beta}')$ IH (3)

$j_\beta \searrow_T \sqsubseteq \rho, e_2, \alpha'$ IH

$j_{\beta \sqcup \bigsqcup \vec{\beta}''} \searrow_T \rho_2, e_2', \alpha'' \sqsubseteq \rho, e_2, \alpha' \quad (\exists \rho_2, e_2', \alpha'')$ monotonicity (4)

$\Rightarrow$ $\dfrac{v_i \searrow_{U_i} \rho_i' \cdot x{:}\, i_{\beta_i''}, e_i', \beta_i' \quad (\forall i \le j) \qquad j_{\beta \sqcup \bigsqcup \beta''} \searrow_T \rho_2, e_2', \alpha''}{\langle \vec{v} \mid j_\beta \rangle_{\alpha \sqcap \alpha'} \searrow_{\langle \vec{U} \mid x \texttt{ in } T_j \rangle} \bigsqcup \vec{\rho}' \sqcup \rho_2, \langle \bigsqcup \vec{e}' \mid x \texttt{ in } e_2' \rangle_{\alpha \sqcap \alpha'}, (\alpha \sqcap \alpha') \sqcup \bigsqcup \vec{\beta}' \sqcup \alpha''}$ $\searrow$-vector (4, 3)

$\Rightarrow (\bigsqcup \vec{\rho}' \sqcup \rho_2, \langle \bigsqcup \vec{e}' \mid x \texttt{ in } e_2' \rangle_{\alpha \sqcap \alpha'}) \sqsubseteq (\rho, \langle e_1 \mid x \texttt{ in } e_2 \rangle_\alpha)$

$\Rightarrow (\alpha \sqcap \alpha') \sqcup \bigsqcup \vec{\beta}' \sqcup \alpha'' \sqsubseteq \alpha'$

Case $\dfrac{e \doteq e_1 \,!\, e_2 \qquad \rho, e_1, \alpha \nearrow_T \doteq \langle \vec{v} \mid j_{\alpha'} \rangle_\beta}{\rho, e, \alpha \nearrow_{T_j \,!\, U_i} v_i} \; i \le j$ $\nearrow$-vector-lookup

$\langle \vec{v} \mid j_{\alpha'} \rangle_\beta \searrow_T \sqsubseteq \rho, e_1, \alpha$ IH

$\langle \vec{\square} \mid j_{\mathrm{ff}} \rangle_{\mathrm{ff}} \lhd i{:}\, v_i \searrow_T \rho_1, e_1', \beta' \sqsubseteq \rho, e_1, \alpha \quad (\exists \rho_1, e_1', \beta')$ monotonicity (5)

$\rho, e_2, \alpha \nearrow_U \doteq i_{\alpha''} \quad (\exists \alpha'')$ codomain of $\nearrow_U$

$i_{\alpha''} \searrow_U \sqsubseteq \rho, e_2, \alpha$ IH

$i_{\mathsf{ff}} \searrow_U \rho_2, e_2', \beta'' \sqsubseteq \rho, e_2, \alpha \quad (\exists \rho_2, e_2', \beta'')$ monotonicity (6)

$\searrow$-vector-lookup

$$\Rightarrow \quad \frac{\langle \vec{\square} \mid j_{\mathsf{ff}} \rangle_{\mathsf{ff}} \lhd i \colon v_i \searrow_T \rho_1, e_1', \beta' \qquad i_{\mathsf{ff}} \searrow_U \rho_2, e_2', \beta''}{v_i \searrow_{T_j \,!\, U_i} \rho_1 \sqcup \rho_2, e_1' \,!\, e_2', \beta' \sqcup \beta''} \qquad (7, 6)$$

$\Rightarrow (\rho_1 \sqcup \rho_2, e_1' \,!\, e_2', \beta' \sqcup \beta'') \sqsubseteq (\rho, e_1 \,!\, e_2, \alpha)$

Case $\nearrow$-vector-length

$$\frac{e \doteq \mathtt{len}\ e' \qquad \rho, e', \alpha \nearrow_T \doteq \langle \vec{v} \mid j_{\alpha'} \rangle_\beta}{\rho, e, \alpha \nearrow_{\mathtt{len}\ T_j} j_{\alpha'}}$$

$\langle \vec{v} \mid j_{\alpha'} \rangle_\beta \searrow_T \sqsubseteq \rho, e', \alpha$ IH

$\langle \vec{\square} \mid j_{\alpha'} \rangle_{\mathsf{ff}} \searrow_T \rho', e'', \beta \sqsubseteq \rho, e', \alpha \quad (\exists \rho', e'', \beta)$ monotonicity (7)

$\searrow$-vector-length

$$\Rightarrow \quad \frac{\langle \vec{\square} \mid j_{\alpha'} \rangle_{\mathsf{ff}} \searrow_T \rho', e'', \beta}{j_{\alpha'} \searrow_{\mathtt{len}\ T_j} \rho', \mathtt{len}\ e'', \beta} \qquad (7, 6)$$

$\Rightarrow (\rho', \mathtt{len}\ e'', \beta) \sqsubseteq (\rho, \mathtt{len}\ e', \alpha)$

Case $\nearrow$-apply-prim-unsat

$$\frac{e \doteq e_1\ e_2 \qquad \rho, e_1, \alpha \nearrow_T \phi(\vec{v}) \qquad \rho, e_2, \alpha \nearrow_U u}{\rho, e, \alpha \nearrow_{T_{(\phi, \vec{n})}\ U_m} \phi(\vec{v} \cdot u)}\ \mathsf{arity}(\phi) > |\vec{n}| + 1$$

$\phi(\vec{v}) \searrow_T \rho_1, e_1', \beta \sqsubseteq \rho, e_1, \alpha \quad (\exists \rho_1, e_1', \beta)$ IH (8)

$u \searrow_U \rho_2, e_2', \beta' \sqsubseteq \rho, e_2, \alpha \quad (\exists \rho_2, e_2', \beta')$ IH (9)

$\searrow$-apply-prim-unsat

$$\Rightarrow \quad \frac{\phi(\vec{v}) \searrow_T \rho_1, e_1', \beta \qquad u \searrow_U \rho_2, e_2', \beta'}{\phi(\vec{v} \cdot u) \searrow_{T_{(\phi, \vec{n})}\ U_m} \rho_1 \sqcup \rho_2, e_1'\ e_2', \beta \sqcup \beta'} \qquad (8, 9)$$

$\Rightarrow (\rho_1 \sqcup \rho_2, e_1'\ e_2', \beta \sqcup \beta') \sqsubseteq (\rho, e_1\ e_2, \alpha)$

Case $\nearrow$-apply-prim-sat

$$\frac{e \doteq e_1\ e_2 \qquad \rho, e_1, \alpha \nearrow_T \phi(\vec{v}) \qquad \rho, e_2, \alpha \nearrow_U u}{\rho, e, \alpha \nearrow_{T_{(\phi, \vec{n})}\ U_m} \phi\text{–fwd}_{\vec{n} \cdot m}(\vec{v} \cdot u)}\ \mathsf{arity}(\phi) = |\vec{n}| + 1$$

$\phi\text{–bwd}_{\vec{n} \cdot m}(\phi\text{–fwd}_{\vec{n} \cdot m}(\vec{v} \cdot u)) = \vec{u} \cdot u' \sqsubseteq \vec{v} \cdot u \quad (\exists \vec{u}, u')$ GC for ϕ (10)

$\phi(\vec{v}) \searrow_T \rho_1, e_1', \beta \sqsubseteq \rho, e_1, \alpha \quad (\exists \rho_1, e_1', \beta)$ IH (11)

$u \searrow_U \rho_2, e_2', \beta' \sqsubseteq \rho, e_2, \alpha \quad (\exists \rho_2, e_2', \beta')$ IH (12)

$\searrow$-apply-prim-sat

$$\dfrac{\phi\text{–bwd}_{\vec{n}\cdot m}(\phi\text{–fwd}_{\vec{n}\cdot m}(\vec{v}\cdot u)) = \vec{u}\cdot u' \qquad \phi(\vec{u}) \searrow_T \rho_1, e_1', \beta \qquad u' \searrow_U \rho_2, e_2', \beta'}{\phi\text{–fwd}_{\vec{n}\cdot m}(\vec{v}\cdot u) \searrow_{T_{(\phi,\vec{n})}\ U_m} \rho_1 \sqcup \rho_2, e_1'\ e_2', \beta \sqcup \beta'} \quad (10, 11, 12)$$

$\Rightarrow (\rho_1 \sqcup \rho_2, e_1'\ e_2', \beta \sqcup \beta') \sqsubseteq (\rho, e_1\ e_2, \alpha)$

Case $\nearrow$-apply

$$\dfrac{e \doteq e_1\ e_2 \qquad \rho, e_1, \alpha \nearrow_T \doteq \mathtt{cl}(\rho_1, h, \sigma) \qquad \rho_1, h \twoheadrightarrow \rho_2 \qquad \rho, e_2, \alpha \nearrow_U v \qquad v, \sigma \nearrow_w \rho_3, e', \beta \qquad \rho_1 \cdot \rho_2 \cdot \rho_3, e', \beta \nearrow_{T'} v'}{\rho, e, \alpha \nearrow_{T\ U \blacktriangleright w:\ T'} v'}$$

$v' \searrow_{T'} \rho_1' \cdot \rho_2' \cdot \rho_3', e'', \beta' \sqsubseteq \rho_1 \cdot \rho_2 \cdot \rho_3, e', \beta \quad (\exists \rho_1', \rho_2', \rho_3', e'', \beta')$ IH (13)

$\rho_3, e', \beta \curvearrowright_w \sqsubseteq v, \sigma$ Theorem 3.8

$\rho_3', e'', \beta' \curvearrowright_w u, \sigma' \sqsubseteq v, \sigma \quad (\exists u, \sigma')$ monotonicity (14)

$v \searrow_U \sqsubseteq \rho, e_2, \alpha$ IH

$u \searrow_U \rho^\dagger, e_2', \alpha' \sqsubseteq \rho, e_2, \alpha \quad (\exists \rho^\dagger, e_2', \alpha')$ monotonicity (15)

$\rho_2 \searrow \sqsubseteq \rho_1, h$ Theorem 3.10

$\rho_2' \searrow \rho_1'', h' \sqsubseteq \rho_1, h \quad (\exists \rho_1'', h')$ monotonicity (16)

$\mathtt{cl}(\rho_1, h, \sigma) \searrow_T \sqsubseteq \rho, e_1, \alpha$ IH

$\mathtt{cl}(\rho_1' \sqcup \rho_1'', h', \sigma') \searrow_T \rho^\ddagger, e_1', \alpha'' \sqsubseteq \rho, e_1, \alpha \quad (\exists \rho^\ddagger, e_1', \alpha'')$ monotonicity (17)

$\searrow$-apply

$$\dfrac{v' \searrow_{T'} \rho_1' \cdot \rho_2' \cdot \rho_3', e'', \beta' \qquad \rho_3', e'', \beta' \curvearrowright_w u, \sigma' \qquad u \searrow_U \rho^\dagger, e_2', \alpha' \qquad \rho_2' \searrow \rho_1'', h' \qquad \mathtt{cl}(\rho_1' \sqcup \rho_1'', h', \sigma') \searrow_T \rho^\ddagger, e_1', \alpha''}{v' \searrow_{T\ U \blacktriangleright w:\ T'} \rho^\dagger \sqcup \rho^\ddagger, e_1'\ e_2', \alpha' \sqcup \alpha''} \quad (13, 14)$$

$\Rightarrow (\rho^\dagger \sqcup \rho^\ddagger, e_1'\ e_2', \alpha' \sqcup \alpha'') \sqsubseteq (\rho, e_1\ e_2, \alpha)$

