Running Probabilistic Programs Backward

Neil Toronto   Jay McCarthy

PLT @ Brigham Young University

ntoronto@racket-lang.org   jay@cs.byu.edu

Abstract

XXX

Categories and Subject Descriptors XXX-CR-number [*XXX-subcategory*]: XXX-third-level

General Terms XXX, XXX

Keywords XXX, XXX

1. Introduction

XXX: conditional probability, measure-theory's take on probability (especially preimage measure)

In this paper, we

1. Define the *bottom arrow*, type $\mathsf{X} \rightsquigarrow_{\bot} \mathsf{Y}$, as a compilation target for first-order functions that may raise errors.
2. Derive the *mapping arrow* from the bottom arrow, type $\mathsf{X} \underset{\mathsf{map}}{\rightsquigarrow} \mathsf{Y}$. Prove that its instances return extensional functions, or mappings, that compute the same values as corresponding bottom arrow computations.
3. Derive the *preimage arrow* from the mapping arrow, type $\mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Y}$. Prove that its instances compute preimages under corresponding mapping (or bottom) arrow instances.
4. Define an arrow transformer via a natural transformation η to thread random stores and avoid divergence.
5. Define a computable approximation of the transformed preimage arrow and report on its implementation.

Most of our correctness theorems can be described in terms of the following commutative diagram:

$$\begin{tikzcd}
\mathsf{X} \rightsquigarrow_{\bot} \mathsf{Y} \arrow[r, "\mathsf{lift_{map}}"] \arrow[d, "\eta_{\bot *}"'] & \mathsf{X} \underset{\mathsf{map}}{\rightsquigarrow} \mathsf{Y} \arrow[r, "\mathsf{lift_{pre}}"] \arrow[d, "\eta_{\mathsf{map} *}"] & \mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Y} \arrow[d, "\eta_{\mathsf{pre} *}"] \\
\mathsf{X} \rightsquigarrow_{\bot *} \mathsf{Y} \arrow[r, "\mathsf{lift_{map*}}"'] & \mathsf{X} \underset{\mathsf{map*}}{\rightsquigarrow} \mathsf{Y} \arrow[r, "\mathsf{lift_{pre*}}"'] & \mathsf{X} \underset{\mathsf{pre*}}{\rightsquigarrow} \mathsf{Y}
\end{tikzcd} \qquad (1)$$

We prove that all the functions between arrow types in (1) are homomorphisms, which implies that $\mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Y}$ and $\mathsf{X} \underset{\mathsf{pre*}}{\rightsquigarrow} \mathsf{Y}$ instances compute preimages correctly.

XXX: something about how we know the approximations are correct

2. Operational Metalanguage

From here on, significant terms are introduced in **bold**, and significant terms we invent are introduced in ***bold italics***.

We write all of the programs in this paper in λ_{ZFC} [2], an untyped, call-by-value lambda calculus designed for deriving implementable programs from contemporary mathematics.

Contemporary mathematics is generally done in **ZFC**: **Zermelo-Fraenkel** set theory extended with the axiom of **Choice** (equivalently unique **Cardinality**). ZFC has only first-order functions and no general recursion, which makes implementing a language defined by a transformation into contemporary mathematics quite difficult. The problem is exacerbated if implementing the language requires approximation. Targeting λ_{ZFC} instead allows creating a precise mathematical specification and deriving an approximating implementation without changing languages.

In λ_{ZFC}, essentially every set is a value, as well as every lambda and every set of lambdas. All operations, including operations on infinite sets, are assumed to complete instantly if they terminate.[1]

Almost everything definable in contemporary mathematics can be formally defined by a finite λ_{ZFC} program, except objects that most mathematicians would agree are nonconstructive. More precisely, any object that *must* be defined by a statement of existence and uniqueness without giving a bounding set is not definable by a *finite* λ_{ZFC} program.

Because λ_{ZFC} includes an inner model of ZFC, essentially every contemporary theorem applies to λ_{ZFC}'s set values without alteration. Further, proofs about λ_{ZFC}'s set values apply to contemporary mathematical objects.[2]

In λ_{ZFC}, algebraic data structures are encoded as sets; e.g. a ***primitive ordered pair*** of x and y is $\{\{\mathsf{x}\}, \{\mathsf{x}, \mathsf{y}\}\}$. Only the *existence* of encodings into sets is important, as it means data structures inherit a defining characteristic of sets: strictness. More precisely, the lengths of paths to data structure leaves is unbounded, but each path must be finite. Less precisely, data may be "infinitely wide" (such as $\mathbb{R}$) but not "infinitely tall" (such as infinite trees and lists).

We assume data structures, including pairs, are encoded as *primitive* ordered pairs with the first element a unique tag, so that they can be distinguished by checking tags. Accessors such as fst and snd are trivial to define.

λ_{ZFC} is untyped so its users can define an auxiliary type system that best suits their application area. For this work, we use an informal, manually checked, polymorphic type system characterized by these rules:

- A free lowercase type variable is universally quantified.

[1] An example of a nonterminating λ_{ZFC} function is one that attempts to decide whether other λ_{ZFC} programs halt.

[2] Assuming the existence of an inaccessible cardinal.

- A free uppercase type variable is a set.
- A set denotes a member of that set.
- $\mathsf{x} \Rightarrow \mathsf{y}$ denotes a partial function.
- $\langle \mathsf{x}, \mathsf{y} \rangle$ denotes a pair of values with types x and y.
- $\mathsf{Set}\ \mathsf{x}$ denotes a set with members of type x.

The type $\mathsf{Set}\ \mathsf{X}$ denotes the same values as the powerset $\mathcal{P}\ \mathsf{X}$, or *subsets* of X. Similarly, the type $\langle \mathsf{X}, \mathsf{Y} \rangle$ denotes the same values as the product set $\mathsf{X} \times \mathsf{Y}$.

We write λ_{ZFC} programs in heavily sugared λ-calculus syntax, with an if expression and these additional primitives:

$$\begin{array}{rr} \mathsf{true} : \mathsf{Bool} & (\in) : \mathsf{x} \Rightarrow \mathsf{Set}\ \mathsf{x} \Rightarrow \mathsf{Bool} \\ \mathsf{false} : \mathsf{Bool} & \mathcal{P} : \mathsf{Set}\ \mathsf{x} \Rightarrow \mathsf{Set}\ (\mathsf{Set}\ \mathsf{x}) \\ \varnothing : \mathsf{Set}\ \mathsf{x} & \bigcup : \mathsf{Set}\ (\mathsf{Set}\ \mathsf{x}) \Rightarrow \mathsf{Set}\ \mathsf{x} \\ \omega : \mathsf{Ord} & \mathsf{image} : (\mathsf{x} \Rightarrow \mathsf{y}) \Rightarrow \mathsf{Set}\ \mathsf{x} \Rightarrow \mathsf{Set}\ \mathsf{y} \\ \mathsf{take} : \mathsf{Set}\ \mathsf{x} \Rightarrow \mathsf{x} & |\cdot| : \mathsf{Set}\ \mathsf{x} \Rightarrow \mathsf{Ord} \end{array} \tag{2}$$

Shortly, $\varnothing$ is the empty set, ω is the cardinality of the natural numbers, $\mathsf{take}\ \{\mathsf{x}\}$ reduces to x and diverges for non-singleton sets, $\mathsf{x} \in \mathsf{A}$ decides membership, $\mathcal{P}\ \mathsf{A}$ reduces to the set of subsets of A, $\bigcup \mathcal{A}$ reduces to the union of the sets in $\mathcal{A}$, $\mathsf{image}\ \mathsf{f}\ \mathsf{A}$ applies f to each member of A and reduces to the set of results, and $|\mathsf{A}|$ reduces to the cardinality of A.

We assume literal set notation such as $\{0, 1, 2\}$ is already defined in terms of the set primitives.

2.1 Internal and External Equality

Set theory extends first-order logic with an axiom that defines equality to be extensional, and with axioms that ensure the existence of sets in the domain of discourse. λ_{ZFC} is defined the same way as any other operational λ-calculus: by (conservatively) extending the domain of discourse with expressions and defining a reduction relation.

While λ_{ZFC} does not have an equality primitive, set theory's extensional equality can be recovered internally using $(\in)$. *Internal* extensional equality is defined by

$$\mathsf{x} = \mathsf{y}\ :=\ \mathsf{x} \in \{\mathsf{y}\} \tag{3}$$

which means

$$(=)\ :=\ \lambda \mathsf{x}.\, \lambda \mathsf{y}.\, \mathsf{x} \in \{\mathsf{y}\} \tag{4}$$

Thus, $1 = 1$ reduces to $1 \in \{1\}$, which reduces to true.[3] Because of the particular way λ_{ZFC}'s lambda terms are defined, for two lambda terms f and g, $\mathsf{f} = \mathsf{g}$ reduces to true when f and g are structurally identical modulo renaming. For example, $(\lambda \mathsf{x}.\, \mathsf{x}) = (\lambda \mathsf{y}.\, \mathsf{y})$ reduces to true, but $(\lambda \mathsf{x}.\, 2) = (\lambda \mathsf{x}.\, 1 + 1)$ reduces to false.

We understand any λ_{ZFC} term e used as a truth statement as shorthand for "e reduces to true." Therefore, while the terms $(\lambda \mathsf{x}.\, \mathsf{x})\ 1$ and 1 are (externally, extensionally) unequal, we can say that $(\lambda \mathsf{x}.\, \mathsf{x})\ 1 = 1$.

Any truth statement e implies that e converges. In particular, the truth statement $e_1 = e_2$ implies that both e_1 and e_2 converge. However, we often want to say that e_1 and e_1 are equivalent when they both diverge. In these cases, we use a slightly weaker equivalence.

Definition 2.1.1 (observational equivalence)**.** *Two λ_{ZFC} terms e_1 and e_2 are **observationally equivalent**, written $e_1 \equiv e_2$, when $e_1 = e_2$ or both e_1 and e_2 diverge.*

[3] Technically, λ_{ZFC} has a big-step semantics, and the derivation tree for $1 = 1$ contains the derivation tree for $1 \in \{1\}$.

It could be helpful to introduce even coarser notions of equivalence, such as applicative or logical bisimilarity. However, we do not want internal equality and external equivalence to differ too much. We therefore introduce type-specific notions of equivalence as needed.

2.2 Additional Functions and Forms

We assume a desugaring pass over λ_{ZFC} expressions, which automatically curries (including for the two-argument primitives $(\in)$ and image), and interprets special binding forms such as indexed unions $\bigcup_{x \in e_A} e$, destructuring binds as in $\mathsf{swap}\ \langle \mathsf{x}, \mathsf{y} \rangle := \langle \mathsf{y}, \mathsf{x} \rangle$, and comprehensions like $\{\mathsf{x} \in \mathsf{A} \mid \mathsf{x} \in \mathsf{B}\}$. (We may be rather informal with the latter two binding forms when the meaning is clear.) We assume we have logical operators, bounded quantifiers (unbounded quantifiers are not λ_{ZFC}-definable), and typical set operations.

We define atypical set operations, such as disjoint union:

$$\begin{aligned} &(\uplus) : \mathsf{Set}\ \mathsf{x} \Rightarrow \mathsf{Set}\ \mathsf{x} \Rightarrow \mathsf{Set}\ \mathsf{x} \\ &\mathsf{A} \uplus \mathsf{B}\ :=\ \mathsf{if}\ (\mathsf{A} \cap \mathsf{B} = \varnothing)\ (\mathsf{A} \cup \mathsf{B})\ (\mathsf{take}\ \varnothing) \end{aligned} \tag{5}$$

which diverges when A and B overlap.

In set theory, functions are encoded as sets of input-output pairs. The increment function for the natural numbers, for example, is $\{\langle 0, 1 \rangle, \langle 1, 2 \rangle, \langle 2, 3 \rangle, ...\}$. To distinguish these hash tables from lambdas, we call them ***mappings***, and use the word **function** for either a lambda or a mapping. For convenience, as with lambdas, we use adjacency (i.e. $(\mathsf{f}\ \mathsf{x})$) to apply mappings.

The set $\mathsf{X} \rightharpoonup \mathsf{Y}$ contains all the *partial* mappings from X to Y. For example, $\mathsf{X} \rightharpoonup \mathsf{Y}$ is the return type for the restriction function:

$$\begin{aligned} &(\cdot)|_{(\cdot)} : (\mathsf{X} \Rightarrow \mathsf{Y}) \Rightarrow \mathsf{Set}\ \mathsf{X} \Rightarrow (\mathsf{X} \rightharpoonup \mathsf{Y}) \\ &\mathsf{f}|_{\mathsf{A}}\ :=\ \mathsf{image}\ (\lambda \mathsf{x}.\, \langle \mathsf{x}, \mathsf{f}\ \mathsf{x} \rangle)\ \mathsf{A} \end{aligned} \tag{6}$$

which converts a lambda or a mapping to a mapping with domain $\mathsf{A} \subseteq \mathsf{X}$. To create mappings using lambda syntax, we define $\lambda x \in e_A.\, e$ as shorthand for $(\lambda x.\, e)|_{e_A}$.

Figure 1 defines more operations on partial mappings: domain, range, $\mathsf{preimage}$, pairing, composition, and disjoint union. The latter three are particularly important in the preimage arrow's derivation, and $\mathsf{preimage}$ is critical in measure theory's account of probability.

The set $\mathsf{X} \to \mathsf{Y}$ contains all the *total* mappings from X to Y. We think of these as possibly infinite vectors, with application for indexing. Projections are produced by

$$\begin{aligned} &\pi : \mathsf{J} \Rightarrow (\mathsf{J} \to \mathsf{X}) \Rightarrow \mathsf{X} \\ &\pi\ \mathsf{j}\ \mathsf{f}\ :=\ \mathsf{f}\ \mathsf{j} \end{aligned} \tag{7}$$

which will be useful when f is unnamed.

Pairs $\langle \mathsf{A}, \mathsf{f} \rangle : \langle \mathsf{Set}\ \mathsf{x}, \mathsf{x} \Rightarrow \mathsf{y} \rangle$ are like functions with an observable domain and range; we call them ***lazy mappings***. We do not use them in this paper, but we define a similar function-like type in Section 5 for computing preimages.