Case $\nearrow$-let-rec

$$\dfrac{e \doteq \mathtt{let}\ h'\ \mathtt{in}\ e' \qquad \rho, h' \twoheadrightarrow \rho_1 \qquad \rho \cdot \rho_1, e', \alpha \nearrow_T v}{\rho, e, \alpha \nearrow_{\mathtt{let}\ h\ \mathtt{in}\ T} v}$$

$v \searrow_T \rho' \cdot \rho_1', e'', \beta \sqsubseteq \rho \cdot \rho_1, e', \alpha \quad (\exists \rho', \rho_1', e'', \beta)$ IH (18)

$\rho_1 \searrow \sqsubseteq \rho, h'$ Theorem 3.10

$\rho_1' \searrow \rho'', h'' \sqsubseteq \rho, h' \quad (\exists \rho'', h'')$ monotonicity (19)

$\searrow$-let-rec

$$\dfrac{v \searrow_T \rho' \cdot \rho_1', e'', \beta \qquad \rho_1' \searrow \rho'', h''}{v \searrow_{\mathtt{let}\ h\ \mathtt{in}\ T} \rho' \sqcup \rho'', \mathtt{let}\ h''\ \mathtt{in}\ e'', \beta} \quad (18, 19)$$

$\Rightarrow (\rho' \sqcup \rho'', \mathtt{let}\ h''\ \mathtt{in}\ e'', \beta) \sqsubseteq (\rho, \mathtt{let}\ h'\ \mathtt{in}\ e', \alpha)$

□

C PROOFS: SURFACE LANGUAGE

C.1 Auxiliary lemmas

Definition C.1. Suppose $r \nearrow e$. Define $\nearrow_r : \mathsf{Sel}_r\,\mathcal{A} \to \mathsf{Sel}_e\,\mathcal{A}$ and $\searrow_r : \mathsf{Sel}_e\,\mathcal{A} \to \mathsf{Sel}_r\,\mathcal{A}$ to be $\nearrow$ domain-restricted to $\mathsf{Sel}_r\,\mathcal{A}$ and $\searrow_r$ domain-restricted to $\mathsf{Sel}_e\,\mathcal{A}$ respectively.

Lemma C.2 (Galois connection for desugaring list rest). *Suppose $r \nearrow e$. Then:*

(1) $\nearrow_r$ *and* $\searrow_r$ *are monotonic.*
(2) $\nearrow_r (\searrow_r (e')) \sqsupseteq e'$.
(3) $\searrow_r (\nearrow_r (r')) \sqsubseteq r'$.

Definition C.3. Suppose $\vec{p}, e \nearrow \sigma$. Define $\mathsf{clause{-}fwd}_{\vec{p}=e} : \mathsf{Sel}_e\,\mathcal{A} \to \mathsf{Sel}_\sigma\,\mathcal{A}$ so that $\mathsf{clause{-}fwd}_{\vec{p}=e}(e') = \sigma'$ iff $p, e' \nearrow \sigma'$ and $\mathsf{clause{-}bwd}_{\vec{p}=e} : \mathsf{Sel}_\sigma\,\mathcal{A} \to \mathsf{Sel}_e\,\mathcal{A}$ so that $\mathsf{clause{-}bwd}_{\vec{p}=e}(\sigma') = e'$ iff $\sigma' \searrow_p e'$.

Lemma C.4 (Galois connection for clause). *Suppose $\vec{p}, e \nearrow \sigma$. Then:*

(1) $\mathsf{clause{-}fwd}_{\vec{p}=e}$ *and* $\mathsf{clause{-}bwd}_{\vec{p}=e}$ *are monotonic.*
(2) $\mathsf{clause{-}fwd}_{\vec{p}=e}(\mathsf{clause{-}bwd}_{\vec{p}=e}(\sigma')) \sqsupseteq \sigma'$.
(3) $\mathsf{clause{-}bwd}_{\vec{p}=e}(\mathsf{clause{-}fwd}_{\vec{p}=e}(e')) \sqsubseteq (e')$.

Definition C.5. Suppose $\vec{c} \nearrow \sigma$. Define $\mathsf{clauses{-}fwd}_{\vec{c}} : \mathsf{Sel}_{\vec{c}}\,\mathcal{A} \to \mathsf{Sel}_\sigma\,\mathcal{A}$ and $\mathsf{clauses{-}bwd}_{\vec{c}} : \mathsf{Sel}_\sigma\,\mathcal{A} \to \mathsf{Sel}_{\vec{c}}\,\mathcal{A}$ to be $\nearrow$ domain-restricted to $\mathsf{Sel}_{\vec{c}}\,\mathcal{A}$ and $\searrow_{\vec{c}}$ domain-restricted to $\mathsf{Sel}_\sigma\,\mathcal{A}$ respectively.

Lemma C.6 (Galois connection for clauses). *Suppose $\vec{c} \nearrow \sigma$. Then:*

(1) $\mathsf{clauses{-}fwd}_{\vec{c}}$ *and* $\mathsf{clauses{-}bwd}_{\vec{c}}$ *are monotonic.*
(2) $\mathsf{clauses{-}fwd}_{\vec{c}}(\mathsf{clauses{-}bwd}_{\vec{c}}(\sigma')) \sqsupseteq \sigma'$.
(3) $\mathsf{clauses{-}bwd}_{\vec{c}}(\mathsf{clauses{-}fwd}_{\vec{c}}(\vec{c})) \sqsubseteq \vec{c}'$.

Definition C.7. Suppose $\kappa, \alpha \nearrow_{\vec{\pi}} \kappa'$. Define $\mathsf{totalise{-}fwd}_{\kappa,\alpha,\vec{\pi}} : \mathsf{Sel}_{(\kappa,\alpha)}\,\mathcal{A} \to \mathsf{Sel}_{\kappa'}\,\mathcal{A}$ and $\mathsf{totalise{-}bwd}_{\kappa,\alpha,\vec{\pi}} : \mathsf{Sel}_{\kappa'}\,\mathcal{A} \to \mathsf{Sel}_{(\kappa,\alpha)}\,\mathcal{A}$ to be $\nearrow_{\vec{\pi}}$ domain-restricted to $\mathsf{Sel}_{(\kappa,\alpha)}\,\mathcal{A}$ and $\searrow_{\vec{\pi}}$ domain-restricted to $\mathsf{Sel}_{\kappa'}\,\mathcal{A}$ respectively.

Lemma C.8 (Galois connection for totalise).
Suppose $\kappa, \alpha \nearrow_{\vec{\pi}} \kappa'$. Then:

(1) $\mathsf{totalise{-}fwd}_{\kappa,\alpha,\vec{\pi}}$ *and* $\mathsf{totalise{-}bwd}_{\kappa,\alpha,\vec{\pi}}$ *are monotonic.*
(2) $\mathsf{totalise{-}fwd}_{\kappa,\alpha,\vec{\pi}}(\mathsf{totalise{-}bwd}_{\kappa,\alpha,\vec{\pi}}(\kappa^\dagger)) \sqsupseteq \kappa^\dagger$.
(3) $\mathsf{totalise{-}bwd}_{\kappa,\alpha,\vec{\pi}}(\mathsf{totalise{-}fwd}_{\kappa,\alpha,\vec{\pi}}(\kappa^\dagger, \alpha')) \sqsubseteq (\kappa^\dagger, \alpha')$.

C.2 Theorem 5.1

C.2.1 Forwards after backwards direction. Induction on the $\searrow$ derivation.

Proof.

Case $\dfrac{e \doteq (\oplus)\ e_1\ e_2 \qquad e_1 \searrow_{s_1} s_1' \qquad e_2 \searrow_{s_2} s_2'}{e \searrow_{s_1 \oplus s_2} s_1' \oplus s_2'}\ \searrow\text{-binary-apply}$

$s_1' \nearrow e_1' \sqsupseteq e_1 \quad (\exists e_1')$ (IH)

$s_2' \nearrow e_2' \sqsupseteq e_2 \quad (\exists e_2')$ (IH)

$\nearrow$-binary-apply

$$\frac{s_1' \nearrow e_1' \qquad s_2' \nearrow e_2'}{s_1' \oplus s_2' \nearrow (\oplus)\ e_1'\ e_2'}$$

$\Rightarrow$

$\Rightarrow (\oplus)\ e_1'\ e_2' \sqsupseteq (\oplus)\ e_1\ e_2 \doteq e$

Case

$\searrow$-nil

$$\frac{e \doteq [\,]_\alpha}{e \searrow_{[\,]} [\,]_\alpha}$$

$\nearrow$-nil

$\Rightarrow$

$$\frac{}{[\,]_\alpha \nearrow [\,]_\alpha}$$

$\Rightarrow [\,]_\alpha \sqsupseteq [\,]_\alpha \doteq e$

Case

$\searrow$-non-empty-list

$$\frac{e \doteq e_1 :_\alpha e_2 \qquad e_1 \searrow_s s' \qquad e_2 \searrow_l l'}{e \searrow_{[\ s\ l} [_\alpha\ s'\ l'}$$

$s' \nearrow e_1' \sqsupseteq e_1 \quad (\exists e_1')$ (IH)

$l' \nearrow e_2' \sqsupseteq e_2 \quad (\exists e_2')$ (Lemma C.2)

$\nearrow$-non-empty-list

$\Rightarrow$

$$\frac{s' \nearrow e_1' \qquad l' \nearrow e_2'}{[_\alpha\ s'\ l' \nearrow e_1' :_\alpha e_2'}$$

$\Rightarrow e_1' :_\alpha e_2' \sqsupseteq e_1 :_\alpha e_2 \doteq e$

Case

$\searrow$-cons

$$\frac{e \doteq e_1 :_\alpha e_2 \qquad e_1 \searrow_{s_1} s_1' \qquad e_2 \searrow_{s_2} s_2'}{e \searrow_{s_1\ :\ s_2} s_1' :_\alpha s_2'}$$

$s_1' \nearrow e_1' \sqsupseteq e_1 \quad (\exists e_1')$ (IH)

$s_2' \nearrow e_2' \sqsupseteq e_2 \quad (\exists e_2')$ (IH)

$\nearrow$-cons

$\Rightarrow$

$$\frac{s_1' \nearrow e_1' \qquad s_2' \nearrow e_2'}{s_1' :_\alpha s_2' \nearrow e_1' :_\alpha e_2'}$$

$\Rightarrow e_1' :_\alpha e_2' \sqsupseteq e_1 :_\alpha e_2 \doteq e$

Case

$\searrow$-let-rec

$$\frac{e \doteq \texttt{let}\ x_1 \colon \sigma_1 \cdot \ldots \cdot x_j \colon \sigma_j\ \texttt{in}\ e_1 \qquad \sigma_i \searrow_{\vec{c_i}} \vec{c_i}' \quad (\forall i \le j) \qquad e_1 \searrow_s s'}{e \searrow_{\texttt{let}\ x_1 \colon \vec{c_1} \cdot \ldots \cdot x_j \colon \vec{c_j}\ \texttt{in}\ s} \texttt{let}\ x_1 \colon \vec{c_1}' \cdot \ldots \cdot x_j \colon \vec{c_j}'\ \texttt{in}\ s'}$$

$\vec{c_i}' \nearrow \sigma_i' \sqsupseteq \sigma_i \quad (\forall i \le j) \quad (\exists \vec{\sigma}')$ (Lemma C.6)

$s' \nearrow e' \sqsupseteq e \quad (\exists e')$ (IH)

$$\Rightarrow \quad \frac{\vec{c_i}' \nearrow \sigma_i' \quad (\forall i \le j) \qquad s' \nearrow e'}{\texttt{let}\ x_1\colon \vec{c_1}' \cdot .. \cdot x_j\colon \vec{c_j}'\ \texttt{in}\ s' \nearrow \texttt{let}\ x_1\colon \sigma_1' \cdot .. \cdot x_j\colon \sigma_j'\ \texttt{in}\ e'}\ \nearrow\text{-let-rec}$$

$\Rightarrow \texttt{let}\ x_1\colon \sigma_1' \cdot .. \cdot x_j\colon \sigma_j'\ \texttt{in}\ e' \sqsupseteq \texttt{let}\ x_1\colon \sigma_1 \cdot .. \cdot x_j\colon \sigma_j\ \texttt{in}\ e_1 \doteq e$

Case $\dfrac{e \doteq e_1\, e_2 \qquad e_1 \searrow_{s_1} s_1' \qquad e_2 \searrow_{s_2} s_2'}{e \searrow_{s_1\, s_2} s_1'\, s_2'}\ \searrow\text{-apply}$

$s_1' \nearrow e_1' \sqsupseteq e_1 \quad (\exists e_1')$ (IH)

$s_2' \nearrow e_2' \sqsupseteq e_2 \quad (\exists e_2')$ (IH)

$$\Rightarrow \quad \frac{s_1' \nearrow e_1' \qquad s_2' \nearrow e_2'}{s_1'\, s_2' \nearrow e_1'\, e_2'}\ \nearrow\text{-apply}$$

$\Rightarrow e_1'\, e_2' \sqsupseteq e_1\, e_2 \doteq e$

Case $\dfrac{e \doteq \lambda\{\texttt{true}\colon e_2, \texttt{false}\colon e_3\}\, e_1 \qquad e_1 \searrow_{s_1} s_1' \qquad e_2 \searrow_{s_2} s_2' \qquad e_3 \searrow_{s_3} s_3'}{e \searrow_{\texttt{if}\ s_1\ \texttt{then}\ s_2\ \texttt{else}\ s_3} \texttt{if}\ s_1'\ \texttt{then}\ s_2'\ \texttt{else}\ s_3'}\ \searrow\text{-if}$

$s_1' \nearrow e_1' \sqsupseteq e_1 \quad (\exists e_1')$ (IH)

$s_2' \nearrow e_2' \sqsupseteq e_2 \quad (\exists e_2')$ (IH)

$s_3' \nearrow e_3' \sqsupseteq e_3 \quad (\exists e_3')$ (IH)

$$\Rightarrow \quad \frac{s_1' \nearrow e_1' \qquad s_2' \nearrow e_2' \qquad s_3' \nearrow e_3'}{\texttt{if}\ s_1'\ \texttt{then}\ s_2'\ \texttt{else}\ s_3' \nearrow \lambda\{\texttt{true}\colon e_2', \texttt{false}\colon e_3'\}\, e_1'}\ \nearrow\text{-if}$$

$\Rightarrow \lambda\{\texttt{true}\colon e_2', \texttt{false}\colon e_3'\}\, e_1' \sqsupseteq \lambda\{\texttt{true}\colon e_2, \texttt{false}\colon e_3\}\, e_1 \doteq e$

Case $\dfrac{e \doteq (\lambda\sigma)\, e_1 \qquad \sigma \searrow_{\vec{c}} \vec{c}' \qquad e_1 \searrow_{s_1} s_1'}{e \searrow_{\texttt{match}\ s_1\ \texttt{as}\ \vec{c}} \texttt{match}\ s_1'\ \texttt{as}\ \vec{c}'}\ \searrow\text{-match}$

$s_1' \nearrow e_1' \sqsupseteq e_1 \quad (\exists e_1')$ (IH)

$\vec{c}' \nearrow \sigma' \sqsupseteq \sigma \quad (\exists \sigma')$ (Lemma C.6)

$$\Rightarrow \quad \frac{s_1' \nearrow e_1' \qquad \vec{c}' \nearrow \sigma'}{\texttt{match}\ s_1'\ \texttt{as}\ \vec{c}' \nearrow (\lambda\sigma)\, e_1'}\ \nearrow\text{-match}$$

$\Rightarrow (\lambda\sigma')\, e_1' \sqsupseteq (\lambda\sigma)\, e_1 \doteq e$

Case $\dfrac{e \doteq (\lambda\sigma)\, e_1 \qquad \sigma \searrow_{p=s_2} s_2' \qquad e_1 \searrow_{s_1} s_1'}{e \searrow_{\texttt{let } p=s_1 \texttt{ in } s_2} \texttt{let } p = s_1' \texttt{ in } s_2'}$ ↘-let

$s_1' \nearrow e_1' \sqsupseteq e_1 \quad (\exists e_1')$ (IH)

$p = s_2' \nearrow \sigma' \sqsupseteq \sigma \quad (\exists \sigma')$ (Lemma C.6)

➪ $\dfrac{s_1' \nearrow e_1' \qquad p = s_2' \nearrow \sigma'}{\texttt{let } p = s_1' \texttt{ in } s_2' \nearrow (\lambda\sigma')\, e_1'}$ ↗-let

➪ $(\lambda\sigma')\, e_1' \sqsupseteq (\lambda\sigma)\, e_1 \doteq e$

Case $\dfrac{e \doteq \texttt{enumFromTo}\, e_1\, e_2 \qquad e_1 \searrow_{s_1} s_1' \qquad e_2 \searrow_{s_2} s_2'}{e \searrow_{[\,s_1\,..\,s_2\,]} [\, s_1' \,..\, s_2' \,]}$ ↘-list-enum

$s_1' \nearrow e_1' \sqsupseteq e_1 \quad (\exists e_1')$ (IH)

$s_2' \nearrow e_2' \sqsupseteq e_2 \quad (\exists e_2')$ (IH)

➪ $\dfrac{s_1' \nearrow e_1' \qquad s_2' \nearrow e_2'}{[\, s_1' \,..\, s_2' \,] \nearrow \texttt{enumFromTo}\, e_1'\, e_2'}$ ↗-list-enum

➪ $\texttt{enumFromTo}\, e_1'\, e_2' \sqsupseteq \texttt{enumFromTo}\, e_1\, e_2 \doteq e$

Case $\dfrac{e \doteq e_1 :_{\alpha'} []_{\alpha} \qquad e_1 \searrow_{s_1} s_1'}{e \searrow_{[\,s_1 \mid \varepsilon\,]} [\, s_1' \mid \varepsilon\,]_{\alpha\sqcup\alpha'}}$ ↘-list-comp-done

$s_1' \nearrow e_1' \sqsupseteq e_1 \quad (\exists e_1')$ (IH)

➪ $\dfrac{s_1' \nearrow e_1'}{[\, s_1' \mid \varepsilon\,]_{\alpha\sqcup\alpha'} \nearrow e_1' :_{\alpha\sqcup\alpha'} []_{\alpha\sqcup\alpha'}}$ ↗-list-comp-done

➪ $e_1' :_{\alpha\sqcup\alpha'} []_{\alpha\sqcup\alpha'} \sqsupseteq e_1 :_{\alpha'} []_{\alpha} \doteq e$

Case $\dfrac{e \doteq \lambda\{\texttt{true}\colon e_1, \texttt{false}\colon []_{\alpha}\}\, e_2 \qquad e_2 \searrow_{s_2} s_2' \qquad e_1 \searrow_{[\,s_1 \mid \vec{q}\,]} [\, s_1' \mid \vec{q}' \,]_{\beta}}{e \searrow_{[\,s_1 \mid s_2 \cdot \vec{q}\,]} [\, s_1' \mid s_2' \cdot \vec{q}' \,]_{\alpha\sqcup\beta}}$ ↘-list-comp-guard

$[\, s_1' \mid \vec{q}' \,]_{\beta} \nearrow \sqsupseteq e_1$ (IH)

$[\, s_1' \mid \vec{q}' \,]_{\alpha\sqcup\beta} \nearrow e_1' \sqsupseteq e_1 \quad (\exists e_1')$ (monotonicity) (1)

$s_2' \nearrow e_2' \sqsupseteq e_2 \quad (\exists e_2')$ (IH) (2)

$\nearrow$-list-comp-guard

$$\dfrac{[\,s_1' \mid \vec{q}'\,]_{\alpha\sqcup\beta} \nearrow e_1' \qquad s_2' \nearrow e_2'}{[\,s_1' \mid s_2' \cdot \vec{q}'\,]_{\alpha\sqcup\beta} \nearrow \lambda\{\texttt{true}\colon e_1', \texttt{false}\colon []_{\alpha\sqcup\beta}\}\ e_2'} \qquad (1, 2)$$

$\Rightarrow \lambda\{\texttt{true}\colon e_1', \texttt{false}\colon []_{\alpha\sqcup\beta}\}\ e_2' \sqsupseteq \lambda\{\texttt{true}\colon e_1, \texttt{false}\colon []_{\alpha}\}\ e_2 \doteq e$

$\searrow$-list-comp-decl

Case $\dfrac{e \doteq (\lambda\sigma)\ e_1 \qquad \sigma \searrow_{p=[\,s_2 \mid \vec{q}\,]} p = [\,s_2' \mid \vec{q}'\,]_\alpha \qquad e_1 \searrow_{s_1} s_1'}{e \searrow_{[\,s_2 \mid \texttt{let}\ p = s_1 \cdot \vec{q}\,]} [\,s_2' \mid \texttt{let}\ p = s_1' \cdot \vec{q}'\,]_\alpha}$

$p = [\,s_2' \mid \vec{q}'\,]_\alpha \nearrow \sigma' \sqsupseteq \sigma \quad (\exists\sigma')$ (Lemma C.6)

$s_1' \nearrow e_1' \sqsupseteq e_1 \quad (\exists e_1')$ (IH)

$\nearrow$-list-comp-decl

$$\dfrac{p = [\,s_2' \mid \vec{q}'\,]_\alpha \nearrow \sigma' \qquad s_1' \nearrow e_1'}{[\,s_2' \mid \texttt{let}\ p = s_1' \cdot \vec{q}'\,]_\alpha \nearrow (\lambda\sigma')\ e_1'}$$

$\Rightarrow (\lambda\sigma')\ e_1' \sqsupseteq (\lambda\sigma)\ e_1 \doteq e$

$\searrow$-list-comp-gen

Case $\dfrac{e \doteq \texttt{concatMap}\ (\lambda\sigma_1)\ e_1 \qquad e_1 \searrow_{s_1} s_1' \qquad \sigma_1 \searrow_p \sigma_2, \beta \qquad \sigma_2 \searrow_{p=[\,s_2 \mid \vec{q}\,]} p = [\,s_2' \mid \vec{q}'\,]_{\beta'}}{e \searrow_{[\,s_2 \mid p \leftarrow s_1 \cdot \vec{q}\,]} [\,s_2' \mid p \leftarrow s_1' \cdot \vec{q}'\,]_{\beta\sqcup\beta'}}$

$p = [\,s_2' \mid \vec{q}'\,]_{\beta'} \nearrow \sigma_2^\dagger \quad (\exists\sigma_2^\dagger)$ (Lemma C.8)

$p = [\,s_2' \mid \vec{q}'\,]_{\beta\sqcup\beta'} \nearrow \sigma_2' \sqsupseteq \sigma_2^\dagger \quad (\exists\sigma_2')$ (monotonicity) (3)

$\sigma_2^\dagger, \beta \nearrow_p \sqsupseteq \sigma_1$ (Lemma C.8)

$\sigma_2', \beta \sqcup \beta' \nearrow_p \sigma_1' \sqsupseteq \sigma_1 \quad (\exists\sigma_1')$ (monotonicity) (4)

$s_1' \nearrow e_1' \sqsupseteq e_1 \quad (\exists e_1')$ (IH) (5)

$\nearrow$-list-comp-gen

$$\Rightarrow \dfrac{p = [\,s_2' \mid \vec{q}'\,]_{\beta\sqcup\beta'} \nearrow \sigma_2' \qquad \sigma_2', \beta \sqcup \beta' \nearrow_p \sigma_1' \qquad s_1' \nearrow e_1'}{[\,s_2' \mid p \leftarrow s_1' \cdot \vec{q}'\,]_{\beta\sqcup\beta'} \nearrow \texttt{concatMap}\ (\lambda\sigma_1')\ e_1'} \qquad (3, 4, 5)$$

$\Rightarrow \texttt{concatMap}\ (\lambda\sigma_1')\ e_1' \sqsupseteq \texttt{concatMap}\ (\lambda\sigma_1)\ e_1 \doteq e$

□

C.2.2 *Backwards after forwards direction.*

Proof. Induction on the $\nearrow$ derivation.