3. Arrows and First-Order Semantics

XXX: really short arrow intro (XXX: cite Hughes, Lindley et al)

3.1 Alternative Arrow Definitions

For every arrow a in this paper, we do not give a typical minimal definition. Instead of $\mathsf{first}_{\mathsf{a}}$, we define $(\&\&\&_{\mathsf{a}})$—typically called **fanout**, but its use will be clearer if we call it **pairing**—which applies two functions to an input and returns the pair of their outputs. Though $\mathsf{first}_{\mathsf{a}}$ may be defined in

$$\mathsf{domain} : (\mathsf{X} \rightharpoonup \mathsf{Y}) \Rightarrow \mathsf{Set\ X}$$
$$\mathsf{domain} \ := \ \mathsf{image\ fst}$$

$$\mathsf{range} : (\mathsf{X} \rightharpoonup \mathsf{Y}) \Rightarrow \mathsf{Set\ Y}$$
$$\mathsf{range} \ := \ \mathsf{image\ snd}$$

$$\mathsf{preimage} : (\mathsf{X} \rightharpoonup \mathsf{Y}) \Rightarrow \mathsf{Set\ Y} \Rightarrow \mathsf{Set\ X}$$
$$\mathsf{preimage\ f\ B} \ := \ \{\mathsf{x} \in \mathsf{domain\ f} \mid \mathsf{f\ x} \in \mathsf{B}\}$$

$$\langle\cdot,\cdot\rangle_{\mathsf{map}} : (\mathsf{X} \rightharpoonup \mathsf{Y_1}) \Rightarrow (\mathsf{X} \rightharpoonup \mathsf{Y_2}) \Rightarrow (\mathsf{X} \rightharpoonup \mathsf{Y_1} \times \mathsf{Y_2})$$
$$\begin{aligned}\langle \mathsf{g_1}, \mathsf{g_2}\rangle_{\mathsf{map}} \ := \ & \mathsf{let}\ \ \mathsf{A} := (\mathsf{domain\ g_1}) \cap (\mathsf{domain\ g_2}) \\ & \mathsf{in}\ \ \lambda \mathsf{x} \in \mathsf{A}.\ \langle \mathsf{g_1\ x}, \mathsf{g_2\ x}\rangle\end{aligned}$$

$$(\circ_{\mathsf{map}}) : (\mathsf{Y} \rightharpoonup \mathsf{Z}) \Rightarrow (\mathsf{X} \rightharpoonup \mathsf{Y}) \Rightarrow (\mathsf{X} \rightharpoonup \mathsf{Z})$$
$$\begin{aligned}\mathsf{g_2} \circ_{\mathsf{map}} \mathsf{g_1} \ := \ & \mathsf{let}\ \ \mathsf{A} := \mathsf{preimage\ g_1\ (domain\ g_2)} \\ & \mathsf{in}\ \ \lambda \mathsf{x} \in \mathsf{A}.\ \mathsf{g_2\ (g_1\ x)}\end{aligned}$$

$$(\uplus_{\mathsf{map}}) : (\mathsf{X} \rightharpoonup \mathsf{Y}) \Rightarrow (\mathsf{X} \rightharpoonup \mathsf{Y}) \Rightarrow (\mathsf{X} \rightharpoonup \mathsf{Y})$$
$$\begin{aligned}\mathsf{g_1} \uplus_{\mathsf{map}} \mathsf{g_2} \ := \ & \mathsf{let}\ \ \mathsf{A} := (\mathsf{domain\ g_1}) \uplus (\mathsf{domain\ g_2}) \\ & \mathsf{in}\ \ \lambda \mathsf{x} \in \mathsf{A}.\ \mathsf{if}\ (\mathsf{x} \in \mathsf{domain\ g_1})\ (\mathsf{g_1\ x})\ (\mathsf{g_2\ x})\end{aligned}$$

Figure 1: Operations on mappings.

terms of $(\&\&\&_{\mathsf{a}})$ and vice-versa [1], we give $(\&\&\&_{\mathsf{a}})$ definitions in this paper because the applicable contemporary theorems are in terms of pairing functions.

One way to strengthen an arrow a is to define an additional combinator $\mathsf{left_a}$, which can be used to choose an arrow computation based on the result of another. Again, we define a different combinator, $\mathsf{ifte_a}$, to make it easier to apply contemporary theorems.

In a nonstrict λ-calculus, simply defining a choice combinator allows writing recursive functions using nothing but arrow combinators and lifted, pure functions. However, any strict λ-calculus (such as λ_{ZFC}) requires an extra combinator to defer computations in conditional branches.

For example, suppose we define the **function arrow** with choice, by defining

$$\begin{aligned}\mathsf{arr\ f} \ &:= \ \mathsf{f} \\ (\mathsf{f_1} \ggg \mathsf{f_2})\ \mathsf{a} \ &:= \ \mathsf{f_2\ (f_1\ a)} \\ (\mathsf{f_1}\ \&\&\&\ \mathsf{f_2})\ \mathsf{a} \ &:= \ \langle \mathsf{f_1\ a}, \mathsf{f_2}, \mathsf{a}\rangle \\ \mathsf{ifte\ f_1\ f_2\ f_3\ a} \ &:= \ \mathsf{if\ (f_1\ a)\ (f_2\ a)\ (f_3\ a)}\end{aligned} \tag{8}$$

and try to define the following recursive function:

$$\mathsf{halt\text{-}on\text{-}true} \ := \ \mathsf{ifte\ (arr\ id)\ (arr\ id)\ halt\text{-}on\text{-}true} \tag{9}$$

The defining expression diverges in a strict λ-calculus. In a nonstrict λ-calculus, it diverges only when applied to false.

Using $\mathsf{lazy\ f\ a} := \mathsf{f\ 0\ a}$, which receives thunks and returns arrow computations, we can write $\mathsf{halt\text{-}on\text{-}true}$ as

$$\mathsf{halt\text{-}on\text{-}true} \ := \ \mathsf{ifte\ (arr\ id)\ (arr\ id)\ (lazy}\ \lambda 0.\ \mathsf{halt\text{-}on\text{-}true)} \tag{10}$$

which diverges only when applied to false in any λ-calculus.

Definition 3.1.1 (arrow with choice)**.** *A binary type constructor* $(\leadsto_{\mathsf{a}})$ *and the combinators*

$$\begin{aligned}\mathsf{arr_a} &: (\mathsf{x} \Rightarrow \mathsf{y}) \Rightarrow (\mathsf{x} \leadsto_{\mathsf{a}} \mathsf{y}) \\ (\ggg_{\mathsf{a}}) &: (\mathsf{x} \leadsto_{\mathsf{a}} \mathsf{y}) \Rightarrow (\mathsf{y} \leadsto_{\mathsf{a}} \mathsf{z}) \Rightarrow (\mathsf{x} \leadsto_{\mathsf{a}} \mathsf{z}) \\ (\&\&\&_{\mathsf{a}}) &: (\mathsf{x} \leadsto_{\mathsf{a}} \mathsf{y}) \Rightarrow (\mathsf{x} \leadsto_{\mathsf{a}} \mathsf{z}) \Rightarrow (\mathsf{x} \leadsto_{\mathsf{a}} \langle \mathsf{y}, \mathsf{z}\rangle)\end{aligned} \tag{11}$$

define an ***arrow*** *if certain monoid, homomorphism, and structural laws hold. The additional combinators*

$$\begin{aligned}\mathsf{ifte_a} &: (\mathsf{x} \leadsto_{\mathsf{a}} \mathsf{Bool}) \Rightarrow (\mathsf{x} \leadsto_{\mathsf{a}} \mathsf{y}) \Rightarrow (\mathsf{x} \leadsto_{\mathsf{a}} \mathsf{y}) \Rightarrow (\mathsf{x} \leadsto_{\mathsf{a}} \mathsf{y}) \\ \mathsf{lazy_a} &: (1 \Rightarrow (\mathsf{x} \leadsto_{\mathsf{a}} \mathsf{y})) \Rightarrow (\mathsf{x} \leadsto_{\mathsf{a}} \mathsf{y})\end{aligned} \tag{12}$$

define an ***arrow with choice*** *if certain additional homomorphism and structural laws hold.*

From here on, as all of our arrows are arrows with choice, we simply call them arrows.

The necessary homomorphism laws ensure that $\mathsf{arr_a}$ distributes over function arrow combinators. These laws can be put in terms of more general homomorphism properties that deal with distributing an arrow-to-arrow lift, which we use extensively to prove correctness.

Definition 3.1.2 (arrow homomorphism)**.** *A function* $\mathsf{lift_b} : (\mathsf{x} \leadsto_{\mathsf{a}} \mathsf{y}) \Rightarrow (\mathsf{x} \leadsto_{\mathsf{b}} \mathsf{y})$ *is an* ***arrow homomorphism*** *from arrow* a *to arrow* b *if the following distributive laws hold for appropriately typed* f*,* $\mathsf{f_1}$*,* $\mathsf{f_2}$ *and* $\mathsf{f_3}$*:*

$$\mathsf{lift_b\ (arr_a\ f)} \ \equiv \ \mathsf{arr_b\ f} \tag{13}$$
$$\mathsf{lift_b}\ (\mathsf{f_1} \ggg_{\mathsf{a}} \mathsf{f_2}) \ \equiv \ (\mathsf{lift_b\ f_1}) \ggg_{\mathsf{b}} (\mathsf{lift_b\ f_2}) \tag{14}$$
$$\mathsf{lift_b}\ (\mathsf{f_1}\ \&\&\&_{\mathsf{a}}\ \mathsf{f_2}) \ \equiv \ (\mathsf{lift_b\ f_1})\ \&\&\&_{\mathsf{b}}\ (\mathsf{lift_b\ f_2}) \tag{15}$$
$$\mathsf{lift_b\ (ifte_a\ f_1\ f_2\ f_3)} \ \equiv \ \mathsf{ifte_b\ (lift_b\ f_1)\ (lift_b\ f_2)\ (lift_b\ f_3)} \tag{16}$$
$$\mathsf{lift_b\ (lazy_a\ f)} \ \equiv \ \mathsf{lazy_b}\ \lambda 0.\ \mathsf{lift_b\ (f\ 0)} \tag{17}$$

The homomorphism laws state that $\mathsf{arr_a}$ must be a homomorphism from the function arrow to arrow a.

The monoid and structural arrow laws play little role in our semantics or its correctness. For the arrows we define, then, we elide the proofs of these arrow laws, and concentrate on homomorphisms.

XXX: actually, need to prove some of them, to prove that the natural transformation for the applicative store-passing arrow transformer is a homomorphism

3.2 First-Order Let-Calculus Semantics

XXX: Figure 2...

XXX: Stack machine...

XXX: Roughly, first-order application $(x\ e)$ runs arrow computation x with a fresh stack with e at the head. The binding form $(\mathsf{let}\ e_0\ e_b)$ pushes e_0 onto the stack. Variables are referenced using $(\mathsf{env}\ n)$ with $(\mathsf{env}\ 0)$ referring to the head.

4. The Bottom and Mapping Arrows

We are certain that the preimage arrow correctly computes preimages under some function f because we ultimately *derive* it from a simpler arrow used to construct f.

One obvious candidate for the simpler arrow is the function arrow, defined in (8). However, we will need to explicitly

$$
\begin{aligned}
[\![x := e;\ \cdots]\!]_{\mathsf{a}} &:\equiv x := [\![e]\!]_{\mathsf{a}}\,;\ \cdots \\
[\![x\ e]\!]_{\mathsf{a}} &:\equiv [\![\langle e, 0\rangle]\!]_{\mathsf{a}} \ggg_{\mathsf{a}} x \\
[\![\langle e_1, e_2\rangle]\!]_{\mathsf{a}} &:\equiv [\![e_1]\!]_{\mathsf{a}}\ \&\&\&_{\mathsf{a}}\ [\![e_2]\!]_{\mathsf{a}} \\
[\![\mathsf{let}\ e_0\ e_b]\!]_{\mathsf{a}} &:\equiv ([\![e_0]\!]_{\mathsf{a}}\ \&\&\&_{\mathsf{a}}\ (\mathsf{arr_a\ id})) \ggg_{\mathsf{a}} [\![e_b]\!]_{\mathsf{a}} \\
[\![\mathsf{env}\ n]\!]_{\mathsf{a}} &:\equiv \mathsf{arr_a}\ \lambda\gamma.\,\mathsf{list\text{-}ref}\ \gamma\ n \\
[\![\mathsf{if}\ e_c\ e_t\ e_f]\!]_{\mathsf{a}} &:\equiv \mathsf{ifte_a}\ [\![e_c]\!]_{\mathsf{a}}\ (\mathsf{lazy_a}\ \lambda 0.\,[\![e_t]\!]_{\mathsf{a}})\ (\mathsf{lazy_a}\ \lambda 0.\,[\![e_f]\!]_{\mathsf{a}})
\end{aligned}
\qquad
\begin{aligned}
[\![v]\!]_{\mathsf{a}} &:\equiv \mathsf{arr_a}\ \lambda\gamma.\,v \\
[\![\mathsf{fst}\ e]\!]_{\mathsf{a}} &:\equiv [\![e]\!]_{\mathsf{a}} \ggg_{\mathsf{a}} (\mathsf{arr_a\ fst}) \\
[\![\mathsf{snd}\ e]\!]_{\mathsf{a}} &:\equiv [\![e]\!]_{\mathsf{a}} \ggg_{\mathsf{a}} (\mathsf{arr_a\ snd}) \\
[\![e_1 + e_2]\!]_{\mathsf{a}} &:\equiv [\![\langle e_1, e_2\rangle]\!]_{\mathsf{a}} \ggg_{\mathsf{a}} (\mathsf{arr_a}\ \lambda\langle \mathsf{x},\mathsf{y}\rangle.\,\mathsf{x}+\mathsf{y}) \\
[\![e_1 < e_2]\!]_{\mathsf{a}} &:\equiv [\![\langle e_1, e_2\rangle]\!]_{\mathsf{a}} \ggg_{\mathsf{a}} (\mathsf{arr_a}\ \lambda\langle \mathsf{x},\mathsf{y}\rangle.\,\mathsf{x}<\mathsf{y}) \\
&\cdots
\end{aligned}
$$

Figure 2: Transformation from a let-calculus with first-order definitions and De-Bruijn-indexed bindings to computations in arrow a.

handle divergence, so we need a slightly more complicated arrow for which running computations may raise an error.

Figure 3 defines the ***bottom arrow***. Its computations are of type $\mathsf{x} \rightsquigarrow_\perp \mathsf{y} ::= \mathsf{x} \Rightarrow \mathsf{y}_\perp$, where the inhabitants of $\mathsf{y}_\perp$ are the error value $\perp$ as well as the inhabitants of y. The type $\mathsf{Bool}_\perp$, for example, denotes the members of $\mathsf{Bool} \cup \{\perp\}$.

Theorem 4.0.1. *$\mathsf{arr}_\perp$, $(\&\&\&_\perp)$, $(\ggg_\perp)$, $\mathsf{ifte}_\perp$ and $\mathsf{lazy}_\perp$ define an arrow.*

Proof. The bottom arrow is the Maybe monad's Kleisli arrow with $\mathsf{Nothing} = \perp$. □

4.1 Deriving the Mapping Arrow

Contemporary theorems about functions are about mappings, not lambdas. As in intermediate step toward the preimage arrow, then, we need an arrow whose computations produce mappings or are mappings themselves.

It is tempting to try to define the mapping arrow's type constructor as $\mathsf{X} \underset{\mathsf{map}}{\rightsquigarrow} \mathsf{Y} ::= \mathsf{X} \rightharpoonup \mathsf{Y}$, and define $\mathsf{f}_1 \ggg_{\mathsf{map}} \mathsf{f}_2 := \mathsf{f}_2 \circ_{\mathsf{map}} \mathsf{f}_1$ and $(\&\&\&_{\mathsf{map}}) := \langle\cdot,\cdot\rangle_{\mathsf{map}}$. Unfortunately, we run into a problem defining $\mathsf{arr_{map}} : (\mathsf{X} \Rightarrow \mathsf{Y}) \Rightarrow (\mathsf{X} \rightharpoonup \mathsf{Y})$: to define a mapping, we need a domain, but lambdas' domains are unobservable.

To parameterize mapping arrow computations on a domain, we define the ***mapping arrow*** computation type as

$$\mathsf{X} \underset{\mathsf{map}}{\rightsquigarrow} \mathsf{Y} \ ::=\ \mathsf{Set\ X} \Rightarrow (\mathsf{X} \rightharpoonup \mathsf{Y}) \tag{18}$$

Notice that $\perp$ is absent in $\mathsf{Set\ X} \Rightarrow (\mathsf{X} \rightharpoonup \mathsf{Y})$. This will make it easier to disregard diverging inputs when computing preimages further on. (XXX: section)

To make the correspondence between bottom arrow and mapping arrow computations as clear as possible, we start by defining a function $\mathsf{lift_{map}} : (\mathsf{X} \rightsquigarrow_\perp \mathsf{Y}) \Rightarrow (\mathsf{X} \underset{\mathsf{map}}{\rightsquigarrow} \mathsf{Y})$ to lift bottom arrow computations. It must restrict its argument f's domain to a subset of X for which f does not return $\perp$. It is helpful to have a standalone function $\mathsf{domain}_\perp$ that computes such domains, so we define that first, and then define $\mathsf{lift_{map}}$ in terms of it:

$$
\begin{aligned}
&\mathsf{domain}_\perp : (\mathsf{X} \rightsquigarrow_\perp \mathsf{Y}) \Rightarrow \mathsf{Set\ X} \Rightarrow \mathsf{Set\ X} \\
&\mathsf{domain}_\perp\ \mathsf{f\ A} \ :=\ \mathsf{preimage}\ \mathsf{f}|_{\mathsf{A}}\ ((\mathsf{image\ f\ A})\backslash\{\perp\})
\end{aligned} \tag{19}
$$

$$
\begin{aligned}
&\mathsf{lift_{map}} : (\mathsf{X} \rightsquigarrow_\perp \mathsf{Y}) \Rightarrow (\mathsf{X} \underset{\mathsf{map}}{\rightsquigarrow} \mathsf{Y}) \\
&\mathsf{lift_{map}}\ \mathsf{f\ A} \ :=\ \mathsf{let}\ \ \mathsf{A}' := \mathsf{domain}_\perp\ \mathsf{f\ A} \\
&\qquad\qquad\qquad \mathsf{in}\ \ \mathsf{f}|_{\mathsf{A}'}
\end{aligned} \tag{20}
$$

The clearest way to ensure that mapping arrow computations mean what we think they mean is to derive each combinator in a way that makes $\mathsf{lift_{map}}$ distribute over bottom arrow computations; i.e. it must be an arrow homomorphism (Definition 3.1.2). If $\mathsf{lift_{map}}$ is a homomorphism, then $[\![e]\!]_{\mathsf{map}} \equiv \mathsf{lift_{map}}\ [\![e]\!]_\perp$ for any let-calculus expression e, because $\mathsf{lift_{map}}$ distributes through its expansion.

To meet the homomorphism laws, we need equivalence to be more extensional for mapping computations.

Definition 4.1.1 (mapping arrow equivalence)**.** *Two mapping arrow computations $\mathsf{g}_1 : \mathsf{X} \underset{\mathsf{map}}{\rightsquigarrow} \mathsf{Y}$ and $\mathsf{g}_2 : \mathsf{X} \underset{\mathsf{map}}{\rightsquigarrow} \mathsf{Y}$ are equivalent, or $\mathsf{g}_1 \equiv \mathsf{g}_2$, when $\mathsf{g}_1\ \mathsf{A} \equiv \mathsf{g}_2\ \mathsf{A}$ for all $\mathsf{A} \subseteq \mathsf{X}$.*

Clearly $\mathsf{arr_b} := \mathsf{lift_b} \circ \mathsf{arr_a}$ meets the first homomorphism identity (13), so we define $\mathsf{arr_{map}}$ as a composition. The following subsections derive $(\&\&\&_{\mathsf{map}})$, $(\ggg_{\mathsf{map}})$, $\mathsf{ifte_{map}}$ and $\mathsf{lazy_{map}}$ from their corresponding bottom arrow combinators, in a way that ensures $\mathsf{lift_{map}}$ is an arrow homomorphism. Figure 4 contains the resulting definitions.

4.2 Case: Pairing

Starting with the left side of (15), we first expand definitions. For any $\mathsf{f}_1 : \mathsf{X} \rightsquigarrow_\perp \mathsf{Y}$, $\mathsf{f}_2 : \mathsf{X} \rightsquigarrow_\perp \mathsf{Z}$, and $\mathsf{A} \subseteq \mathsf{X}$,

$$
\begin{aligned}
&\mathsf{lift_{map}}\ (\mathsf{f}_1\ \&\&\&_\perp\ \mathsf{f}_2)\ \mathsf{A} \\
&\quad \equiv\ \mathsf{lift_{map}}\ (\lambda \mathsf{x}.\,\mathsf{if}\ (\mathsf{f}_1\ \mathsf{x} = \perp\ \mathsf{or}\ \mathsf{f}_2\ \mathsf{x} = \perp)\ \perp\ \langle \mathsf{f}_1\ \mathsf{x}, \mathsf{f}_2\ \mathsf{x}\rangle)\ \mathsf{A} \\
&\quad \equiv\ \mathsf{let}\quad \mathsf{f} := \lambda \mathsf{x}.\,\mathsf{if}\ (\mathsf{f}_1\ \mathsf{x} = \perp\ \mathsf{or}\ \mathsf{f}_2\ \mathsf{x} = \perp)\ \perp\ \langle \mathsf{f}_1\ \mathsf{x}, \mathsf{f}_2\ \mathsf{x}\rangle \\
&\qquad\qquad \mathsf{A}' := \mathsf{domain}_\perp\ \mathsf{f\ A} \\
&\qquad\quad \mathsf{in}\ \ \mathsf{f}|_{\mathsf{A}'}
\end{aligned} \tag{21}
$$

Next, we replace the definition of A' with one that does not depend on f, and rewrite in terms of $\mathsf{lift_{map}}\ \mathsf{f}_1$ and $\mathsf{lift_{map}}\ \mathsf{f}_2$:

$$
\begin{aligned}
&\mathsf{lift_{map}}\ (\mathsf{f}_1\ \&\&\&_\perp\ \mathsf{f}_2)\ \mathsf{A} \\
&\quad \equiv\ \mathsf{let}\ \ \mathsf{A}_1 := (\mathsf{domain}_\perp\ \mathsf{f}_1\ \mathsf{A}) \\
&\qquad\qquad \mathsf{A}_2 := (\mathsf{domain}_\perp\ \mathsf{f}_2\ \mathsf{A}) \\
&\qquad\qquad \mathsf{A}' := \mathsf{A}_1 \cap \mathsf{A}_2 \\
&\qquad\quad \mathsf{in}\ \ \lambda \mathsf{x} \in \mathsf{A}'.\,\langle \mathsf{f}_1\ \mathsf{x}, \mathsf{f}_2\ \mathsf{x}\rangle \\
&\quad \equiv\ \mathsf{let}\ \ \mathsf{g}_1 := \mathsf{lift_{map}}\ \mathsf{f}_1\ \mathsf{A} \\
&\qquad\qquad \mathsf{g}_2 := \mathsf{lift_{map}}\ \mathsf{f}_2\ \mathsf{A} \\
&\qquad\qquad \mathsf{A}' := (\mathsf{domain\ g}_1) \cap (\mathsf{domain\ g}_2) \\
&\qquad\quad \mathsf{in}\ \ \lambda \mathsf{x} \in \mathsf{A}'.\,\langle \mathsf{g}_1\ \mathsf{x}, \mathsf{g}_2\ \mathsf{x}\rangle \\
&\quad \equiv\ \langle \mathsf{lift_{map}}\ \mathsf{f}_1\ \mathsf{A}, \mathsf{lift_{map}}\ \mathsf{f}_2\ \mathsf{A}\rangle_{\mathsf{map}}
\end{aligned} \tag{22}
$$

Substituting g_1 for $\mathsf{lift_{map}}\ \mathsf{f}_1$ and g_2 for $\mathsf{lift_{map}}\ \mathsf{f}_2$ gives a definition for $(\&\&\&_{\mathsf{map}})$ (Figure 4) for which (15) holds.

4.3 Case: Composition

The derivation of $(\ggg_{\mathsf{map}})$ is similar to that of $(\&\&\&_{\mathsf{map}})$ but a little more involved.

XXX: include it?

4.4 Case: Conditional

Starting with the left side of (16), we expand definitions, and simplify f by restricting it to a domain for which $\mathsf{f}_1\ \mathsf{x}$

$$x \rightsquigarrow_\perp y \ ::= \ x \Rightarrow y_\perp$$

$$\begin{aligned}
&\mathrm{arr}_\perp : (x \Rightarrow y) \Rightarrow (x \rightsquigarrow_\perp y)\\
&\mathrm{arr}_\perp\ f \ := \ f
\end{aligned}$$

$$\begin{aligned}
&(\ggg_\perp) : (x \rightsquigarrow_\perp y) \Rightarrow (y \rightsquigarrow_\perp z) \Rightarrow (x \rightsquigarrow_\perp z)\\
&(f_1 \ggg_\perp f_2)\ x \ := \ \mathrm{if}\ (f_1\ x = \perp)\ \perp\ (f_2\ (f_1\ x))
\end{aligned}$$

$$\begin{aligned}
&(\&\&\&_\perp) : (x \rightsquigarrow_\perp y_1) \Rightarrow (x \rightsquigarrow_\perp y_2) \Rightarrow (x \rightsquigarrow_\perp \langle y_1, y_2\rangle)\\
&(f_1 \ \&\&\&_\perp\ f_2)\ x \ := \ \mathrm{if}\ (f_1\ x = \perp\ \mathrm{or}\ f_2\ x = \perp)\ \perp\ \langle f_1\ x, f_2\ x\rangle
\end{aligned}$$

$$\begin{aligned}
&\mathrm{ifte}_\perp : (x \rightsquigarrow_\perp \mathrm{Bool}) \Rightarrow (x \rightsquigarrow_\perp y) \Rightarrow (x \rightsquigarrow_\perp y) \Rightarrow (x \rightsquigarrow_\perp y)\\
&\mathrm{ifte}_\perp\ f_1\ f_2\ f_3\ x \ := \ \mathrm{case}\ \ f_1\ x\\
&\qquad\qquad\qquad\qquad \mathrm{true} \ \Longrightarrow\ f_2\ x\\
&\qquad\qquad\qquad\qquad \mathrm{false} \ \Longrightarrow\ f_3\ x\\
&\qquad\qquad\qquad\qquad \mathrm{else} \ \Longrightarrow\ \perp
\end{aligned}$$

$$\begin{aligned}
&\mathrm{lazy}_\perp : (1 \Rightarrow (x \rightsquigarrow_\perp y)) \Rightarrow (x \rightsquigarrow_\perp y)\\
&\mathrm{lazy}_\perp\ f\ x \ := \ f\ 0\ x
\end{aligned}$$

Figure 3: Bottom arrow definitions.