Case $\dfrac{s_1 \nearrow e_1 \qquad s_2 \nearrow e_2}{s_1 \oplus s_2 \nearrow (\oplus)\ e_1\ e_2}$ $\nearrow$-binary-apply

$e_1 \searrow_{s_1} s_1' \sqsubseteq s_1 \quad (\exists s_1')$ (IH)

$e_2 \searrow_{s_2} s_2' \sqsubseteq s_2 \quad (\exists s_2')$ (IH)

$\searrow$-binary-apply

$$\frac{e \doteq (\oplus)\ e_1\ e_2 \qquad e_1 \searrow_{s_1} s_1' \qquad e_2 \searrow_{s_2} s_2'}{e \searrow_{s_1 \oplus s_2} s_1' \oplus s_2'}$$

$\Rightarrow s_1' \oplus s_2' \sqsubseteq s_1 \oplus s_2$

Case

$\nearrow$-nil

$$\frac{}{[]_\alpha \nearrow []_\alpha}$$

$\searrow$-nil

$$\frac{e \doteq []_\alpha}{e \searrow_{[]} []_\alpha}$$

$\Rightarrow []_\alpha \sqsubseteq []_\alpha$

Case

$\nearrow$-non-empty-list

$$\frac{s \nearrow e_1 \qquad l \nearrow e_2}{[_\alpha\ s\ l \nearrow e_1 :_\alpha e_2}$$

$e_1 \searrow_s s' \sqsubseteq s \quad (\exists s')$ (IH)

$e_2 \searrow_l l' \sqsubseteq l \quad (\exists l')$ (IH)

$\searrow$-non-empty-list

$$\frac{e \doteq e_1 :_\alpha e_2 \qquad e_1 \searrow_s s' \qquad e_2 \searrow_l l'}{e \searrow_{[\ s\ l} [_\alpha\ s'\ l'}$$

$\Rightarrow [_\alpha\ s'\ l' \sqsubseteq [_\alpha\ s\ l$

Case

$\nearrow$-cons

$$\frac{s_1 \nearrow e_1 \qquad s_2 \nearrow e_2}{s_1 :_\alpha s_2 \nearrow e_1 :_\alpha e_2}$$

$e_1 \searrow_{s_1} s_1' \sqsubseteq s_1 \quad (\exists s_1')$ (IH)

$e_2 \searrow_{s_2} s_2' \sqsubseteq s_2 \quad (\exists s_2')$ (IH)

$\searrow$-cons

$$\frac{e \doteq e_1 :_\alpha e_2 \qquad e_1 \searrow_{s_1} s_1' \qquad e_2 \searrow_{s_2} s_2'}{e \searrow_{s_1\ :\ s_2} s_1' :_\alpha s_2'}$$

$\Rightarrow s_1' :_\alpha s_2' \sqsubseteq s_1 :_\alpha s_2$

Case

$\nearrow$-let-rec

$$\frac{\overrightarrow{c_i} \nearrow \sigma_i \quad (\forall i \le j) \qquad s \nearrow e_1}{\texttt{let}\ x_1 \colon \overrightarrow{c_1} \cdot \ldots \cdot x_j \colon \overrightarrow{c_j}\ \texttt{in}\ s \nearrow \texttt{let}\ x_1 \colon \sigma_1 \cdot \ldots \cdot x_j \colon \sigma_j\ \texttt{in}\ e_1}$$

$\sigma_i \searrow_{\overrightarrow{c_i}} \overrightarrow{c_i'} \sqsubseteq \overrightarrow{c_i} \quad (\exists \overrightarrow{c_i'}) \quad (\forall i \le j)$ (Lemma C.6)

$e_1 \searrow_s s' \sqsubseteq s \quad (\exists s')$ (IH)

$\searrow$-let-rec

$$\dfrac{e \doteq \texttt{let } x_1\colon \sigma_1 \cdot .. \cdot x_j\colon \sigma_j \texttt{ in } e_1 \qquad \sigma_i \searrow_{\overrightarrow{c_i}} \overrightarrow{c_i}' \quad (\forall i \le j) \qquad e_1 \searrow_s s'}{e \searrow_{\texttt{let } x_1\colon \overrightarrow{c}_1 \cdot .. \cdot x_j\colon \overrightarrow{c_j} \texttt{ in } s} \texttt{let } x_1\colon \overrightarrow{c_1}' \cdot .. \cdot x_j\colon \overrightarrow{c_j}' \texttt{ in } s'}$$

$\Rightarrow \texttt{let } x_1\colon \overrightarrow{c_1}' \cdot .. \cdot x_j\colon \overrightarrow{c_j}' \texttt{ in } s' \sqsubseteq \texttt{let } x_1\colon \overrightarrow{c_1} \cdot .. \cdot x_j\colon \overrightarrow{c_j} \texttt{ in } s$

Case $\dfrac{s_1 \nearrow e_1 \qquad s_2 \nearrow e_2}{s_1\, s_2 \nearrow e_1\, e_2}$ $\nearrow$-apply

$e_1 \searrow_{s_1} s_1' \sqsubseteq s_1 \quad (\exists s_1')$ (IH)

$e_2 \searrow_{s_2} s_2' \sqsubseteq s_2 \quad (\exists s_2')$ (IH)

$\Rightarrow \dfrac{e \doteq e_1\, e_2 \qquad e_1 \searrow_{s_1} s_1' \qquad e_2 \searrow_{s_2} s_2'}{e \searrow_{s_1\, s_2} s_1'\, s_2'}$ $\searrow$-apply

$\Rightarrow s_1'\, s_2' \sqsubseteq s_1\, s_2$

Case $\dfrac{s_1 \nearrow e_1 \qquad \overrightarrow{c} \nearrow \sigma}{\texttt{match } s_1 \texttt{ as } \overrightarrow{c} \nearrow (\lambda\sigma)\, e_1}$ $\nearrow$-match

$\sigma \searrow_{\overrightarrow{c}} \overrightarrow{c}' \sqsubseteq \overrightarrow{c} \quad (\exists \overrightarrow{c}')$ (Lemma C.6)

$e_1 \searrow_{s_1} s_1' \sqsubseteq s_1 \quad (\exists s_1')$ (IH)

$\Rightarrow \dfrac{e \doteq (\lambda\sigma)\, e_1 \qquad \sigma \searrow_{\overrightarrow{c}} \overrightarrow{c}' \qquad e_1 \searrow_{s_1} s_1'}{e \searrow_{\texttt{match } s_1 \texttt{ as } \overrightarrow{c}} \texttt{match } s_1' \texttt{ as } \overrightarrow{c}'}$ $\searrow$-match

$\Rightarrow \texttt{match } s_1' \texttt{ as } \overrightarrow{c}' \sqsubseteq \texttt{match } s_1 \texttt{ as } \overrightarrow{c}$

Case $\dfrac{s_1 \nearrow e_1 \qquad p = s_2 \nearrow \sigma}{\texttt{let } p = s_1 \texttt{ in } s_2 \nearrow (\lambda\sigma)\, e_1}$ $\nearrow$-let

$\sigma \searrow_{p=s_2} s_2' \sqsubseteq s_2 \quad (\exists s_2')$ (Lemma C.6)

$e_1 \searrow_{s_1} s_1' \sqsubseteq s_1 \quad (\exists s_1')$ (IH)

$\Rightarrow \dfrac{e \doteq (\lambda\sigma)\, e_1 \qquad \sigma \searrow_{p=s_2} s_2' \qquad e_1 \searrow_{s_1} s_1'}{e, \searrow_{\texttt{let } p=s_1 \texttt{ in } s_2} \texttt{let } p = s_1' \texttt{ in } s_2'}$ $\searrow$-let

$\Rightarrow \texttt{let } p = s_1' \texttt{ in } s_2' \sqsubseteq \texttt{let } p = s_1 \texttt{ in } s_2$

Case $\dfrac{s_1 \nearrow e_1 \qquad s_2 \nearrow e_2 \qquad s_3 \nearrow e_3}{\texttt{if } s_1 \texttt{ then } s_2 \texttt{ else } s_3 \nearrow \lambda\{\texttt{true: } e_2, \texttt{false: } e_3\}\, e_1}$ ↗-if

$e_1 \searrow_{s_1} s_1' \sqsubseteq s_1 \quad (\exists s_1')$ (IH)

$e_2 \searrow_{s_2} s_2' \sqsubseteq s_2 \quad (\exists s_2')$ (IH)

$e_3 \searrow_{s_3} s_3' \sqsubseteq s_3 \quad (\exists s_3')$ (IH)

➪ $\dfrac{e \doteq \lambda\{\texttt{true: } e_2, \texttt{false: } e_3\}\, e_1 \qquad e_1 \searrow_{s_1} s_1' \qquad e_2 \searrow_{s_2} s_2' \qquad e_3 \searrow_{s_3} s_3'}{e \searrow_{\texttt{if } s_1 \texttt{ then } s_2 \texttt{ else } s_3} \texttt{if } s_1' \texttt{ then } s_2' \texttt{ else } s_3'}$ ↘-if

➪ $\texttt{if } s_1' \texttt{ then } s_2' \texttt{ else } s_3' \sqsubseteq \texttt{if } s_1 \texttt{ then } s_2 \texttt{ else } s_3$

Case $\dfrac{s_1 \nearrow e_1 \qquad s_2 \nearrow e_2}{[\, s_1 \,..\, s_2 \,] \nearrow \texttt{enumFromTo}\, e_1\, e_2}$ ↗-list-enum

$e_1 \searrow_{s_1} s_1' \sqsubseteq s_1 \quad (\exists s_1')$ (IH)

$e_2 \searrow_{s_2} s_2' \sqsubseteq s_2 \quad (\exists s_2')$ (IH)

➪ $\dfrac{e \doteq \texttt{enumFromTo}\, e_1\, e_2 \qquad e_1 \searrow_{s_1} s_1' \qquad e_2 \searrow_{s_2} s_2'}{e \searrow_{[\, s_1 \,..\, s_2 \,]} [\, s_1' \,..\, s_2' \,]}$ ↘-list-enum

➪ $[\, s_1' \,..\, s_2' \,] \sqsubseteq [\, s_1 \,..\, s_2 \,]$

Case $\dfrac{s_1 \nearrow e_1}{[\, s_1 \mid \varepsilon \,]_\alpha \nearrow e_1 :_\alpha [\,]_\alpha}$ ↗-list-comp-done

$e_1 \searrow_{s_1} s_1' \sqsubseteq s_1 \quad (\exists s_1')$ (IH)

➪ $\dfrac{e \doteq e_1 :_\alpha [\,]_\alpha \qquad e_1 \searrow_{s_1} s_1'}{e \searrow_{[\, s_1 \mid \varepsilon \,]} [\, s_1' \mid \varepsilon \,]_{\alpha \sqcup \alpha}}$ ↘-list-comp-done

➪ $[\, s_1' \mid \varepsilon \,]_{\alpha \sqcup \alpha} \sqsubseteq [\, s_1 \mid \varepsilon \,]_\alpha$

Case $\dfrac{[\, s_1 \mid \vec{q} \,]_\alpha \nearrow e_1 \qquad s_2 \nearrow e_2}{[\, s_1 \mid s_2 \cdot \vec{q} \,]_\alpha \nearrow \lambda\{\texttt{true: } e_1, \texttt{false: } [\,]_\alpha\}\, e_2}$ ↗-list-comp-guard

$e_2 \searrow_{s_2} s_2' \sqsubseteq s_2 \quad (\exists s_2')$ (IH)

$e_1 \searrow_{[\, s_1 \mid \vec{q} \,]} [\, s_1' \mid \vec{q}' \,]_\beta \sqsubseteq [\, s_1 \mid \vec{q} \,]_\alpha \quad (\exists s_1', \vec{q}', \beta)$ (IH)

$\searrow$-list-comp-guard

$$\Rightarrow \quad \frac{e \doteq \lambda\{\texttt{true: } e_1, \texttt{false: } [\,]_\alpha\}\ e_2 \qquad e_2 \searrow_{s_2} s_2' \qquad e_1 \searrow_{[\,s_1 \mid \vec{q}\,]} [\,s_1' \mid \vec{q}'\,]_\beta}{e \searrow_{[\,s_1 \mid s_2 \cdot \vec{q}\,]} [\,s_1' \mid s_2' \cdot \vec{q}'\,]_{\alpha \sqcup \beta}}$$

$\Rightarrow [\,s_1' \mid s_2' \cdot \vec{q}'\,]_{\alpha\sqcup\beta} \sqsubseteq [\,s_1 \mid s_2 \cdot \vec{q}\,]_\alpha$

$\nearrow$-list-comp-decl

Case $$\frac{p = [\,s_2 \mid \vec{q}\,]_\alpha \nearrow \sigma \qquad s_1 \nearrow e_1}{[\,s_2 \mid \texttt{let } p = s_1 \cdot \vec{q}\,]_\alpha \nearrow (\lambda\sigma)\, e_1}$$

$\sigma, \searrow_{p=[\,s_2 \mid \vec{q}\,]} p = [\,s_2' \mid \vec{q}'\,]_\beta \sqsubseteq p = [\,s_2 \mid \vec{q}\,]_\alpha \quad (\exists s_2', \vec{q}', \beta)$ (Lemma C.4)

$e_1 \searrow_{s_1} s_1' \sqsubseteq s_1 \quad (\exists s_1')$ (IH)

$\searrow$-list-comp-decl

$$\Rightarrow \quad \frac{e \doteq (\lambda\sigma)\, e_1 \qquad \sigma \searrow_{p=[\,s_2 \mid \vec{q}\,]_\alpha} p = [\,s_2' \mid \vec{q}'\,]_\beta \qquad e_1, s_1 \searrow s_1'}{e \searrow_{[\,s_2 \mid \texttt{let } p = s_1 \cdot \vec{q}\,]} [\,s_2' \mid \texttt{let } p = s_1' \cdot \vec{q}'\,]_\beta}$$

$\Rightarrow [\,s_2' \mid \texttt{let } p = s_1' \cdot \vec{q}'\,]_\beta \sqsubseteq [\,s_2 \mid \texttt{let } p = s_1 \cdot \vec{q}\,]_\alpha$

$\nearrow$-list-comp-gen

Case $$\frac{p = [\,s_2 \mid \vec{q}\,]_\alpha \nearrow \sigma_1 \qquad \sigma_1, \alpha \nearrow\!\!\!\!\nearrow_p \sigma_2 \qquad s_1 \nearrow e_1}{[\,s_2 \mid p \leftarrow s_1 \cdot \vec{q}\,]_\alpha \nearrow \texttt{concatMap}\,(\lambda\sigma_2)\, e_1}$$

$e_1 \searrow_{s_1} s_1' \quad (\exists s_1')$ (IH)

$\sigma_2 \searrow\!\!\!\!\searrow_p \sigma_1', \beta$ with $\beta \sqsubseteq \alpha \quad (\exists \sigma_1', \beta)$ (Lemma C.8)

$\sigma_1' \searrow_{p=[\,s_2 \mid \vec{q}\,]} p = [\,s_2' \mid \vec{q}'\,]_{\beta'} \sqsubseteq p = [\,s_2 \mid \vec{q}\,]_\alpha \quad (\exists s_2', \vec{q}', \beta')$ (Lemma C.8)

$\searrow$-list-comp-gen

$$\Rightarrow \quad \frac{e \doteq \texttt{concatMap}\,(\lambda\sigma_2)\, e_1 \qquad e_1 \searrow_{s_1} s_1' \qquad \sigma_2 \searrow\!\!\!\!\searrow_p \sigma_1', \beta \qquad \sigma_1' \searrow_{p=[\,s_2 \mid \vec{q}\,]} [\,s_2' \mid \vec{q}'\,]_{\beta'}}{e \searrow_{[\,s_2 \mid p \leftarrow s_1 \cdot \vec{q}\,]} [\,s_2' \mid p \leftarrow s_1' \cdot \vec{q}'\,]_{\beta\sqcup\beta'}}$$

$\Rightarrow [\,s_2' \mid p \leftarrow s_1' \cdot \vec{q}'\,]_{\beta\sqcup\beta'} \sqsubseteq [\,s_2 \mid p \leftarrow s_1 \cdot \vec{q}\,]_\alpha$

□

C.3 Lemma C.2

Suppose $r \nearrow e$. Then $\nearrow_r (\searrow_r (e')) \sqsupseteq e'$.

Proof. 2

$\searrow$-list-rest-end

Case $$\frac{}{[\,]_\alpha \searrow_{]} \,]_\alpha}$$

$\nearrow$-list-rest-end

$$\Rightarrow \quad \frac{}{]_\alpha \nearrow [\,]_\alpha}$$

$\leftarrow [\,]_\alpha \sqsupseteq [\,]_\alpha$

Case $\dfrac{e_1 \searrow_t s \qquad e_2 \searrow_r r}{e_1 :_\alpha e_2 \searrow_{(,\ t\ r)} (,_\alpha\ s\ r)}$ ↘-list-rest-cons

$s \nearrow e_1' \sqsupseteq e_1 \quad (\exists e_1')$ (IH)

$r \nearrow e_2' \sqsupseteq e_2 \quad (\exists e_2')$ (IH)

$\leftarrow \dfrac{s \nearrow e_1' \qquad r \nearrow e_2'}{(,_\alpha\ s\ r) \nearrow e_1' :_\alpha e_2'}$ ↗-list-rest-cons

$\leftarrow e_1' :_\alpha e_2' \sqsupseteq e_1 :_\alpha e_2$

□

Suppose $r \nearrow e$. Then $\searrow_r (\nearrow_r (r')) \sqsubseteq r'$.

Proof. 3

Case $\dfrac{}{]_\alpha \nearrow [\,]_\alpha}$ ↗-list-rest-end

$\leftarrow \dfrac{}{[\,]_\alpha \searrow_]]_\alpha}$ ↘-list-rest-end

$\leftarrow]_\alpha \sqsubseteq]_\alpha$

Case $\dfrac{s \nearrow e_1 \qquad r \nearrow e_2}{(,_\alpha\ s\ r) \nearrow e_1 :_\alpha e_2}$ ↗-list-rest-cons

$e_1 \searrow_t s' \sqsubseteq s \quad (\exists s')$ (IH)

$e_2 \searrow_r r' \sqsubseteq r \quad (\exists r')$ (IH)

$\leftarrow \dfrac{e_1 \searrow_t s' \qquad e_2 \searrow_r r'}{e_1 :_\alpha e_2 \searrow_{(,\ t\ r)} (,_\alpha\ s'\ r')}$ ↘-list-rest-cons

$\leftarrow (,_\alpha\ s'\ r') \sqsubseteq (,_\alpha\ s\ r)$

□

C.4 Lemma C.4, part (i)

Suppose $\sigma \searrow_{\vec{p}} e$. We show $\vec{p}, e \nearrow \sigma' \sqsupseteq \sigma$.

Proof.

Case $\dfrac{}{x\colon \kappa \searrow_x \kappa}\ \searrow\text{-var}$

➪ $\dfrac{}{x, \kappa \nearrow x\colon \kappa}\ \nearrow\text{-var}$

➪ $x\colon \kappa \sqsupseteq x\colon \kappa$

Case $\dfrac{}{\{[]\colon \kappa\} \searrow_{[]} \kappa}\ \searrow\text{-nil}$

➪ $\dfrac{}{[], \kappa \nearrow \{[]\colon \kappa\}}\ \nearrow\text{-nil}$

➪ $\{[]\colon \kappa\} \sqsupseteq \{[]\colon \kappa\}$

Case $\dfrac{\sigma \searrow_p \tau \qquad \tau \searrow_{p'} \kappa}{\{(\mathbf{:})\colon \sigma\} \searrow_{p\,\mathbf{:}\,p'} \kappa}\ \searrow\text{-cons}$

$p', \kappa \nearrow \tau' \sqsupseteq \tau \quad (\exists \tau')$ (IH)

$p, \tau \nearrow \sqsupseteq \sigma$ (IH)

$p, \tau' \nearrow \sigma' \sqsupseteq \sigma \quad (\exists \sigma')$ (Monotonicity)

➪ $\dfrac{p', \kappa \nearrow \tau' \qquad p, \tau' \nearrow \sigma'}{p\,\mathbf{:}\,p', \kappa \nearrow \{(\mathbf{:})\colon \sigma'\}}\ \nearrow\text{-cons}$

$\{(\mathbf{:})\colon \sigma'\} \sqsupseteq \{(\mathbf{:})\colon \sigma\}$

Case $\dfrac{\sigma \searrow_p \tau \qquad \tau \searrow_o \kappa}{\{(\mathbf{:})\colon \sigma\} \searrow_{[\ p\ o} \kappa}\ \searrow\text{-non-empty-list}$

$o, \kappa \nearrow \tau' \sqsupseteq \tau \quad (\exists \tau')$ (IH)

$p, \tau \nearrow \sqsupseteq \sigma$ (IH)

$p, \tau' \nearrow \sigma' \sqsupseteq \sigma \quad (\exists \sigma')$ (Monotonicity)

➪ $\dfrac{o, \kappa \nearrow \tau' \qquad p, \tau' \nearrow \sigma'}{[\ p\ o, \kappa \nearrow \{(\mathbf{:})\colon \sigma'\}}\ \nearrow\text{-non-empty-list}$

➪ $\{(\mathbf{:})\colon \sigma'\} \sqsupseteq \{(\mathbf{:})\colon \sigma\}$

Case $\dfrac{\sigma \searrow_{p} \tau \qquad \tau \searrow_{p'} \kappa}{\{(,): \sigma\} \searrow_{(p,p')} \kappa}$ ↘-pair

$p', \kappa \nearrow \tau' \sqsupseteq \tau \quad (\exists \tau')$ (IH)

$p, \tau \nearrow \sqsupseteq \sigma$ (IH)

$p, \tau' \nearrow \sigma' \sqsupseteq \sigma \quad (\exists \sigma')$ (Monotonicity)

➪ $\dfrac{p', \kappa \nearrow \tau' \qquad p, \tau' \nearrow \sigma'}{(p, p'), \kappa \nearrow \{(,): \sigma'\}}$ ↗-pair

➪ $\{(,): \sigma'\} \sqsupseteq \{(,): \sigma\}$

Case $\dfrac{\sigma \searrow_{p} \doteq \lambda\tau \qquad \tau \searrow_{\vec{p}} e}{\sigma \searrow_{p \cdot \vec{p}} e}\ \vec{p} \neq \varepsilon$ ↘-seq

$\vec{p}, e \nearrow \tau' \sqsupseteq \tau \quad (\exists \tau')$ (IH)

$p, \lambda\tau \nearrow \sqsupseteq \sigma$ (IH)

$p, \lambda\tau' \nearrow \sigma' \sqsupseteq \sigma \quad (\exists \sigma')$ (Monotonicity)

➪ $\dfrac{\vec{p}, e \nearrow \tau' \qquad p, \lambda\tau' \nearrow \sigma'}{p \cdot \vec{p}, e \nearrow \sigma'}\ \vec{p} \neq \varepsilon$ ↗-seq

➪ $\sigma' \sqsupseteq \sigma$

Case $\dfrac{}{\{[]: \kappa\} \searrow_{]} \kappa}$ ↘-list-rest-end

➪ $\dfrac{}{], \kappa \nearrow \{[]: \kappa\}}$ ↗-list-rest-end

➪ $\{[]: \kappa\} \sqsupseteq \{[]: \kappa\}$

Case $\dfrac{\sigma \searrow_{p} \tau \qquad \tau \searrow_{o} \kappa}{\{(:): \sigma\} \searrow_{(,\ p\ o)} \kappa}$ ↘-list-rest-cons

$o, \kappa \nearrow \tau' \sqsupseteq \tau \quad (\exists \tau')$ (IH)

$p, \tau \nearrow \sqsupseteq \sigma$ (IH)

$p, \tau' \nearrow \sigma' \sqsupseteq \sigma \quad (\exists \sigma')$ (Monotonicity)

$$\dfrac{o, \kappa \nearrow \tau' \qquad p, \tau' \nearrow \sigma'}{(\texttt{,}\ p\ o), \kappa \nearrow \{(\texttt{:}) \colon \sigma'\}}\ \nearrow\text{-list-rest-cons}$$

➪ $\{(\texttt{:}) \colon \sigma'\} \sqsupseteq \{(\texttt{:}) \colon \sigma\}$

□

Suppose $\vec{p}, e \nearrow \sigma$. We show $\sigma \searrow_{\vec{p}} e' \sqsubseteq e$.