$$X \underset{\mathrm{map}}{\rightsquigarrow} Y \ ::= \ \mathrm{Set}\ X \Rightarrow (X \rightharpoonup Y)$$

$$\begin{aligned}
&\mathrm{arr}_{\mathrm{map}} : (X \Rightarrow Y) \Rightarrow (X \underset{\mathrm{map}}{\rightsquigarrow} Y)\\
&\mathrm{arr}_{\mathrm{map}} \ := \ \mathrm{lift}_{\mathrm{map}} \circ \mathrm{arr}_\perp
\end{aligned}$$

$$\begin{aligned}
&(\ggg_{\mathrm{map}}) : (X \underset{\mathrm{map}}{\rightsquigarrow} Y) \Rightarrow (Y \underset{\mathrm{map}}{\rightsquigarrow} Z) \Rightarrow (X \underset{\mathrm{map}}{\rightsquigarrow} Z)\\
&(g_1 \ggg_{\mathrm{map}} g_2)\ A \ := \ \mathrm{let}\ \ g_1' := g_1\ A\\
&\qquad\qquad\qquad\qquad\quad\ \ g_2' := g_2\ (\mathrm{range}\ g_1')\\
&\qquad\qquad\qquad\qquad \mathrm{in}\ \ g_2' \circ_{\mathrm{map}} g_1'
\end{aligned}$$

$$\begin{aligned}
&(\&\&\&_{\mathrm{map}}) : (X \underset{\mathrm{map}}{\rightsquigarrow} Y_1) \Rightarrow (X \underset{\mathrm{map}}{\rightsquigarrow} Y_2) \Rightarrow (X \underset{\mathrm{map}}{\rightsquigarrow} \langle Y_1, Y_2\rangle)\\
&(g_1 \ \&\&\&_{\mathrm{map}}\ g_2)\ A \ := \ \langle g_1\ A, g_2\ A\rangle_{\mathrm{map}}
\end{aligned}$$

$$\begin{aligned}
&\mathrm{ifte}_{\mathrm{map}} : (X \underset{\mathrm{map}}{\rightsquigarrow} \mathrm{Bool}) \Rightarrow (X \underset{\mathrm{map}}{\rightsquigarrow} Y) \Rightarrow (X \underset{\mathrm{map}}{\rightsquigarrow} Y) \Rightarrow (X \underset{\mathrm{map}}{\rightsquigarrow} Y)\\
&\mathrm{ifte}_{\mathrm{map}}\ g_1\ g_2\ g_3\ A \ := \ \mathrm{let}\ \ g_1' := g_1\ A\\
&\qquad\qquad\qquad\qquad\qquad\quad g_2' := g_2\ (\mathrm{preimage}\ g_1'\ \{\mathrm{true}\})\\
&\qquad\qquad\qquad\qquad\qquad\quad g_3' := g_3\ (\mathrm{preimage}\ g_1'\ \{\mathrm{false}\})\\
&\qquad\qquad\qquad\qquad\quad \mathrm{in}\ \ g_2' \uplus_{\mathrm{map}} g_3'
\end{aligned}$$

$$\begin{aligned}
&\mathrm{lazy}_{\mathrm{map}} : (1 \Rightarrow (X \underset{\mathrm{map}}{\rightsquigarrow} Y)) \Rightarrow (X \underset{\mathrm{map}}{\rightsquigarrow} Y)\\
&\mathrm{lazy}_{\mathrm{map}}\ g\ A \ := \ \mathrm{if}\ (A = \varnothing)\ \varnothing\ (g\ 0\ A)
\end{aligned}$$

$$\begin{aligned}
&\mathrm{lift}_{\mathrm{map}} : (X \rightsquigarrow_\perp Y) \Rightarrow (X \underset{\mathrm{map}}{\rightsquigarrow} Y)\\
&\mathrm{lift}_{\mathrm{map}}\ f\ A \ := \ \{\langle x, y\rangle \in f|_A \mid y \neq \perp\}
\end{aligned}$$

Figure 4: Mapping arrow definitions.

cannot be $\perp$:

$$\begin{aligned}
&\mathrm{lift}_{\mathrm{map}}\ (\mathrm{ifte}_\perp\ f_1\ f_2\ f_3)\ A\\
&\quad \equiv\ \mathrm{let}\ \ \ f := \lambda x.\,\mathrm{case}\ \ f_1\ x\\
&\qquad\qquad\qquad\qquad \mathrm{true} \ \Longrightarrow\ f_2\ x\\
&\qquad\qquad\qquad\qquad \mathrm{false} \ \Longrightarrow\ f_3\ x\\
&\qquad\qquad\qquad\qquad \mathrm{else} \ \Longrightarrow\ \perp\\
&\qquad\qquad A' := \mathrm{domain}_\perp\ f\ A\\
&\qquad\quad \mathrm{in}\ \ f|_{A'}\\
&\quad \equiv\ \mathrm{let}\ \ A_2 := \mathrm{preimage}\ f_1|_A\ \{\mathrm{true}\}\\
&\qquad\qquad A_3 := \mathrm{preimage}\ f_1|_A\ \{\mathrm{false}\}\\
&\qquad\qquad\ \ f := \lambda x.\,\mathrm{if}\ (f_1\ x)\ (f_2\ x)\ (f_3\ x)\\
&\qquad\qquad A' := \mathrm{domain}_\perp\ f\ (A_2 \uplus A_3)\\
&\qquad\quad \mathrm{in}\ \ f|_{A'}
\end{aligned} \tag{23}$$

We finish by converting bottom arrow computations to the mapping arrow and rewriting in terms of $(\uplus_{\mathrm{map}})$:

$$\begin{aligned}
&\mathrm{lift}_{\mathrm{map}}\ (\mathrm{ifte}_\perp\ f_1\ f_2\ f_3)\ A\\
&\quad \equiv\ \mathrm{let}\ \ g_1 := \mathrm{lift}_{\mathrm{map}}\ f_1\ A\\
&\qquad\qquad g_2 := \mathrm{lift}_{\mathrm{map}}\ f_2\ (\mathrm{preimage}\ g_1\ \{\mathrm{true}\})\\
&\qquad\qquad g_3 := \mathrm{lift}_{\mathrm{map}}\ f_3\ (\mathrm{preimage}\ g_1\ \{\mathrm{false}\})\\
&\qquad\qquad A' := (\mathrm{domain}\ g_2) \uplus (\mathrm{domain}\ g_3)\\
&\qquad\quad \mathrm{in}\ \ \lambda x \in A'.\,\mathrm{if}\ (x \in \mathrm{domain}\ g_2)\ (g_2\ x)\ (g_3\ x)\\
&\quad \equiv\ \mathrm{let}\ \ g_1 := \mathrm{lift}_{\mathrm{map}}\ f_1\ A\\
&\qquad\qquad g_2 := \mathrm{lift}_{\mathrm{map}}\ f_2\ (\mathrm{preimage}\ g_1\ \{\mathrm{true}\})\\
&\qquad\qquad g_3 := \mathrm{lift}_{\mathrm{map}}\ f_3\ (\mathrm{preimage}\ g_1\ \{\mathrm{false}\})\\
&\qquad\quad \mathrm{in}\ \ g_2 \uplus_{\mathrm{map}} g_3
\end{aligned} \tag{24}$$

Substituting g_1 for $\mathrm{lift}_{\mathrm{map}}\ f_1$, g_2 for $\mathrm{lift}_{\mathrm{map}}\ f_2$, and g_3 for $\mathrm{lift}_{\mathrm{map}}\ f_3$ gives a definition for $\mathrm{ifte}_{\mathrm{map}}$ (Figure 4) for which (16) holds.

4.5 Case: Laziness

Starting with the left side of (17), we first expand definitions:

$$\begin{aligned}
&\mathrm{lift}_{\mathrm{map}}\ (\mathrm{lazy}_\perp\ f)\ A\\
&\quad \equiv\ \mathrm{let}\ \ A' := \mathrm{domain}_\perp\ (\lambda x.\,f\ 0\ x)\ A\\
&\qquad\quad \mathrm{in}\ \ (\lambda x.\,f\ 0\ x)|_{A'}
\end{aligned}$$

λ_{ZFC} does not have an η rule (i.e. $\lambda x.\,e\ x \not\equiv e$ because e may diverge), but we can use weaker facts. If $A \neq \varnothing$, then $\mathrm{domain}_\perp\ (\lambda x.\,f\ 0\ x)\ A \equiv \mathrm{domain}_\perp\ (f\ 0)\ A$. Further, it diverges iff $f\ 0$ diverges, which diverges iff $(f\ 0)|_{A'}$ diverges. Therefore, if $A \neq \varnothing$, we can replace $\lambda x.\,f\ 0\ x$ with $f\ 0$. If $A = \varnothing$, then $\mathrm{lift}_{\mathrm{map}}\ (\mathrm{lazy}_\perp\ f)\ A = \varnothing$ (the empty mapping), so

$$\begin{aligned}
&\mathrm{lift}_{\mathrm{map}}\ (\mathrm{lazy}_\perp\ f)\ A\\
&\quad \equiv\ \mathrm{if}\ (A = \varnothing)\ \varnothing\ \mathrm{let}\ \ A' := \mathrm{domain}_\perp\ (f\ 0)\ A\\
&\qquad\qquad\qquad\qquad\quad \mathrm{in}\ \ (f\ 0)|_{A'}\\
&\quad \equiv\ \mathrm{if}\ (A = \varnothing)\ \varnothing\ (\mathrm{lift}_{\mathrm{map}}\ (f\ 0)\ A)
\end{aligned}$$

Substituting $g\ 0$ for $\mathrm{lift}_{\mathrm{map}}\ (f\ 0)$ gives a definition for $\mathrm{lazy}_{\mathrm{map}}$ (Figure 4) for which (17) holds.

4.6 Correctness

Theorem 4.6.1 (mapping arrow correctness)**.** $\mathrm{lift}_{\mathrm{map}}$ *is an arrow homomorphism.*

Proof. By construction. □

Corollary 4.6.2 (semantic correctness). *If* $[\![e]\!]_\perp : \mathsf{X} \rightsquigarrow_\perp \mathsf{Y}$, *then* $\mathsf{lift_{map}}\ [\![e]\!]_\perp \equiv [\![e]\!]_{\mathsf{map}}$ *and* $[\![e]\!]_{\mathsf{map}} : \mathsf{X} \underset{\mathsf{map}}{\rightsquigarrow} \mathsf{Y}$.

5. Lazy Preimage Mappings

On a computer, we will not often have the luxury of testing each function input to see whether it belongs to a preimage set. Even for finite domains, doing so is often intractable.

If we wish to compute with infinite sets in the language implementation, we will need an abstraction that makes it easy to replace computation on points with computation on sets. Therefore, in the preimage arrow, we will confine computation on points to ***lazy preimage mappings***, or just *preimage mappings*. Further on, we will need their ranges to be observable, so we define their type as

$$\mathsf{X} \underset{\mathsf{pre}}{\rightharpoonup} \mathsf{Y} \ ::= \ \langle \mathsf{Set\ Y}, \mathsf{Set\ Y} \Rightarrow \mathsf{Set\ X} \rangle \tag{25}$$

Converting a mapping to a lazy preimage mapping:

$$\begin{aligned} &\mathsf{pre} : (\mathsf{X} \rightharpoonup \mathsf{Y}) \Rightarrow (\mathsf{X} \underset{\mathsf{pre}}{\rightharpoonup} \mathsf{Y}) \\ &\mathsf{pre\ g} \ := \ \mathsf{let}\ \ \mathsf{Y}' := \mathsf{range\ g} \\ &\qquad\qquad\qquad\quad \mathsf{p} := \lambda \mathsf{B}.\, \mathsf{preimage\ g\ B} \\ &\qquad\qquad\quad \mathsf{in}\ \ \langle \mathsf{Y}', \mathsf{p} \rangle \end{aligned} \tag{26}$$

Applying a preimage mapping to any subset of its codomain:

$$\begin{aligned} &\mathsf{pre\text{-}ap} : (\mathsf{X} \underset{\mathsf{pre}}{\rightharpoonup} \mathsf{Y}) \Rightarrow \mathsf{Set\ Y} \Rightarrow \mathsf{Set\ X} \\ &\mathsf{pre\text{-}ap}\ \langle \mathsf{Y}', \mathsf{p} \rangle\ \mathsf{B} \ := \ \mathsf{p}\ (\mathsf{B} \cap \mathsf{Y}') \end{aligned} \tag{27}$$

The necessary property here is that using pre-ap to compute preimages is the same as computing them from a mapping using preimage.

Lemma 5.0.3. *Let* $\mathsf{g} \in \mathsf{X} \rightharpoonup \mathsf{Y}$. *For all* $\mathsf{B} \subseteq \mathsf{Y}$ *and* Y' *such that* $\mathsf{range\ g} \subseteq \mathsf{Y}' \subseteq \mathsf{Y}$, $\mathsf{preimage\ g}\ (\mathsf{B} \cap \mathsf{Y}') = \mathsf{preimage\ g\ B}$.

Theorem 5.0.4 (pre-ap computes preimages). *Let* $\mathsf{g} \in \mathsf{X} \rightharpoonup \mathsf{Y}$. *For all* $\mathsf{B} \subseteq \mathsf{Y}$, $\mathsf{pre\text{-}ap}\ (\mathsf{pre\ g})\ \mathsf{B} = \mathsf{preimage\ g\ B}$.

Proof. Expand definitions and apply Lemma 5.0.3 with $\mathsf{Y}' = \mathsf{range\ g}$. □

Figure 5 defines more operations on preimage mappings, including pairing, composition, and disjoint union operations corresponding to the mapping operations in Figure 1. Roughly, the correspondence is that pre distributes over mapping operations to yield preimage mapping operations. The precise correspondence is the subject of the next three theorems, which will be used to derive the preimage arrow from the mapping arrow.

First, we need a new notion of equivalence.

Definition 5.0.5. *Two preimage mappings* $\mathsf{h_1} : \mathsf{X} \underset{\mathsf{pre}}{\rightharpoonup} \mathsf{Y}$ *and* $\mathsf{h_2} : \mathsf{X} \underset{\mathsf{pre}}{\rightharpoonup} \mathsf{Y}$ *are equivalent, or* $\mathsf{h_1} \equiv \mathsf{h_2}$, *when* $\mathsf{pre\text{-}ap\ h_1\ B} = \mathsf{pre\text{-}ap\ h_2\ B}$ *for all* $\mathsf{B} \subseteq \mathsf{Y}$.

XXX: define equivalence in terms of equivalence, check observational equivalence in the proofs (specifically divergence)

5.1 Preimage Mapping Pairing

XXX: moar wurds in this section

Lemma 5.1.1 (preimage distributes over $\langle\cdot,\cdot\rangle_{\mathsf{map}}$ and $(\times)$). *Let* $\mathsf{g_1} \in \mathsf{X} \rightharpoonup \mathsf{Y_1}$ *and* $\mathsf{g_2} \in \mathsf{X} \rightharpoonup \mathsf{Y_2}$. *For all* $\mathsf{B_1} \subseteq \mathsf{Y_1}$ *and* $\mathsf{B_2} \subseteq \mathsf{Y_2}$, $\mathsf{preimage}\ \langle \mathsf{g_1}, \mathsf{g_2} \rangle_{\mathsf{map}}\ (\mathsf{B_1} \times \mathsf{B_2}) = (\mathsf{preimage\ g_1\ B_1}) \cap (\mathsf{preimage\ g_2\ B_2})$.