Proof.

Case $\dfrac{}{x, \kappa \nearrow x \colon \kappa}\ \nearrow\text{-var}$

➪ $\dfrac{}{x \colon \kappa \searrow_x \kappa}\ \searrow\text{-var}$

➪ $(x, \kappa) \sqsubseteq (x, \kappa)$

Case $\dfrac{}{[\,], \kappa \nearrow \{[\,] \colon \kappa\}}\ \nearrow\text{-nil}$

➪ $\dfrac{}{\{[\,] \colon \kappa\} \searrow_{[\,]} \kappa}\ \searrow\text{-nil}$

$([\,], \kappa) \sqsubseteq ([\,], \kappa)$

Case $\dfrac{p', \kappa \nearrow \tau \qquad p, \tau \nearrow \sigma}{p \texttt{ : } p', \kappa \nearrow \{(\texttt{:}) \colon \sigma\}}\ \nearrow\text{-cons}$

$\sigma \searrow_p \tau' \sqsubseteq \tau \quad (\exists \tau')$ (IH)

$\tau \searrow_{p'} \sqsubseteq \kappa$ (IH)

$\tau' \searrow_{p'} \kappa' \sqsubseteq \kappa \quad (\exists \kappa')$ (Monotonicity)

➪ $\dfrac{\sigma \searrow_p \tau' \qquad \tau' \searrow_{p'} \kappa'}{\{(\texttt{:}) \colon \sigma\} \searrow_{p \texttt{ : } p'} \kappa'}\ \searrow\text{-cons}$

➪ $(p \texttt{ : } p', \kappa') \sqsubseteq (p \texttt{ : } p', \kappa)$

Case $\dfrac{o, \kappa \nearrow \tau \qquad p, \tau \nearrow \sigma}{[\ p\ o, \kappa \nearrow \{(\texttt{:}) \colon \sigma\}}\ \nearrow\text{-non-empty-list}$

$\sigma \searrow_p \tau' \sqsubseteq \tau \quad (\exists \tau')$ (IH)

$\tau \searrow_o \sqsubseteq \kappa$ (IH)

$\tau' \searrow_o \kappa' \sqsubseteq \kappa \quad (\exists \kappa')$ (Monotonicity)

$$\text{➪} \qquad \frac{\sigma \searrow_p \tau' \qquad \tau' \searrow_o \kappa'}{\{(\mathtt{:})\colon \sigma\} \searrow_{[\ p\ o} \kappa'} \ \searrow\text{-non-empty-list}$$

➪ $([\ p\ o, \kappa') \sqsubseteq ([\ p\ o, \kappa)$

Case $$\frac{p', \kappa \nearrow \tau \qquad p, \tau \nearrow \sigma}{(p \mathtt{,} p'), \kappa \nearrow \{(\mathtt{,})\colon \sigma\}} \ \nearrow\text{-pair}$$

$\sigma \searrow_p \tau' \sqsubseteq \tau \quad (\exists \tau')$ (IH)

$\tau \searrow_{p'} \sqsubseteq \kappa$ (IH)

$\tau' \searrow_{p'} \kappa' \sqsubseteq \kappa \quad (\exists \kappa')$ (Monotonicity)

$$\text{➪} \qquad \frac{\sigma \searrow_p \tau' \qquad \tau' \searrow_{p'} \kappa'}{\{(\mathtt{,})\colon \sigma\} \searrow_{(p \mathtt{,} p')} \kappa'} \ \searrow\text{-pair}$$

➪ $((p \mathtt{,} p'), \kappa') \sqsubseteq ((p \mathtt{,} p'), \kappa)$

Case $$\frac{\vec{p}, e \nearrow \tau \qquad p, \lambda\tau \nearrow \sigma}{p \cdot \vec{p}, e \nearrow \sigma} \ \vec{p} \neq \varepsilon \ \nearrow\text{-seq}$$

$\sigma \searrow_p \doteq \lambda\tau' \sqsubseteq \lambda\tau \quad (\exists \tau')$ (IH)

$\tau \searrow_{\vec{p}} \sqsubseteq e$ (IH)

$\tau' \searrow_{\vec{p}} e' \sqsubseteq e \quad (\exists e')$ (Monotonicity)

$$\text{➪} \qquad \frac{\sigma \searrow_p \doteq \lambda\tau' \qquad \tau' \searrow_{\vec{p}} e'}{\sigma \searrow_{p \cdot \vec{p}} e'} \ \vec{p} \neq \varepsilon \ \searrow\text{-seq}$$

➪ $(p \cdot \vec{p}, e') \sqsubseteq (p \cdot \vec{p}, e)$

Case $$\frac{}{], \kappa \nearrow \{[]\colon \kappa\}} \ \nearrow\text{-list-rest-end}$$

$$\text{➪} \qquad \frac{}{\{[]\colon \kappa\} \searrow_{]} \kappa} \ \searrow\text{-list-rest-end}$$

➪ $(], \kappa) \sqsubseteq (], \kappa)$

Case $\dfrac{o, \kappa \nearrow \tau \qquad p, \tau \nearrow \sigma}{(,\ p\ o), \kappa \nearrow \{(:)\colon \sigma\}}$ $\nearrow$-list-rest-cons

$\sigma \searrow_p \tau' \sqsubseteq \tau \quad (\exists \tau')$ (IH)

$\tau \searrow_o \sqsubseteq \kappa$ (IH)

$\tau' \searrow_o \kappa' \sqsubseteq \kappa \quad (\exists \kappa')$ (Monotonicity)

$\dfrac{\sigma \searrow_p \tau' \qquad \tau' \searrow_o \kappa'}{\{(:)\colon \sigma\} \searrow_{(,\ p\ o)} \kappa'}$ $\searrow$-list-rest-cons

$\Rightarrow (,\ p\ o, \kappa') \sqsubseteq (,\ p\ o, \kappa)$

□

C.5 Lemma C.6

Suppose $\sigma \searrow_{\vec{c}} \vec{c}'$. We show $\vec{c}' \nearrow \sqsupseteq \sigma$.

Proof.

Case $\dfrac{\sigma \searrow_{\vec{p}} e \qquad e \searrow_s s'}{\sigma \searrow_{\vec{p}=s} \vec{p} = s'}$ $\searrow$-clause

$s' \nearrow e' \sqsupseteq e \quad (\exists e')$ Theorem 5.1 (1)

$\vec{p}, e \nearrow \sqsupseteq \sigma$ Lemma C.4

$\vec{p}, e' \nearrow \sigma' \sqsupseteq \sigma \quad (\exists \sigma')$ monotonicity (2)

$\dfrac{s' \nearrow e' \qquad \vec{p}, e' \nearrow \sigma'}{\vec{p} = s' \nearrow \sigma'}$ $\nearrow$-clause (1, 2)

$\Rightarrow \sigma' \sqsupseteq \sigma$

Case $\dfrac{\sigma \doteq \sigma' \uplus \tau \qquad \sigma' \searrow_c c' \qquad \tau \searrow_{\vec{c}} \vec{c}'}{\sigma \searrow_{c \cdot \vec{c}} c' \cdot \vec{c}'}\ \vec{c} \neq \varepsilon$ $\searrow$-clause-seq

$c' \nearrow \sigma^\dagger \sqsupseteq \sigma' \quad (\exists \sigma^\dagger)$ IH (3)

$\vec{c}' \nearrow \tau' \sqsupseteq \tau \quad (\exists \tau')$ IH (4)

$\sigma^\dagger \uplus \tau' = \sigma^\ddagger \quad (\exists \sigma^\ddagger)$ $\sigma' \uplus \tau$ defined; (3, 4)

$\Rightarrow$ $\dfrac{c' \nearrow \sigma^\dagger \qquad \vec{c}' \nearrow \tau' \qquad \sigma^\dagger \uplus \tau' = \sigma^\ddagger}{c' \cdot \vec{c}' \nearrow \sigma^\ddagger}\ \vec{c}' \neq \varepsilon$ $\nearrow$-clause-seq (3, 4)

$\Rightarrow \sigma^\ddagger \sqsupseteq \sigma$ monotonicity of $\uplus$

□

Suppose $\overrightarrow{c} \nearrow \sigma$. We show $\sigma \searrow_{\overrightarrow{c}} \sqsubseteq \overrightarrow{c}$.

Proof.

Case $\dfrac{s \nearrow e \qquad \overrightarrow{p}, e \nearrow \sigma}{\overrightarrow{p} = s \nearrow \sigma}$ (↗-clause)

$\sigma \searrow_{\overrightarrow{p}} e' \sqsubseteq e \quad (\exists e')$ Lemma C.4 (5)

$e \searrow_s \sqsubseteq s$ Theorem 5.1

$e' \searrow_s s' \sqsubseteq s$ monotonicity (6)

➪ $\dfrac{\sigma \searrow_{\overrightarrow{p}} e' \qquad e' \searrow_s s'}{\sigma \searrow_{\overrightarrow{p}=s} \overrightarrow{p} = s'}$ (↘-clause) (5, 6)

➪ $s' \sqsubseteq s$

Case $\dfrac{c \nearrow \sigma \qquad \overrightarrow{c} \nearrow \sigma' \qquad \sigma \uplus \sigma' = \tau}{c \cdot \overrightarrow{c} \nearrow \tau}\ \overrightarrow{c} \neq \varepsilon$ (↗-clause-seq)

$\sigma \searrow_c c' \sqsubseteq c \quad (\exists c')$ IH (7)

$\sigma' \searrow_{\overrightarrow{c}} \overrightarrow{c}' \sqsubseteq \overrightarrow{c} \quad (\exists \overrightarrow{c}')$ IH (8)

➪ $\dfrac{\tau \doteq \sigma' \uplus \sigma \qquad \sigma \searrow_c c' \qquad \sigma' \searrow_{\overrightarrow{c}} \overrightarrow{c}'}{\tau \searrow_{c \cdot \overrightarrow{c}} c' \cdot \overrightarrow{c}'}\ \overrightarrow{c} \neq \varepsilon$ (↘-clause-seq) (7, 8)

➪ $c' \cdot \overrightarrow{c}' \sqsubseteq c \cdot \overrightarrow{c}$

□

C.6 Lemma C.8

Suppose $\kappa, \alpha \nearrow_{\overrightarrow{\pi}} \kappa'$. Then $\mathsf{totalise{-}fwd}_{\kappa,\alpha,\overrightarrow{\pi}}(\mathsf{totalise{-}bwd}_{\kappa,\alpha,\overrightarrow{\pi}}(\kappa^\dagger)) \sqsupseteq \kappa^\dagger$.

Proof. 2

Case $\dfrac{\kappa_1 \searrow_{\overrightarrow{\pi}} \kappa_2, \alpha}{x\colon \kappa_1 \searrow_{x \cdot \overrightarrow{\pi}} x\colon \kappa_2, \alpha}$ (↘-var)

$\kappa_2, \alpha \nearrow_{\overrightarrow{\pi}} \kappa_1' \sqsupseteq \kappa_1 \quad (\exists \kappa_1')$ (IH)

➪ $\dfrac{\kappa_2, \alpha \nearrow_{\overrightarrow{\pi}} \kappa_1'}{x\colon \kappa_2, \alpha \nearrow_{x \cdot \overrightarrow{\pi}} x\colon \kappa_1'}$ (↗-elim-var)

➪ $x\colon \kappa_1' \sqsupseteq x\colon \kappa_1$

Case $\dfrac{\kappa_1 \searrow_{\vec{\pi}} \kappa_2, \beta}{\{\texttt{true}\colon \kappa_1, \texttt{false}\colon []_\alpha\} \searrow_{\texttt{true}\cdot\vec{\pi}} \{\texttt{true}\colon \kappa_2\}, \alpha \sqcup \beta}$ ($\searrow$-true)

$\kappa_2, \beta \nearrow_{\vec{\pi}} \sqsupseteq \kappa_1$ (IH)

$\kappa_2, \alpha \sqcup \beta \nearrow_{\vec{\pi}} \kappa_1' \sqsupseteq \kappa_1 \quad (\exists \kappa_1')$ (Monotonicity)

➪ $\dfrac{\kappa_2, \alpha \sqcup \beta \nearrow_{\vec{\pi}} \kappa_1'}{\{\texttt{true}\colon \kappa_2\}, \alpha \sqcup \beta \nearrow_{\texttt{true}\cdot\vec{\pi}} \{\texttt{true}\colon \kappa_1', \texttt{false}\colon []_{\alpha\sqcup\beta}\}}$ ($\nearrow$-elim-true)

➪ $\{\texttt{true}\colon \kappa_1', \texttt{false}\colon []_{\alpha\sqcup\beta}\} \sqsupseteq \{\texttt{true}\colon \kappa_1, \texttt{false}\colon []_\alpha\}$

Case $\dfrac{\kappa_1 \searrow_{\vec{\pi}} \kappa_2, \beta}{\{\texttt{true}\colon []_\alpha, \texttt{false}\colon \kappa_1\} \searrow_{\texttt{false}\cdot\vec{\pi}} \{\texttt{false}\colon \kappa_2\}, \alpha \sqcup \beta}$ ($\searrow$-false)

$\kappa_2, \beta \nearrow_{\vec{\pi}} \sqsupseteq \kappa_1$ (IH)

$\kappa_2, \alpha \sqcup \beta \nearrow_{\vec{\pi}} \kappa_1' \sqsupseteq \kappa_1 \quad (\exists \kappa_1')$ (Monotonicity)

➪ $\dfrac{\kappa_2, \alpha \sqcup \beta \nearrow_{\vec{\pi}} \kappa_1'}{\{\texttt{false}\colon \kappa_2\}, \alpha \sqcup \beta \nearrow_{\texttt{false}\cdot\vec{\pi}} \{\texttt{true}\colon []_{\alpha\sqcup\beta}, \texttt{false}\colon \kappa_1'\}}$ ($\nearrow$-elim-false)

➪ $\{\texttt{true}\colon []_{\alpha\sqcup\beta}, \texttt{false}\colon \kappa_1'\} \sqsupseteq \{\texttt{true}\colon []_\alpha, \texttt{false}\colon \kappa_1\}$

Case $\dfrac{\sigma_1 \searrow_{p\cdot p'\cdot\vec{\pi}} \sigma_2, \alpha}{\{(\texttt{,})\colon \sigma_1\} \searrow_{(p,p')\cdot\vec{\pi}} \{(\texttt{,})\colon \sigma_2\}, \alpha}$ ($\searrow$-prod)

$\sigma_2, \alpha \nearrow_{p\cdot p'\cdot\vec{\pi}} \sigma_1' \sqsupseteq \sigma_1 \quad (\exists \sigma_1')$ (IH)

➪ $\dfrac{\sigma_2, \alpha \nearrow_{p\cdot p'\cdot\vec{\pi}} \sigma_1'}{\{(\texttt{,})\colon \sigma_2\}, \alpha \nearrow_{(p,p')\cdot\vec{\pi}} \{(\texttt{,})\colon \sigma_1'\}}$ ($\nearrow$-elim-prod)

➪ $\{(\texttt{,})\colon \sigma_1'\} \sqsupseteq \{(\texttt{,})\colon \sigma_1\}$

Case $\dfrac{\kappa_1 \searrow_{\vec{\pi}} \kappa_2, \beta}{\{[]\colon \kappa_1, (\texttt{:})\colon x\colon y\colon []_\alpha\} \searrow_{[]\cdot\vec{\pi}} \{[]\colon \kappa_2\}, \alpha \sqcup \beta}$ ($\searrow$-nil)

$\kappa_2, \beta \nearrow_{\vec{\pi}} \sqsupseteq \kappa_1$ (IH)

$\kappa_2, \alpha \sqcup \beta \nearrow_{\vec{\pi}} \kappa_1' \sqsupseteq \kappa_1 \quad (\exists \kappa_1')$ (Monotonicity)

➪ $\dfrac{\kappa_2, \alpha \sqcup \beta \nearrow_{\vec{\pi}} \kappa_1'}{\{[]\colon \kappa_2\}, \alpha \sqcup \beta \nearrow_{[]\cdot\vec{\pi}} \{[]\colon \kappa_1', (\texttt{:})\colon x\colon y\colon []_{\alpha\sqcup\beta}\}}$ ($\nearrow$-elim-nil)

➪ $\{[]\colon \kappa_1', (\texttt{:})\colon x\colon y\colon []_{\alpha\sqcup\beta}\} \sqsupseteq \{[]\colon \kappa_1, (\texttt{:})\colon x\colon y\colon []_\alpha\} \doteq$

Case $\searrow$-cons

$$\frac{\sigma_1 \searrow_{p\cdot p'\cdot \overrightarrow{\pi}} \sigma_2, \beta}{\{[]\colon []_\alpha, (:)\colon \sigma_1\} \searrow_{(p\,:\,p')\cdot\overrightarrow{\pi}} \{(:)\colon \sigma_2\}, \alpha \sqcup \beta}$$

$\sigma_2, \beta \nearrow_{p\cdot p'\cdot\overrightarrow{\pi}} \sqsupseteq \sigma_1$ (IH)

$\sigma_2, \alpha \sqcup \beta \nearrow_{p\cdot p'\cdot\overrightarrow{\pi}} \sigma_1' \sqsupseteq \sigma_1 \quad (\exists \sigma_1')$ (Monotonicity)

$\nearrow$-elim-cons

$$\Rightarrow \quad \frac{\sigma_2, \alpha \sqcup \beta \nearrow_{p\cdot p'\cdot\overrightarrow{\pi}} \sigma_1'}{\{(:)\colon \sigma_2\}, \alpha \sqcup \beta \nearrow_{(p\,:\,p')\cdot\overrightarrow{\pi}} \{[]\colon []_{\alpha\sqcup\beta}, (:)\colon \sigma_1'\}}$$

$\Rightarrow \{[]\colon []_{\alpha\sqcup\beta}, (:)\colon \sigma_1'\} \sqsupseteq \{[]\colon []_\alpha, (:)\colon \sigma_1\}$

Case $\searrow$-non-empty-list

$$\frac{\sigma_1 \searrow_{p\cdot o\cdot \overrightarrow{\pi}} \sigma_2, \beta}{\{[]\colon []_\alpha, (:)\colon \sigma_1\} \searrow_{([\ p\ o)\cdot\overrightarrow{\pi}} \{(:)\colon \sigma_2\}, \alpha \sqcup \beta}$$

$\sigma_2, \beta \nearrow_{p\cdot o\cdot\overrightarrow{\pi}} \sqsupseteq \sigma_1$ (IH)

$\sigma_2, \alpha \sqcup \beta \nearrow_{p\cdot o\cdot\overrightarrow{\pi}} \sigma_1' \sqsupseteq \sigma_1 \quad (\exists \sigma_1')$ (Monotonicity)

$\nearrow$-elim-non-empty-list

$$\Rightarrow \quad \frac{\sigma_2, \alpha \sqcup \beta \nearrow_{p\cdot o\cdot\overrightarrow{\pi}} \sigma_1'}{\{(:)\colon \sigma_2\}, \alpha \sqcup \beta \nearrow_{([\ p\ o)\cdot\overrightarrow{\pi}} \{[]\colon []_{\alpha\sqcup\beta}, (:)\colon \sigma_1'\}}$$

$\Rightarrow \{[]\colon []_{\alpha\sqcup\beta}, (:)\colon \sigma_1'\} \sqsupseteq \{[]\colon []_\alpha, (:)\colon \sigma_1\}$

Case $\searrow$-list-rest-end

$$\frac{\kappa_1 \searrow_{\overrightarrow{\pi}} \kappa_2, \beta}{\{[]\colon \kappa_1, (:)\colon x\colon y\colon []_\alpha\} \searrow_{]\cdot\overrightarrow{\pi}} \{[]\colon \kappa_2\}, \alpha \sqcup \beta}$$

$\kappa_2, \beta \nearrow_{\overrightarrow{\pi}} \sqsupseteq \kappa_1$ (IH)

$\kappa_2, \alpha \sqcup \beta \nearrow_{\overrightarrow{\pi}} \kappa_1' \sqsupseteq \kappa_1 \quad (\exists \kappa_1')$ (Monotonicity)

$\nearrow$-elim-list-rest-end

$$\Rightarrow \quad \frac{\kappa_2, \alpha \sqcup \beta \nearrow_{\overrightarrow{\pi}} \kappa_1'}{\{[]\colon \kappa_2\}, \alpha \sqcup \beta \nearrow_{]\cdot\overrightarrow{\pi}} \{[]\colon \kappa_1', (:)\colon x\colon y\colon []_{\alpha\sqcup\beta}\}}$$

$\Rightarrow \{[]\colon \kappa_1', (:)\colon x\colon y\colon []_{\alpha\sqcup\beta}\} \sqsupseteq \{[]\colon \kappa_1, (:)\colon x\colon y\colon []_\alpha\}$

Case $\searrow$-list-rest-cons

$$\frac{\sigma_1 \searrow_{p\cdot o\cdot \overrightarrow{\pi}} \sigma_2, \beta}{\{[]\colon []_\alpha, (:)\colon \sigma_1\} \searrow_{(,\ p\ o)\cdot\overrightarrow{\pi}} \{(:)\colon \sigma_2\}, \alpha \sqcup \beta}$$

$\sigma_2, \beta \nearrow_{p\cdot o\cdot\overrightarrow{\pi}} \sqsupseteq \sigma_1$ (IH)

$\sigma_2, \alpha \sqcup \beta \nearrow_{p\cdot o\cdot\overrightarrow{\pi}} \sigma_1' \sqsupseteq \sigma_1 \quad (\exists \sigma_1')$ (Monotonicity)

$\nearrow$-elim-list-rest-cons

$$\Rightarrow \quad \frac{\sigma_2, \alpha \sqcup \beta \nearrow_{p\cdot o\cdot\overrightarrow{\pi}} \sigma_1'}{\{(:)\colon \sigma_2\}, \alpha \sqcup \beta \nearrow_{(,\ p\ o)\cdot\overrightarrow{\pi}} \{[]\colon []_{\alpha\sqcup\beta}, (:)\colon \sigma_1'\}}$$

$\Rightarrow \{\texttt{[]}\colon \texttt{[]}_{\alpha \sqcup \beta}, (\texttt{:})\colon \sigma_1'\} \sqsupseteq \{\texttt{[]}\colon \texttt{[]}_{\alpha}, (\texttt{:})\colon \sigma_1\}$

□

Suppose $\kappa, \alpha \nearrow_{\vec{\pi}} \kappa'$. Then $\text{totalise–bwd}_{\kappa,\alpha,\vec{\pi}}(\text{totalise–fwd}_{\kappa,\alpha,\vec{\pi}}(\kappa^\dagger, \alpha')) \sqsubseteq (\kappa^\dagger, \alpha')$.