Theorem 5.1.2 (pre distributes over $\langle\cdot,\cdot\rangle_{\mathsf{map}}$). *Let* $\mathsf{g_1} \in \mathsf{X} \rightharpoonup \mathsf{Y_1}$ *and* $\mathsf{g_2} \in \mathsf{X} \rightharpoonup \mathsf{Y_2}$. *Then* $\mathsf{pre}\ \langle \mathsf{g_1}, \mathsf{g_2} \rangle_{\mathsf{map}} \equiv \langle \mathsf{pre\ g_1}, \mathsf{pre\ g_2} \rangle_{\mathsf{pre}}$.

Proof. Let $\langle \mathsf{Y}_1', \mathsf{p_1} \rangle := \mathsf{pre\ g_1}$ and $\langle \mathsf{Y}_2', \mathsf{p_2} \rangle := \mathsf{pre\ g_2}$. Starting from the right side, for all $\mathsf{B} \in \mathsf{Y_1} \times \mathsf{Y_2}$,

$$\begin{aligned} &\mathsf{pre\text{-}ap}\ \langle \mathsf{pre\ g_1}, \mathsf{pre\ g_2} \rangle_{\mathsf{pre}}\ \mathsf{B} \\ &\quad = \ \mathsf{let}\ \ \mathsf{Y}' := \mathsf{Y}_1' \times \mathsf{Y}_2' \\ &\qquad\qquad\quad \mathsf{p} := \lambda \mathsf{B}.\ \bigcup_{\langle \mathsf{y_1}, \mathsf{y_2} \rangle \in \mathsf{B}} (\mathsf{p_1}\ \{\mathsf{y_1}\}) \cap (\mathsf{p_2}\ \{\mathsf{y_2}\}) \\ &\qquad\quad\ \ \mathsf{in}\ \ \mathsf{p}\ (\mathsf{B} \cap \mathsf{Y}') \\ &\quad = \bigcup_{\langle \mathsf{y_1}, \mathsf{y_2} \rangle \in \mathsf{B} \cap (\mathsf{Y}_1' \times \mathsf{Y}_2')} (\mathsf{p_1}\ \{\mathsf{y_1}\}) \cap (\mathsf{p_2}\ \{\mathsf{y_2}\}) \\ &\quad = \bigcup_{\langle \mathsf{y_1}, \mathsf{y_2} \rangle \in \mathsf{B} \cap (\mathsf{Y}_1' \times \mathsf{Y}_2')} (\mathsf{preimage\ g_1}\ \{\mathsf{y_1}\}) \cap (\mathsf{preimage\ g_2}\ \{\mathsf{y_2}\}) \\ &\quad = \bigcup_{\mathsf{y} \in \mathsf{B} \cap (\mathsf{Y}_1' \times \mathsf{Y}_2')} (\mathsf{preimage}\ \langle \mathsf{g_1}, \mathsf{g_2} \rangle_{\mathsf{map}}\ \{\mathsf{y}\}) \\ &\quad = \ \mathsf{preimage}\ \langle \mathsf{g_1}, \mathsf{g_2} \rangle_{\mathsf{map}}\ (\mathsf{B} \cap (\mathsf{Y}_1' \times \mathsf{Y}_2')) \\ &\quad = \ \mathsf{preimage}\ \langle \mathsf{g_1}, \mathsf{g_2} \rangle_{\mathsf{map}}\ \mathsf{B} \\ &\quad = \ \mathsf{pre\text{-}ap}\ (\mathsf{pre}\ \langle \mathsf{g_1}, \mathsf{g_2} \rangle_{\mathsf{map}})\ \mathsf{B} \end{aligned}$$

□

5.2 Preimage Mapping Composition

XXX: moar wurds in this section

Lemma 5.2.1 (preimage distributes over $(\circ_{\mathsf{map}})$). *Let* $\mathsf{g_1} \in \mathsf{X} \rightharpoonup \mathsf{Y}$ *and* $\mathsf{g_2} \in \mathsf{Y} \rightharpoonup \mathsf{Z}$. *For all* $\mathsf{C} \subseteq \mathsf{Z}$, $\mathsf{preimage}\ (\mathsf{g_2} \circ_{\mathsf{map}} \mathsf{g_1})\ \mathsf{C} = \mathsf{preimage\ g_1}\ (\mathsf{preimage\ g_2\ C})$.

Theorem 5.2.2 (pre distributes over $(\circ_{\mathsf{map}})$). *Let* $\mathsf{g_1} \in \mathsf{X} \rightharpoonup \mathsf{Y}$ *and* $\mathsf{g_2} \in \mathsf{Y} \rightharpoonup \mathsf{Z}$. *Then* $\mathsf{pre}\ (\mathsf{g_2} \circ_{\mathsf{map}} \mathsf{g_1}) \equiv (\mathsf{pre\ g_2}) \circ_{\mathsf{pre}} (\mathsf{pre\ g_1})$.

Proof. Let $\langle \mathsf{Z}', \mathsf{p_2} \rangle := \mathsf{pre\ g_2}$. Starting from the right side, for all $\mathsf{C} \subseteq \mathsf{Z}$,

$$\begin{aligned} &\mathsf{pre\text{-}ap}\ ((\mathsf{pre\ g_2}) \circ_{\mathsf{pre}} (\mathsf{pre\ g_1}))\ \mathsf{C} \\ &\quad = \ \mathsf{let}\ \ \mathsf{h} := \lambda \mathsf{C}.\, \mathsf{pre\text{-}ap}\ (\mathsf{pre\ g_1})\ (\mathsf{p_2\ C}) \\ &\qquad\quad\ \mathsf{in}\ \ \mathsf{h}\ (\mathsf{C} \cap \mathsf{Z}') \\ &\quad = \ \mathsf{pre\text{-}ap}\ (\mathsf{pre\ g_1})\ (\mathsf{p_2}\ (\mathsf{C} \cap \mathsf{Z}')) \\ &\quad = \ \mathsf{pre\text{-}ap}\ (\mathsf{pre\ g_1})\ (\mathsf{pre\text{-}ap}\ (\mathsf{pre\ g_2})\ \mathsf{C}) \\ &\quad = \ \mathsf{preimage\ g_1}\ (\mathsf{preimage\ g_2\ C}) \\ &\quad = \ \mathsf{preimage}\ (\mathsf{g_2} \circ_{\mathsf{map}} \mathsf{g_1})\ \mathsf{C} \\ &\quad = \ \mathsf{pre\text{-}ap}\ (\mathsf{pre}\ (\mathsf{g_2} \circ_{\mathsf{map}} \mathsf{g_1}))\ \mathsf{C} \end{aligned}$$

□

5.3 Preimage Mapping Disjoint Union

XXX: moar wurds in this section

Lemma 5.3.1 (preimage distributes over $(\uplus_{\mathsf{map}})$). *Let* $\mathsf{g_1} \in \mathsf{X} \rightharpoonup \mathsf{Y}$ *and* $\mathsf{g_2} \in \mathsf{X} \rightharpoonup \mathsf{Y}$ *be disjoint mappings. For all* $\mathsf{B} \subseteq \mathsf{Y}$, $\mathsf{preimage}\ (\mathsf{g_1} \uplus_{\mathsf{map}} \mathsf{g_2})\ \mathsf{B} = (\mathsf{preimage\ g_1\ B}) \uplus (\mathsf{preimage\ g_2\ B})$.

Theorem 5.3.2 (pre distributes over $(\uplus_{\mathsf{map}})$). *Let* $\mathsf{g_1} \in \mathsf{X} \rightharpoonup \mathsf{Y}$ *and* $\mathsf{g_2} \in \mathsf{X} \rightharpoonup \mathsf{Y}$ *have disjoint domains. Then* $\mathsf{pre}\ (\mathsf{g_1} \uplus_{\mathsf{map}} \mathsf{g_2}) \equiv (\mathsf{pre\ g_1}) \uplus_{\mathsf{pre}} (\mathsf{pre\ g_2})$.

$$\mathsf{X} \underset{\mathsf{pre}}{\rightharpoonup} \mathsf{Y} ::= \langle \mathsf{Set\ Y}, \mathsf{Set\ Y} \Rightarrow \mathsf{Set\ X} \rangle$$

$$\begin{aligned}&\mathsf{pre} : (\mathsf{X} \underset{\mathsf{map}}{\rightsquigarrow} \mathsf{Y}) \Rightarrow (\mathsf{X} \underset{\mathsf{pre}}{\rightharpoonup} \mathsf{Y})\\ &\mathsf{pre\ g} \ :=\ \langle \mathsf{range\ g}, \lambda \mathsf{B}.\, \mathsf{preimage\ g\ B} \rangle\end{aligned}$$

$$\begin{aligned}&\mathsf{pre\text{-}ap} : (\mathsf{X} \underset{\mathsf{pre}}{\rightharpoonup} \mathsf{Y}) \Rightarrow \mathsf{Set\ Y} \Rightarrow \mathsf{Set\ X}\\ &\mathsf{pre\text{-}ap}\ \langle \mathsf{Y}', \mathsf{p} \rangle\ \mathsf{B} \ :=\ \mathsf{p}\ (\mathsf{B} \cap \mathsf{Y}')\end{aligned}$$

$$\begin{aligned}&\mathsf{pre\text{-}range} : (\mathsf{X} \underset{\mathsf{pre}}{\rightharpoonup} \mathsf{Y}) \Rightarrow \mathsf{Set\ Y}\\ &\mathsf{pre\text{-}range} \ :=\ \mathsf{fst}\end{aligned}$$

$$\begin{aligned}&\langle \cdot, \cdot \rangle_{\mathsf{pre}} : (\mathsf{X} \underset{\mathsf{pre}}{\rightharpoonup} \mathsf{Y}_1) \Rightarrow (\mathsf{X} \underset{\mathsf{pre}}{\rightharpoonup} \mathsf{Y}_2) \Rightarrow (\mathsf{X} \underset{\mathsf{pre}}{\rightharpoonup} \mathsf{Y}_1 \times \mathsf{Y}_2)\\ &\langle \langle \mathsf{Y}_1', \mathsf{p}_1 \rangle, \langle \mathsf{Y}_2', \mathsf{p}_2 \rangle \rangle_{\mathsf{pre}} \ :=\ \mathsf{let}\ \ \mathsf{Y}' := \mathsf{Y}_1' \times \mathsf{Y}_2'\\ &\qquad\qquad \mathsf{p} := \lambda \mathsf{B}. \bigcup_{\langle \mathsf{y}_1, \mathsf{y}_2 \rangle \in \mathsf{B}} (\mathsf{p}_1\ \{\mathsf{y}_1\}) \cap (\mathsf{p}_2\ \{\mathsf{y}_2\})\\ &\qquad\quad \mathsf{in}\ \ \langle \mathsf{Y}', \mathsf{p} \rangle\end{aligned}$$

$$\begin{aligned}&(\circ_{\mathsf{pre}}) : (\mathsf{Y} \underset{\mathsf{pre}}{\rightharpoonup} \mathsf{Z}) \Rightarrow (\mathsf{X} \underset{\mathsf{pre}}{\rightharpoonup} \mathsf{Y}) \Rightarrow (\mathsf{X} \underset{\mathsf{pre}}{\rightharpoonup} \mathsf{Z})\\ &\langle \mathsf{Z}', \mathsf{p}_2 \rangle \circ_{\mathsf{pre}} \mathsf{h}_1 \ :=\ \langle \mathsf{Z}', \lambda \mathsf{C}.\, \mathsf{pre\text{-}ap}\ \mathsf{h}_1\ (\mathsf{p}_2\ \mathsf{C}) \rangle\end{aligned}$$

$$\begin{aligned}&(\uplus_{\mathsf{pre}}) : (\mathsf{X} \underset{\mathsf{pre}}{\rightharpoonup} \mathsf{Y}) \Rightarrow (\mathsf{X} \underset{\mathsf{pre}}{\rightharpoonup} \mathsf{Y}) \Rightarrow (\mathsf{X} \underset{\mathsf{pre}}{\rightharpoonup} \mathsf{Y})\\ &\mathsf{h}_1 \uplus_{\mathsf{pre}} \mathsf{h}_2 \ :=\ \mathsf{let}\ \ \mathsf{Y}' := (\mathsf{pre\text{-}range}\ \mathsf{h}_1) \cup (\mathsf{pre\text{-}range}\ \mathsf{h}_2)\\ &\qquad\qquad \mathsf{p} := \lambda \mathsf{B}.\, (\mathsf{pre\text{-}ap}\ \mathsf{h}_1\ \mathsf{B}) \uplus (\mathsf{pre\text{-}ap}\ \mathsf{h}_2\ \mathsf{B})\\ &\qquad\quad \mathsf{in}\ \ \langle \mathsf{Y}', \mathsf{p} \rangle\end{aligned}$$

Figure 5: Lazy preimage mappings and operations.