Proof. 3

Case $\dfrac{\kappa_1, \alpha \nearrow_{\vec{\pi}} \kappa_2}{x\colon \kappa_1, \alpha \nearrow_{x\cdot\vec{\pi}} x\colon \kappa_2}$ ($\nearrow$-elim-var)

$\kappa_2 \searrow_{\vec{\pi}} \kappa_1', \beta \sqsubseteq \kappa_1, \alpha \quad (\exists \kappa_1', \beta)$ (IH)

$\Rightarrow \dfrac{\kappa_2 \searrow_{\vec{\pi}} \kappa_1', \beta}{x\colon \kappa_2 \searrow_{x\cdot\vec{\pi}} x\colon \kappa_1', \beta}$ ($\searrow$-var)

$\Rightarrow (x\colon \kappa_1', \beta) \sqsubseteq (x\colon \kappa_1, \alpha)$

Case $\dfrac{\kappa_1, \alpha \nearrow_{\vec{\pi}} \kappa_2}{\{\texttt{true}\colon \kappa_1\}, \alpha \nearrow_{\texttt{true}\cdot\vec{\pi}} \{\texttt{true}\colon \kappa_2, \texttt{false}\colon \texttt{[]}_\alpha\}}$ ($\nearrow$-elim-true)

$\kappa_2 \searrow_{\vec{\pi}} \kappa_1', \beta \sqsubseteq \kappa_1, \alpha \quad (\exists \kappa_1', \beta)$ (IH)

$\Rightarrow \dfrac{\kappa_2 \searrow_{\vec{\pi}} \kappa_1', \beta}{\{\texttt{true}\colon \kappa_2, \texttt{false}\colon \texttt{[]}_\alpha\} \searrow_{\texttt{true}\cdot\vec{\pi}} \{\texttt{true}\colon \kappa_1'\}, \alpha \sqcup \beta}$ ($\searrow$-true)

$\Rightarrow (\{\texttt{true}\colon \kappa_1'\}, \alpha \sqcup \beta) \sqsubseteq (\{\texttt{true}\colon \kappa_1\}, \alpha)$

Case $\dfrac{\kappa_1, \alpha \nearrow_{\vec{\pi}} \kappa_2}{\{\texttt{false}\colon \kappa_1\}, \alpha \nearrow_{\texttt{false}\cdot\vec{\pi}} \{\texttt{true}\colon \texttt{[]}_\alpha, \texttt{false}\colon \kappa_2\}}$ ($\nearrow$-elim-false)

$\kappa_2 \searrow_{\vec{\pi}} \kappa_1', \beta \sqsubseteq \kappa_1, \alpha \quad (\exists \kappa_1', \beta)$ (IH)

$\Rightarrow \dfrac{\kappa_2 \searrow_{\vec{\pi}} \kappa_1', \beta}{\{\texttt{true}\colon \texttt{[]}_\alpha, \texttt{false}\colon \kappa_2\} \searrow_{\texttt{false}\cdot\vec{\pi}} \{\texttt{false}\colon \kappa_1'\}, \alpha \sqcup \beta}$ ($\searrow$-false)

$\Rightarrow (\{\texttt{false}\colon \kappa_1'\}, \alpha \sqcup \beta) \sqsubseteq (\{\texttt{false}\colon \kappa_1\}, \alpha)$

Case $\dfrac{\sigma_1, \alpha \nearrow_{p\cdot p'\cdot\vec{\pi}} \sigma_2}{\{(\texttt{,})\colon \sigma_1\}, \alpha \nearrow_{(p,p')\cdot\vec{\pi}} \{(\texttt{,})\colon \sigma_2\}}$ ($\nearrow$-elim-prod)

$\sigma_2 \searrow_{p\cdot p'\cdot\vec{\pi}} \sigma_1', \beta \sqsubseteq \sigma_1, \alpha \quad (\exists \sigma_1', \beta)$ (IH)

$\Rightarrow \dfrac{\sigma_2 \searrow_{p\cdot p'\cdot\vec{\pi}} \sigma_1', \beta}{\{(\texttt{,})\colon \sigma_2\} \searrow_{(p,p')\cdot\vec{\pi}} \{(\texttt{,})\colon \sigma_1'\}, \beta}$ ($\searrow$-prod)

$\Rightarrow (\{(\texttt{,}) \colon \sigma_1'\}, \beta) \sqsubseteq (\{(\texttt{,}) \colon \sigma_1\}, \alpha)$

Case $\dfrac{\kappa_1, \alpha \nearrow_{\overrightarrow{\pi}} \kappa_2}{\{[\,] \colon \kappa_1\}, \alpha \nearrow_{[\,]\cdot\overrightarrow{\pi}} \{[\,] \colon \kappa_2, (\texttt{:}) \colon x \colon y \colon []_\alpha\}}$ ($\nearrow$-elim-nil)

$\kappa_2 \searrow_{\overrightarrow{\pi}} \kappa_1', \beta \sqsubseteq \kappa_1, \alpha \quad (\exists \kappa_1', \beta)$ (IH)

$\Rightarrow$ $\dfrac{\kappa_2 \searrow_{\overrightarrow{\pi}} \kappa_1', \beta}{\{[\,] \colon \kappa_2, (\texttt{:}) \colon x \colon y \colon []_\alpha\} \searrow_{[\,]\cdot\overrightarrow{\pi}} \{[\,] \colon \kappa_1'\}, \alpha \sqcup \beta}$ ($\searrow$-nil)

$\Rightarrow (\{[\,] \colon \kappa_1'\}, \alpha \sqcup \beta) \sqsubseteq (\{[\,] \colon \kappa_1\}, \alpha)$

Case $\dfrac{\sigma_1, \alpha \nearrow_{p\cdot p'\cdot\overrightarrow{\pi}} \sigma_2}{\{(\texttt{:}) \colon \sigma_1\}, \alpha \nearrow_{(p\,:\,p')\cdot\overrightarrow{\pi}} \{[\,] \colon []_\alpha, (\texttt{:}) \colon \sigma_2\}}$ ($\nearrow$-elim-cons)

$\sigma_2 \searrow_{p\cdot p'\cdot\overrightarrow{\pi}} \sigma_1', \beta \sqsubseteq \sigma_1, \alpha \quad (\exists \sigma_1', \beta)$ (IH)

$\Rightarrow$ $\dfrac{\sigma_2 \searrow_{p\cdot p'\cdot\overrightarrow{\pi}} \sigma_1', \beta}{\{[\,] \colon []_\alpha, (\texttt{:}) \colon \sigma_2\} \searrow_{(p\,:\,p')\cdot\overrightarrow{\pi}} \{(\texttt{:}) \colon \sigma_1'\}, \alpha \sqcup \beta}$ ($\searrow$-cons)

$\Rightarrow (\{(\texttt{:}) \colon \sigma_1'\}, \alpha \sqcup \beta) \sqsubseteq (\{(\texttt{:}) \colon \sigma_1\}, \alpha)$

Case $\dfrac{\sigma_1, \alpha \nearrow_{p\cdot o\cdot\overrightarrow{\pi}} \sigma_2}{\{(\texttt{:}) \colon \sigma_1\}, \alpha \nearrow_{([\;p\;o)\cdot\overrightarrow{\pi}} \{[\,] \colon []_\alpha, (\texttt{:}) \colon \sigma_2\}}$ ($\nearrow$-elim-non-empty-list)

$\sigma_2 \searrow_{p\cdot o\cdot\overrightarrow{\pi}} \sigma_1', \beta \sqsubseteq \sigma_1, \alpha \quad (\exists \sigma_1', \beta)$ (IH)

$\Rightarrow$ $\dfrac{\sigma_2 \searrow_{p\cdot o\cdot\overrightarrow{\pi}} \sigma_1', \beta}{\{[\,] \colon []_\alpha, (\texttt{:}) \colon \sigma_2\} \searrow_{([\;p\;o)\cdot\overrightarrow{\pi}} \{(\texttt{:}) \colon \sigma_1'\}, \alpha \sqcup \beta}$ ($\searrow$-non-empty-list)

$\Rightarrow (\{(\texttt{:}) \colon \sigma_1'\}, \alpha \sqcup \beta) \sqsubseteq (\{(\texttt{:}) \colon \sigma_1\}, \alpha)$

Case $\dfrac{\kappa_1, \alpha \nearrow_{\overrightarrow{\pi}} \kappa_2}{\{[\,] \colon \kappa_1\}, \alpha \nearrow_{]\cdot\overrightarrow{\pi}} \{[\,] \colon \kappa_2, (\texttt{:}) \colon x \colon y \colon []_\alpha\}}$ ($\nearrow$-elim-list-rest-end)

$\kappa_2 \searrow_{\overrightarrow{\pi}} \kappa_1', \beta \sqsubseteq \kappa_1, \alpha \quad (\exists \kappa_1', \beta)$ (IH)

$\Rightarrow$ $\dfrac{\kappa_2 \searrow_{\overrightarrow{\pi}} \kappa_1', \beta}{\{[\,] \colon \kappa_2, (\texttt{:}) \colon x \colon y \colon []_\alpha\} \searrow_{]\cdot\overrightarrow{\pi}} \{[\,] \colon \kappa_1'\}, \alpha \sqcup \beta}$ ($\searrow$-list-rest-end)

$\Rightarrow (\{[\,] \colon \kappa_1'\}, \alpha \sqcup \beta) \sqsubseteq (\{[\,] \colon \kappa_1\}, \alpha)$

Case $\dfrac{\sigma_1, \alpha \nearrow_{p \cdot o \cdot \vec{\pi}} \sigma_2}{\{(\texttt{:}) \colon \sigma_1\}, \alpha \nearrow_{(\ p\ o) \cdot \vec{\pi}} \{[\,] \colon [\,]_\alpha, (\texttt{:}) \colon \sigma_2\}}$ ↗-elim-list-rest-cons

$\sigma_2 \searrow_{p \cdot o \cdot \vec{\pi}} \sigma_1', \beta \sqsubseteq \sigma_1, \alpha \quad (\exists \sigma_1', \beta)$ (IH)

$\Rightarrow \dfrac{\sigma_2 \searrow_{p \cdot o \cdot \vec{\pi}} \sigma_1', \beta}{\{[\,] \colon [\,]_\alpha, (\texttt{:}) \colon \sigma_2\} \searrow_{(\ p\ o) \cdot \vec{\pi}} \{(\texttt{:}) \colon \sigma_1'\}, \alpha \sqcup \beta}$ ↘-list-rest-cons

$\Rightarrow (\{(\texttt{:}) \colon \sigma_1'\}, \alpha \sqcup \beta) \sqsubseteq (\{(\texttt{:}) \colon \sigma_1\}, \alpha)$

□