Proof. Let $\mathsf{Y}_1' := \mathsf{range\ g}_1$ and $\mathsf{Y}_2' := \mathsf{range\ g}_2$. Starting from the right side, for all $\mathsf{B} \subseteq \mathsf{Y}$,

$$\begin{aligned}&\mathsf{pre\text{-}ap}\ ((\mathsf{pre\ g}_1) \uplus_{\mathsf{pre}} (\mathsf{pre\ g}_2))\ \mathsf{B}\\ &\quad = \mathsf{let}\ \ \mathsf{Y}' := \mathsf{Y}_1' \cup \mathsf{Y}_2'\\ &\qquad\qquad \mathsf{h} := \lambda \mathsf{B}.\, (\mathsf{pre\text{-}ap}\ (\mathsf{pre\ g}_1)\ \mathsf{B}) \uplus (\mathsf{pre\text{-}ap}\ (\mathsf{pre\ g}_2)\ \mathsf{B})\\ &\qquad\ \ \mathsf{in}\ \ \mathsf{h}\ (\mathsf{B} \cap \mathsf{Y}')\\ &\quad = (\mathsf{pre\text{-}ap}\ (\mathsf{pre\ g}_1)\ (\mathsf{B} \cap (\mathsf{Y}_1' \cup \mathsf{Y}_2'))) \uplus\\ &\qquad (\mathsf{pre\text{-}ap}\ (\mathsf{pre\ g}_2)\ (\mathsf{B} \cap (\mathsf{Y}_1' \cup \mathsf{Y}_2')))\\ &\quad = (\mathsf{preimage\ g}_1\ (\mathsf{B} \cap (\mathsf{Y}_1' \cup \mathsf{Y}_2'))) \uplus\\ &\qquad (\mathsf{preimage\ g}_2\ (\mathsf{B} \cap (\mathsf{Y}_1' \cup \mathsf{Y}_2')))\\ &\quad = \mathsf{preimage}\ (\mathsf{g}_1 \uplus_{\mathsf{map}} \mathsf{g}_2)\ (\mathsf{B} \cap (\mathsf{Y}_1' \cup \mathsf{Y}_2'))\\ &\quad = \mathsf{preimage}\ (\mathsf{g}_1 \uplus_{\mathsf{map}} \mathsf{g}_2)\ \mathsf{B}\\ &\quad = \mathsf{pre\text{-}ap}\ (\mathsf{pre}\ (\mathsf{g}_1 \uplus_{\mathsf{map}} \mathsf{g}_2))\ \mathsf{B}\end{aligned}$$

□

6. Deriving the Preimage Arrow

XXX: intro

$$\mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Y} \ ::=\ \mathsf{Set\ X} \Rightarrow (\mathsf{X} \underset{\mathsf{pre}}{\rightharpoonup} \mathsf{Y}) \tag{28}$$

$$\begin{aligned}&\mathsf{lift}_{\mathsf{pre}} : (\mathsf{X} \underset{\mathsf{map}}{\rightsquigarrow} \mathsf{Y}) \Rightarrow (\mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Y})\\ &\mathsf{lift}_{\mathsf{pre}}\ \mathsf{g\ A} \ :=\ \mathsf{pre}\ (\mathsf{g\ A})\end{aligned} \tag{29}$$

Definition 6.0.3 (Preimage arrow equivalence)**.** *Two preimage arrow computations* $\mathsf{h}_1 : \mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Y}$ *and* $\mathsf{h}_2 : \mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Y}$ *are equivalent, or* $\mathsf{h}_1 \equiv \mathsf{h}_2$*, when* $\mathsf{h}_1\ \mathsf{A} \equiv \mathsf{h}_2\ \mathsf{A}$ *for all* $\mathsf{A} \subseteq \mathsf{X}$.

As with $\mathsf{arr}_{\mathsf{map}}$, defining $\mathsf{arr}_{\mathsf{pre}}$ as a composition meets (13). The following subsections derive $(\&\&\&_{\mathsf{pre}})$, $(\ggg_{\mathsf{pre}})$, $\mathsf{ifte}_{\mathsf{pre}}$ and $\mathsf{lazy}_{\mathsf{pre}}$ from their corresponding mapping arrow combinators, in a way that ensures $\mathsf{lift}_{\mathsf{pre}}$ is an arrow homomorphism from the mapping arrow to the preimage arrow. Figure 6 contains the resulting definitions.

6.1 Case: Pairing

Starting with the left side of (15), we expand definitions, apply Theorem 5.1.2, and rewrite in terms of $\mathsf{lift}_{\mathsf{pre}}$:

$$\begin{aligned}&\mathsf{pre\text{-}ap}\ (\mathsf{lift}_{\mathsf{pre}}\ (\mathsf{g}_1\ \&\&\&_{\mathsf{map}}\ \mathsf{g}_2)\ \mathsf{A})\ \mathsf{B}\\ &\quad \equiv\ \mathsf{pre\text{-}ap}\ (\mathsf{pre}\ \langle \mathsf{g}_1\ \mathsf{A}, \mathsf{g}_2\ \mathsf{A} \rangle_{\mathsf{map}})\ \mathsf{B}\\ &\quad \equiv\ \mathsf{pre\text{-}ap}\ \langle \mathsf{pre}\ (\mathsf{g}_1\ \mathsf{A}), \mathsf{pre}\ (\mathsf{g}_2\ \mathsf{A}) \rangle_{\mathsf{pre}}\ \mathsf{B}\\ &\quad \equiv\ \mathsf{pre\text{-}ap}\ \langle \mathsf{lift}_{\mathsf{pre}}\ \mathsf{g}_1\ \mathsf{A}, \mathsf{lift}_{\mathsf{pre}}\ \mathsf{g}_2\ \mathsf{A} \rangle_{\mathsf{pre}}\ \mathsf{B}\end{aligned}$$

Substituting h_1 for $\mathsf{lift}_{\mathsf{pre}}\ \mathsf{g}_1$ and h_2 for $\mathsf{lift}_{\mathsf{pre}}\ \mathsf{g}_2$, and removing the application of $\mathsf{pre\text{-}ap}$ from both sides of the equivalence gives a definition of $(\&\&\&_{\mathsf{pre}})$ (Figure 6) for which (15) holds.

6.2 Case: Composition

Starting with the left side of (14), we expand definitions, apply Theorem 5.2.2 and rewrite in terms of $\mathsf{lift}_{\mathsf{pre}}$:

$$\begin{aligned}&\mathsf{pre\text{-}ap}\ (\mathsf{lift}_{\mathsf{pre}}\ (\mathsf{g}_1 \ggg_{\mathsf{map}} \mathsf{g}_2)\ \mathsf{A})\ \mathsf{C}\\ &\quad \equiv\ \mathsf{let}\ \ \mathsf{g}_1' := \mathsf{g}_1\ \mathsf{A}\\ &\qquad\qquad \mathsf{g}_2' := \mathsf{g}_2\ (\mathsf{range\ g}_1')\\ &\qquad\quad \mathsf{in}\ \ \mathsf{pre\text{-}ap}\ (\mathsf{pre}\ (\mathsf{g}_2' \circ_{\mathsf{map}} \mathsf{g}_1'))\ \mathsf{C}\\ &\quad \equiv\ \mathsf{let}\ \ \mathsf{g}_1' := \mathsf{g}_1\ \mathsf{A}\\ &\qquad\qquad \mathsf{g}_2' := \mathsf{g}_2\ (\mathsf{range\ g}_1')\\ &\qquad\quad \mathsf{in}\ \ \mathsf{pre\text{-}ap}\ ((\mathsf{pre\ g}_1') \circ_{\mathsf{pre}} (\mathsf{pre\ g}_2'))\ \mathsf{C}\\ &\quad \equiv\ \mathsf{let}\ \ \mathsf{h}_1 := \mathsf{lift}_{\mathsf{pre}}\ \mathsf{g}_1\ \mathsf{A}\\ &\qquad\qquad \mathsf{h}_2 := \mathsf{lift}_{\mathsf{pre}}\ \mathsf{g}_2\ (\mathsf{pre\text{-}range}\ \mathsf{h}_1)\\ &\qquad\quad \mathsf{in}\ \ \mathsf{pre\text{-}ap}\ (\mathsf{h}_2 \circ_{\mathsf{pre}} \mathsf{h}_1)\ \mathsf{C}\end{aligned} \tag{30}$$

Substituting h_1 for $\mathsf{lift}_{\mathsf{pre}}\ \mathsf{g}_1$ and h_2 for $\mathsf{lift}_{\mathsf{pre}}\ \mathsf{g}_2$, and removing the application of $\mathsf{pre\text{-}ap}$ from both sides of the equivalence gives a definition of $(\ggg_{\mathsf{pre}})$ (Figure 6) for which (14) holds.

6.3 Case: Conditional

Starting with the left side of (16), we expand terms, apply Theorem 5.3.2, rewrite in terms of $\mathsf{lift}_{\mathsf{pre}}$, and apply Theo-

$$\mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Y} ::= \mathsf{Set\ X} \Rightarrow (\mathsf{X} \underset{\mathsf{pre}}{\rightharpoonup} \mathsf{Y})$$

$$\begin{aligned}
&\mathsf{arr_{pre}} : (\mathsf{X} \Rightarrow \mathsf{Y}) \Rightarrow (\mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Y}) \\
&\mathsf{arr_{pre}} \ := \ \mathsf{lift_{pre}} \circ \mathsf{arr_{map}}
\end{aligned}$$

$$\begin{aligned}
&(\mathbin{>\!\!>\!\!>_{\mathsf{pre}}}) : (\mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Y}) \Rightarrow (\mathsf{Y} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Z}) \Rightarrow (\mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Z}) \\
&(\mathsf{h_1} \mathbin{>\!\!>\!\!>_{\mathsf{pre}}} \mathsf{h_2})\ \mathsf{A} \ := \ \mathsf{let}\ \ \mathsf{h}'_1 := \mathsf{h_1\ A} \\
&\qquad\qquad\qquad\qquad\quad\ \ \mathsf{h}'_2 := \mathsf{h_2}\ (\mathsf{pre\text{-}range}\ \mathsf{h}'_1) \\
&\qquad\qquad\qquad\quad\ \ \mathsf{in}\ \ \mathsf{h}'_2 \circ_{\mathsf{pre}} \mathsf{h}'_1
\end{aligned}$$

$$\begin{aligned}
&(\&\&\&_{\mathsf{pre}}) : (\mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Y}) \Rightarrow (\mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Z}) \Rightarrow (\mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Y} \times \mathsf{Z}) \\
&(\mathsf{h_1} \ \&\&\&_{\mathsf{pre}}\ \mathsf{h_2})\ \mathsf{A} \ := \ \langle \mathsf{h_1\ A}, \mathsf{h_2\ A} \rangle_{\mathsf{pre}}
\end{aligned}$$

$$\begin{aligned}
&\mathsf{ifte_{pre}} : (\mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Bool}) \Rightarrow (\mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Y}) \Rightarrow (\mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Y}) \Rightarrow (\mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Y}) \\
&\mathsf{ifte_{pre}\ h_1\ h_2\ h_3\ A} \ := \ \mathsf{let}\ \ \mathsf{h}'_1 := \mathsf{h_1\ A} \\
&\qquad\qquad\qquad\qquad\qquad\ \ \mathsf{h}'_2 := \mathsf{h_2}\ (\mathsf{pre\text{-}ap}\ \mathsf{h}'_1\ \{\mathsf{true}\}) \\
&\qquad\qquad\qquad\qquad\qquad\ \ \mathsf{h}'_3 := \mathsf{h_3}\ (\mathsf{pre\text{-}ap}\ \mathsf{h}'_1\ \{\mathsf{false}\}) \\
&\qquad\qquad\qquad\qquad\ \ \mathsf{in}\ \ \mathsf{h}'_2 \uplus_{\mathsf{pre}} \mathsf{h}'_3
\end{aligned}$$

$$\begin{aligned}
&\mathsf{lazy_{pre}} : (1 \Rightarrow (\mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Y})) \Rightarrow (\mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Y}) \\
&\mathsf{lazy_{pre}\ h\ A} \ := \ \mathsf{if}\ (\mathsf{A} = \varnothing)\ (\mathsf{pre}\ \varnothing)\ (\mathsf{h\ 0\ A})
\end{aligned}$$

$$\begin{aligned}
&\mathsf{lift_{pre}} : (\mathsf{X} \underset{\mathsf{map}}{\rightsquigarrow} \mathsf{Y}) \Rightarrow (\mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Y}) \\
&\mathsf{lift_{pre}\ g\ A} \ := \ \mathsf{pre\ (g\ A)}
\end{aligned}$$

Figure 6: Preimage arrow definitions.

rem 5.0.4 in the definitions of $\mathsf{h_2}$ and $\mathsf{h_3}$:

$$\begin{aligned}
&\mathsf{pre\text{-}ap}\ (\mathsf{lift_{pre}}\ (\mathsf{ifte_{map}\ g_1\ g_2\ g_3})\ \mathsf{A})\ \mathsf{B} \\
&\quad \equiv \ \mathsf{let}\ \ \mathsf{g}'_1 := \mathsf{g_1\ A} \\
&\qquad\qquad\ \ \mathsf{g}'_2 := \mathsf{g_2}\ (\mathsf{preimage}\ \mathsf{g}'_1\ \{\mathsf{true}\}) \\
&\qquad\qquad\ \ \mathsf{g}'_3 := \mathsf{g_3}\ (\mathsf{preimage}\ \mathsf{g}'_1\ \{\mathsf{false}\}) \\
&\qquad\quad\ \mathsf{in}\ \ \mathsf{pre\text{-}ap}\ (\mathsf{pre}\ (\mathsf{g}'_2 \uplus_{\mathsf{map}} \mathsf{g}'_3))\ \mathsf{B} \\
&\quad \equiv \ \mathsf{let}\ \ \mathsf{g}'_1 := \mathsf{g_1\ A} \\
&\qquad\qquad\ \ \mathsf{g}'_2 := \mathsf{g_2}\ (\mathsf{preimage}\ \mathsf{g}'_1\ \{\mathsf{true}\}) \\
&\qquad\qquad\ \ \mathsf{g}'_3 := \mathsf{g_3}\ (\mathsf{preimage}\ \mathsf{g}'_1\ \{\mathsf{false}\}) \\
&\qquad\quad\ \mathsf{in}\ \ \mathsf{pre\text{-}ap}\ ((\mathsf{pre}\ \mathsf{g}'_2) \uplus_{\mathsf{pre}} (\mathsf{pre}\ \mathsf{g}'_3))\ \mathsf{B} \\
&\quad \equiv \ \mathsf{let}\ \ \mathsf{h_1} := \mathsf{lift_{pre}\ g_1\ A} \\
&\qquad\qquad\ \ \mathsf{h_2} := \mathsf{lift_{pre}\ g_2}\ (\mathsf{pre\text{-}ap\ h_1}\ \{\mathsf{true}\}) \\
&\qquad\qquad\ \ \mathsf{h_3} := \mathsf{lift_{pre}\ g_3}\ (\mathsf{pre\text{-}ap\ h_1}\ \{\mathsf{false}\}) \\
&\qquad\quad\ \mathsf{in}\ \ \mathsf{pre\text{-}ap}\ (\mathsf{h_2} \uplus_{\mathsf{pre}} \mathsf{h_3})\ \mathsf{B}
\end{aligned}$$

Substituting $\mathsf{h_1}$ for $\mathsf{lift_{pre}\ g_1}$, $\mathsf{h_2}$ for $\mathsf{lift_{pre}\ g_2}$ and $\mathsf{h_3}$ for $\mathsf{lift_{pre}\ g_3}$, and removing the application of $\mathsf{pre\text{-}ap}$ from both sides of the equivalence gives a definition of $\mathsf{ifte_{pre}}$ (Figure 6) for which (16) holds.

6.4 Case: Laziness

Starting with the left side of (17), expand definitions, distribute pre over the branches of if, and rewrite in terms of $\mathsf{lift_{pre}}\ (\mathsf{g}\ 0)$:

$$\begin{aligned}
&\mathsf{pre\text{-}ap}\ (\mathsf{lift_{pre}}\ (\mathsf{lazy_{map}\ g})\ \mathsf{A})\ \mathsf{B} \\
&\quad \equiv \ \mathsf{let}\ \ \mathsf{g}' := \mathsf{if}\ (\mathsf{A} = \varnothing)\ \varnothing\ (\mathsf{g\ 0\ A}) \\
&\qquad\quad\ \mathsf{in}\ \ \mathsf{pre\text{-}ap}\ (\mathsf{pre\ g}')\ \mathsf{B} \\
&\quad \equiv \ \mathsf{let}\ \ \mathsf{h} := \mathsf{if}\ (\mathsf{A} = \varnothing)\ (\mathsf{pre}\ \varnothing)\ (\mathsf{pre\ (g\ 0\ A)}) \\
&\qquad\quad\ \mathsf{in}\ \ \mathsf{pre\text{-}ap\ h\ B} \\
&\quad \equiv \ \mathsf{let}\ \ \mathsf{h} := \mathsf{if}\ (\mathsf{A} = \varnothing)\ (\mathsf{pre}\ \varnothing)\ (\mathsf{lift_{pre}\ (g\ 0)\ A}) \\
&\qquad\quad\ \mathsf{in}\ \ \mathsf{pre\text{-}ap\ h\ B}
\end{aligned}$$

Substituting $\mathsf{h\ 0}$ for $\mathsf{lift_{pre}\ (g\ 0)}$ and removing the application of $\mathsf{pre\text{-}ap}$ from both sides of the equivalence gives a definition for $\mathsf{lazy_{pre}}$ (Figure 6) for which (17) holds.

6.5 Correctness

Theorem 6.5.1 (preimage arrow correctness)**.** $\mathsf{lift_{pre}}$ *is an arrow homomorphism.*

Proof. By construction. □

Corollary 6.5.2 (semantic correctness)**.** *If* $[\![e]\!]_{\mathsf{map}} : \mathsf{X} \underset{\mathsf{map}}{\rightsquigarrow} \mathsf{Y}$, *then* $\mathsf{lift_{pre}}\ [\![e]\!]_{\mathsf{map}} \equiv [\![e]\!]_{\mathsf{pre}}$ *and* $[\![e]\!]_{\mathsf{pre}} : \mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Y}$.

In particular, $[\![e]\!]_{\mathsf{pre}}$ correctly computes preimages under the interpretation of e as a function from a random source.

7. Preimages Under Partial Functions

Probabilistic functions that may diverge, but converge with probability 1, are common. They come up not only when practitioners want to build data with random size or structure, but in simpler circumstances as well.

Suppose random retrieves a number $\mathsf{x_j} \in [0, 1]$ from a uniform random source x. The following recursive function, which defines the well-known **geometric distribution** with parameter p, counts the number of times $\mathsf{random} < \mathsf{p}$ is false:

$$\mathsf{geometric\ p} \ := \ \mathsf{if}\ (\mathsf{random} < \mathsf{p})\ 0\ (1 + \mathsf{geometric\ p}) \qquad (31)$$

For any $\mathsf{p} > 0$, $\mathsf{geometric\ p}$ may diverge, but the probability of always taking the false branch is $(1 - \mathsf{p}) \times (1 - \mathsf{p}) \times (1 - \mathsf{p}) \times \cdots = 0$. Divergence with probability 0 simply does not happen in practice.

Suppose we interpret (31) as $\mathsf{h} : \mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathbb{N}$, a preimage arrow computation from random sources in X to natural numbers, and that we have a probability measure $\mathsf{P} \in \mathcal{P}\ \mathsf{X} \rightharpoonup [0, 1]$. We could compute the probability of any output set $\mathsf{N} \subseteq \mathbb{N}$ using $\mathsf{P\ (h\ A\ N)}$, where $\mathsf{A} \subseteq \mathsf{X}$ and $\mathsf{P\ A} = 1$. We have three hurdles to overcome:

1. Ensuring $\mathsf{h\ A}$ converges.
2. Determining how random indexes numbers in x.
3. Ensuring each $\mathsf{x} \in \mathsf{X}$ contains enough random numbers.

Ensuring $\mathsf{h\ A}$ converges is the most difficult, but doing the other two will provide structure that makes it much easier.

7.1 Threading and Indexing

We clearly need a new arrow that threads a random source through its computations. To ensure it contains enough random numbers, the source should be infinite.

In a pure λ-calculus, random sources are typically infinite lists, threaded monadically: each computation receives and produces a random source. A new combinator is defined that removes the head of the random source and passes the tail along. This is likely preferred because pseudorandom number generators are almost universally monadic.

A little-used alternative is for the random source to be an infinite tree, threaded applicatively: each computation receives, but does not produce, a random source. Multiargument combinators split the tree and pass sub-trees to sub-computations.

We have tried both ways with arrows defined using pairing. The resulting definitions are large, making them conceptually difficult and hard to manipulate. Fortunately, assigning each sub-computation a unique index into a tree-shaped random source, and passing it unchanged, is relatively easy.

We need a way to assign unique indexes to expressions.

Definition 7.1.1 (binary indexing scheme). *Let* J *be an index set,* $\mathsf{j}_0 \in \mathsf{J}$ *a distinguished element, and* $\mathsf{left} : \mathsf{J} \Rightarrow \mathsf{J}$ *and* $\mathsf{right} : \mathsf{J} \Rightarrow \mathsf{J}$ *be total functions. If for every finite composition* next *of* left *and* right*,* $\mathsf{next}\ \mathsf{j}_0$ *is unique, then* J*,* j_0*,* left *and* right *define a **binary indexing scheme**.*

For example, let J be the set of lists of booleans, j_0 the empty list, and define

$$\begin{aligned} \mathsf{left}\ \mathsf{xs} &:= \langle \mathsf{true}, \mathsf{xs} \rangle \\ \mathsf{right}\ \mathsf{xs} &:= \langle \mathsf{false}, \mathsf{xs} \rangle \end{aligned} \tag{32}$$

Alternatively, let J be the set of dyadic rationals in $(0,1)$ (i.e. those with power-of-two denominators), $\mathsf{j}_0 := \frac{1}{2}$ and

$$\begin{aligned} \mathsf{left}\ (\mathsf{p}/\mathsf{q}) &:= (\mathsf{p} - \tfrac{1}{2})/\mathsf{q} \\ \mathsf{right}\ (\mathsf{p}/\mathsf{q}) &:= (\mathsf{p} + \tfrac{1}{2})/\mathsf{q} \end{aligned} \tag{33}$$

With this alternative, left-to-right evaluation order can be made to correspond with the natural order $(<)$ over J.

7.2 Applicative, Associative Store

XXX: **arrow transformer**: an arrow whose combinators are defined entirely in terms of another arrow

XXX: computations receive an index and return an arrow from a store of type s paired with x, to y:

$$\mathsf{AStore}\ \mathsf{s}\ (\mathsf{x} \rightsquigarrow_{\mathsf{a}} \mathsf{y}) ::= \mathsf{J} \Rightarrow (\langle \mathsf{s}, \mathsf{x} \rangle \rightsquigarrow_{\mathsf{a}} \mathsf{y}) \tag{34}$$

XXX: motivational wurds for definition of lift:

$$\begin{aligned} &\eta_{\mathsf{a}^*} : (\mathsf{x} \rightsquigarrow_{\mathsf{a}} \mathsf{y}) \Rightarrow \mathsf{AStore}\ \mathsf{s}\ (\mathsf{x} \rightsquigarrow_{\mathsf{a}} \mathsf{y}) \\ &\eta_{\mathsf{a}^*}\ \mathsf{f}\ \mathsf{j} := \mathsf{arr}_{\mathsf{a}}\ \mathsf{snd} \ggg_{\mathsf{a}} \mathsf{f} \end{aligned} \tag{35}$$

Figure 7 defines the AStore arrow transformer. As with the other arrows, proving that its lift is a homomorphism allows us to prove that programs interpreted as its computations are correct. Again, to do so, we need to extend equivalence to be more extensional for arrows $\mathsf{AStore}\ \mathsf{s}\ (\mathsf{x} \rightsquigarrow_{\mathsf{a}} \mathsf{y})$.

Definition 7.2.1 (AStore arrow equivalence). *Two* AStore *arrow computations* k_1 *and* k_2 *are equivalent, or* $\mathsf{k}_1 \equiv \mathsf{k}_2$*, when* $\mathsf{k}_1\ \mathsf{j} \equiv \mathsf{k}_2\ \mathsf{j}$ *for all* $\mathsf{j} \in \mathsf{J}$.

Theorem 7.2.2 (AStore arrow correctness). *Let* $\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{y} ::= \mathsf{AStore}\ \mathsf{s}\ (\mathsf{x} \rightsquigarrow_{\mathsf{a}} \mathsf{y})$*. Then* η_{a^*} *is an arrow homomorphism.*

Proof. Defining $\mathsf{arr}_{\mathsf{a}^*}$ as a composition clearly meets the first homomorphism identity (13).

Composition. Starting with the right side of (14), expand definitions and use $(\mathsf{arr}_{\mathsf{a}}\ \mathsf{f}\ \&\&\&_{\mathsf{a}}\ \mathsf{f}_1) \ggg_{\mathsf{a}} \mathsf{arr}_{\mathsf{a}}\ \mathsf{snd} \equiv \mathsf{f}_1$:

$$\begin{aligned} &(\eta_{\mathsf{a}^*}\ \mathsf{f}_1 \ggg_{\mathsf{a}^*} \eta_{\mathsf{a}^*}\ \mathsf{f}_2)\ \mathsf{j} \\ &\quad\equiv (\mathsf{arr}_{\mathsf{a}}\ \mathsf{fst}\ \&\&\&_{\mathsf{a}}\ (\mathsf{arr}_{\mathsf{a}}\ \mathsf{snd} \ggg_{\mathsf{a}} \mathsf{f}_1)) \ggg_{\mathsf{a}} \mathsf{arr}_{\mathsf{a}}\ \mathsf{snd} \ggg_{\mathsf{a}} \mathsf{f}_2 \\ &\quad\equiv \mathsf{arr}_{\mathsf{a}}\ \mathsf{snd} \ggg_{\mathsf{a}} \mathsf{f}_1 \ggg_{\mathsf{a}} \mathsf{f}_2 \\ &\quad\equiv \eta_{\mathsf{a}^*}\ (\mathsf{f}_1 \ggg_{\mathsf{a}} \mathsf{f}_2)\ \mathsf{j} \end{aligned}$$

Pairing. Starting with the right side of (15), expand definitions and use the arrow law $\mathsf{arr}_{\mathsf{a}}\ \mathsf{f} \ggg_{\mathsf{a}} (\mathsf{f}_1\ \&\&\&_{\mathsf{a}}\ \mathsf{f}_2) \equiv (\mathsf{arr}_{\mathsf{a}}\ \mathsf{f} \ggg_{\mathsf{a}} \mathsf{f}_1)\ \&\&\&_{\mathsf{a}}\ (\mathsf{arr}_{\mathsf{a}}\ \mathsf{f} \ggg_{\mathsf{a}} \mathsf{f}_2)$:

$$\begin{aligned} &(\eta_{\mathsf{a}^*}\ \mathsf{f}_1\ \&\&\&_{\mathsf{a}^*}\ \eta_{\mathsf{a}^*}\ \mathsf{f}_2)\ \mathsf{j} \\ &\quad\equiv (\mathsf{arr}_{\mathsf{a}}\ \mathsf{snd} \ggg_{\mathsf{a}} \mathsf{f}_1)\ \&\&\&_{\mathsf{a}}\ (\mathsf{arr}_{\mathsf{a}}\ \mathsf{snd} \ggg_{\mathsf{a}} \mathsf{f}_2) \\ &\quad\equiv \mathsf{arr}_{\mathsf{a}}\ \mathsf{snd} \ggg_{\mathsf{a}} (\mathsf{f}_1\ \&\&\&_{\mathsf{a}}\ \mathsf{f}_2) \\ &\quad\equiv \eta_{\mathsf{a}^*}\ (\mathsf{f}_1\ \&\&\&_{\mathsf{a}}\ \mathsf{f}_2)\ \mathsf{j} \end{aligned}$$

Conditional. Starting with the right side of (16), expand definitions and use the arrow law $\mathsf{arr}_{\mathsf{a}}\ \mathsf{f} \ggg_{\mathsf{a}} \mathsf{ifte}_{\mathsf{a}}\ \mathsf{f}_1\ \mathsf{f}_2\ \mathsf{f}_3 \equiv \mathsf{ifte}_{\mathsf{a}}\ (\mathsf{arr}_{\mathsf{a}}\ \mathsf{f} \ggg_{\mathsf{a}} \mathsf{f}_1)\ (\mathsf{arr}_{\mathsf{a}}\ \mathsf{f} \ggg_{\mathsf{a}} \mathsf{f}_2)\ (\mathsf{arr}_{\mathsf{a}}\ \mathsf{f} \ggg_{\mathsf{a}} \mathsf{f}_3)$:

$$\begin{aligned} &(\mathsf{ifte}_{\mathsf{a}^*}\ (\eta_{\mathsf{a}^*}\ \mathsf{f}_1)\ (\eta_{\mathsf{a}^*}\ \mathsf{f}_2)\ (\eta_{\mathsf{a}^*}\ \mathsf{f}_3))\ \mathsf{j} \\ &\quad\equiv \mathsf{ifte}_{\mathsf{a}}\ (\mathsf{arr}_{\mathsf{a}}\ \mathsf{snd} \ggg_{\mathsf{a}} \mathsf{f}_1) \\ &\qquad\qquad (\mathsf{arr}_{\mathsf{a}}\ \mathsf{snd} \ggg_{\mathsf{a}} \mathsf{f}_2) \\ &\qquad\qquad (\mathsf{arr}_{\mathsf{a}}\ \mathsf{snd} \ggg_{\mathsf{a}} \mathsf{f}_3) \\ &\quad\equiv \mathsf{arr}_{\mathsf{a}}\ \mathsf{snd} \ggg_{\mathsf{a}} (\mathsf{ifte}\ \mathsf{f}_1\ \mathsf{f}_2\ \mathsf{f}_3) \\ &\quad\equiv \eta_{\mathsf{a}^*}\ (\mathsf{ifte}\ \mathsf{f}_1\ \mathsf{f}_2\ \mathsf{f}_3)\ \mathsf{j} \end{aligned}$$

Laziness. Starting with the right side of (17), expand definitions, β-expand within the outer thunk, and use the arrow law $\mathsf{arr}_{\mathsf{a}}\ \mathsf{f} \ggg_{\mathsf{a}} \mathsf{lazy}_{\mathsf{a}}\ \mathsf{f}_1 \equiv \mathsf{lazy}_{\mathsf{a}}\ \lambda 0.\ \mathsf{arr}_{\mathsf{a}}\ \mathsf{f} \ggg_{\mathsf{a}} \mathsf{f}_1\ 0$:

$$\begin{aligned} &(\mathsf{lazy}_{\mathsf{a}^*}\ \lambda 0.\ \eta_{\mathsf{a}^*}\ (\mathsf{f}\ 0))\ \mathsf{j} \\ &\quad\equiv \mathsf{lazy}_{\mathsf{a}}\ \lambda 0.\ (\lambda 0.\ \lambda \mathsf{j}.\ \mathsf{arr}_{\mathsf{a}}\ \mathsf{snd} \ggg_{\mathsf{a}} \mathsf{f}\ 0)\ 0\ \mathsf{j} \\ &\quad\equiv \mathsf{lazy}_{\mathsf{a}}\ \lambda 0.\ \mathsf{arr}_{\mathsf{a}}\ \mathsf{snd} \ggg_{\mathsf{a}} \mathsf{f}\ 0 \\ &\quad\equiv \mathsf{arr}_{\mathsf{a}}\ \mathsf{snd} \ggg_{\mathsf{a}} \mathsf{lazy}_{\mathsf{a}}\ \mathsf{f} \\ &\quad\equiv \eta_{\mathsf{a}^*}\ (\mathsf{lazy}_{\mathsf{a}}\ \mathsf{f})\ \mathsf{j} \end{aligned}$$

XXX: all of these rely on arrow laws that aren't proved for the mapping and preimage arrows ☐

Corollary 7.2.3 (semantic correctness). *Let* $\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{y} ::= \mathsf{AStore}\ \mathsf{s}\ (\mathsf{x} \rightsquigarrow_{\mathsf{a}} \mathsf{y})$*. If* $[\![e]\!]_{\mathsf{a}} : \mathsf{x} \rightsquigarrow_{\mathsf{a}} \mathsf{y}$*, then* $\eta_{\mathsf{a}^*}\ [\![e]\!]_{\mathsf{a}} \equiv [\![e]\!]_{\mathsf{a}^*}$ *and* $[\![e]\!]_{\mathsf{a}^*} : \mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{y}$.

In particular, Corollary 7.2.3 implies that, if a pure let-calculus expression is interpreted as a computation $\mathsf{k} : \mathsf{AStore}\ \mathsf{S}\ (\mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Y})$, then $\mathsf{k}\ \mathsf{j}_0$ correctly computes preimages. We still need to know that preimages under functions that access the store are computed correctly, which we will get to after defining stores and combinators that access them.

7.3 Probabilistic Programs

Definition 7.3.1 (random source). *Let* $\mathsf{R} := \mathsf{J} \to [0,1]$*. A **random source** is a total mapping* $\mathsf{r} \in \mathsf{R}$*; equivalently, an infinite vector of random numbers indexed by* J.

Let $\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{y} ::= \mathsf{AStore}\ \mathsf{R}\ (\mathsf{x} \rightsquigarrow_{\mathsf{a}} \mathsf{y})$. The following combinator returns the number at its own index in the random source:

$$\begin{aligned} &\mathsf{random}_{\mathsf{a}^*} : \mathsf{x} \rightsquigarrow_{\mathsf{a}^*} [0,1] \\ &\mathsf{random}_{\mathsf{a}^*}\ \mathsf{j} := \mathsf{arr}_{\mathsf{a}}\ (\mathsf{fst} \ggg \pi\ \mathsf{j}) \end{aligned} \tag{36}$$

We extend the let-calculus semantic function with

$$[\![\mathsf{random}]\!]_{\mathsf{a}^*} :\equiv \mathsf{random}_{\mathsf{a}^*} \tag{37}$$

for arrows a^* for which $\mathsf{random}_{\mathsf{a}^*}$ is defined.

7.4 Partial Programs

The most effective and ultimately implementable way we have found to avoid divergence in computing preimages is to use the store to dictate which branch of each conditional, if any, is allowed to be taken.

Definition 7.4.1 (branch trace). *A **branch trace** is a total mapping (i.e. vector)* $\mathsf{t} \in \mathsf{J} \to \mathsf{Bool}_{\perp}$ *such that* $\mathsf{t}\ \mathsf{j} = \mathsf{true}$ *or* $\mathsf{t}\ \mathsf{j} = \mathsf{false}$ *for no more than finitely many* $\mathsf{j} \in \mathsf{J}$.

$$\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{y} \ ::= \ \mathsf{AStore\ s}\ (\mathsf{x} \rightsquigarrow_{\mathsf{a}} \mathsf{y}) \ ::= \ \mathsf{J} \Rightarrow (\langle \mathsf{s}, \mathsf{x} \rangle \rightsquigarrow_{\mathsf{a}} \mathsf{y})$$

$$\begin{aligned}
&\mathsf{arr}_{\mathsf{a}^*} : (\mathsf{x} \Rightarrow \mathsf{y}) \Rightarrow (\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{y}) \\
&\mathsf{arr}_{\mathsf{a}^*} \ := \ \eta_{\mathsf{a}^*} \circ \mathsf{arr}_{\mathsf{a}}
\end{aligned}$$

$$\begin{aligned}
&(\ggg_{\mathsf{a}^*}) : (\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{y}) \Rightarrow (\mathsf{y} \rightsquigarrow_{\mathsf{a}^*} \mathsf{z}) \Rightarrow (\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{z}) \\
&(\mathsf{k}_1 \ggg_{\mathsf{a}^*} \mathsf{k}_2)\ \mathsf{j} \ := \\
&\quad (\mathsf{arr_a\ fst}\ \&\&\&_{\mathsf{a}}\ \mathsf{k}_1\ (\mathsf{left\ j})) \ggg_{\mathsf{a}} \mathsf{k}_2\ (\mathsf{right\ j})
\end{aligned}$$

$$\begin{aligned}
&(\&\&\&_{\mathsf{a}^*}) : (\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{y}_1) \Rightarrow (\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{y}_2) \Rightarrow (\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \langle \mathsf{y}_1, \mathsf{y}_2 \rangle) \\
&(\mathsf{k}_1\ \&\&\&_{\mathsf{a}^*}\ \mathsf{k}_2)\ \mathsf{j} \ := \ \mathsf{k}_1\ (\mathsf{left\ j})\ \&\&\&_{\mathsf{a}}\ \mathsf{k}_2\ (\mathsf{right\ j})
\end{aligned}$$

$$\begin{aligned}
&\mathsf{ifte}_{\mathsf{a}^*} : (\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{Bool}) \Rightarrow (\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{y}) \Rightarrow (\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{y}) \Rightarrow (\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{y}) \\
&\mathsf{ifte}_{\mathsf{a}^*}\ \mathsf{k}_1\ \mathsf{k}_2\ \mathsf{k}_3\ \mathsf{j} \ := \ \mathsf{ifte}_{\mathsf{a}}\ (\mathsf{k}_1\ (\mathsf{left\ j})) \\
&\qquad\qquad\qquad\qquad\qquad (\mathsf{k}_2\ (\mathsf{left}\ (\mathsf{right\ j}))) \\
&\qquad\qquad\qquad\qquad\qquad (\mathsf{k}_3\ (\mathsf{right}\ (\mathsf{right\ j})))
\end{aligned}$$

$$\begin{aligned}
&\mathsf{lazy}_{\mathsf{a}^*} : (1 \Rightarrow (\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{y})) \Rightarrow (\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{y}) \\
&\mathsf{lazy}_{\mathsf{a}^*}\ \mathsf{k\ j} \ := \ \mathsf{lazy}_{\mathsf{a}}\ \lambda 0.\, \mathsf{k\ 0\ j}
\end{aligned}$$

$$\begin{aligned}
&\eta_{\mathsf{a}^*} : (\mathsf{x} \rightsquigarrow_{\mathsf{a}} \mathsf{y}) \Rightarrow (\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{y}) \\
&\eta_{\mathsf{a}^*}\ \mathsf{f\ j} \ := \ \mathsf{arr_a\ snd} \ggg_{\mathsf{a}} \mathsf{f}
\end{aligned}$$

Figure 7: AStore (associative store) arrow transformer definitions.

Let $\mathsf{T} \subset \mathsf{J} \to \mathsf{Bool}_\perp$ be the set of all branch traces, and $\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{y} ::= \mathsf{AStore\ T}\ (\mathsf{x} \rightsquigarrow_{\mathsf{a}} \mathsf{y})$. The following combinator returns $\mathsf{t\ j}$ using its own index j:

$$\begin{aligned}
&\mathsf{branch}_{\mathsf{a}^*} : \mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{Bool} \\
&\mathsf{branch}_{\mathsf{a}^*}\ \mathsf{j} \ := \ \mathsf{arr_a}\ (\mathsf{fst} \ggg \pi\ \mathsf{j})
\end{aligned} \tag{38}$$

Using $\mathsf{branch}_{\mathsf{a}^*}$, we define an additional if-then-else combinator, which ensures its conditional expression agrees with the branch trace:

$$\begin{aligned}
&\mathsf{agrees} : \langle \mathsf{Bool}, \mathsf{Bool} \rangle \Rightarrow \mathsf{Bool}_\perp \\
&\mathsf{agrees}\ \langle \mathsf{b}_1, \mathsf{b}_2 \rangle \ := \ \mathsf{if}\ (\mathsf{b}_1 = \mathsf{b}_2)\ \mathsf{b}_1\ \perp
\end{aligned} \tag{39}$$

$$\begin{aligned}
&\mathsf{ifte}'_{\mathsf{a}^*} : (\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{Bool}) \Rightarrow (\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{y}) \Rightarrow (\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{y}) \Rightarrow (\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{y}) \\
&\mathsf{ifte}'_{\mathsf{a}^*}\ \mathsf{k}_1\ \mathsf{k}_2\ \mathsf{k}_3 \ := \\
&\quad \mathsf{ifte}_{\mathsf{a}^*}\ ((\mathsf{k}_1\ \&\&\&_{\mathsf{a}^*}\ \mathsf{branch}_{\mathsf{a}^*}) \ggg_{\mathsf{a}^*} \mathsf{arr}_{\mathsf{a}^*}\ \mathsf{agrees})\ \mathsf{k}_2\ \mathsf{k}_3
\end{aligned} \tag{40}$$

If the branch trace agrees with the conditional expression, it computes a branch; otherwise, it returns an error.

Every computation defined using the let-calculus semantic function $[\![\cdot]\!]_{\mathsf{a}}$, whose *defining expression* converges, must have its recurrences guarded by an if. Thus, if we stick to well-defined let-calculus programs, we need only replace $\mathsf{ifte}_{\mathsf{a}^*}$ with $\mathsf{ifte}'_{\mathsf{a}^*}$ to ensure *computations* always converge. Therefore, we can define a semantic function $[\![\cdot]\!]'_{\mathsf{a}^*}$ for let-calculus programs whose computations always converge by overriding only the if rule:

$$\begin{aligned}
[\![\mathsf{if}\ e_c\ e_t\ e_f]\!]'_{\mathsf{a}^*} \ &:\equiv \ \mathsf{ifte}'_{\mathsf{a}^*}\ [\![e_c]\!]_{\mathsf{a}^*} \\
&\qquad\qquad (\mathsf{lazy_a}\ \lambda 0.\, [\![e_t]\!]_{\mathsf{a}^*}) \\
&\qquad\qquad (\mathsf{lazy_a}\ \lambda 0.\, [\![e_f]\!]_{\mathsf{a}^*}) \\
[\![e]\!]'_{\mathsf{a}^*} \ &:\equiv \ [\![e]\!]_{\mathsf{a}^*}
\end{aligned} \tag{41}$$

7.5 Partial, Probabilistic Programs

Let $\mathsf{S} ::= \mathsf{R} \times \mathsf{T}$ and $\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{y} ::= \mathsf{AStore\ S}\ (\mathsf{x} \rightsquigarrow_{\mathsf{a}} \mathsf{y})$, and update the $\mathsf{random}_{\mathsf{a}^*}$ and $\mathsf{branch}_{\mathsf{a}^*}$ combinators to reflect that the store is now a pair:

$$\begin{aligned}
&\mathsf{random}_{\mathsf{a}^*} : \mathsf{x} \rightsquigarrow_{\mathsf{a}^*} [0,1] \\
&\mathsf{random}_{\mathsf{a}^*}\ \mathsf{j} \ := \ \mathsf{arr_a}\ (\mathsf{fst} \ggg \mathsf{fst} \ggg \pi\ \mathsf{j})
\end{aligned} \tag{42}$$

$$\begin{aligned}
&\mathsf{branch}_{\mathsf{a}^*} : \mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{Bool} \\
&\mathsf{branch}_{\mathsf{a}^*}\ \mathsf{j} \ := \ \mathsf{arr_a}\ (\mathsf{fst} \ggg \mathsf{snd} \ggg \pi\ \mathsf{j})
\end{aligned} \tag{43}$$

The $\mathsf{ifte}'_{\mathsf{a}^*}$ combinator's definition remains the same.

From here on, let $\mathsf{x} \rightsquigarrow_{\perp^*} \mathsf{y} ::= \mathsf{AStore\ S}\ (\mathsf{x} \rightsquigarrow_{\perp} \mathsf{y})$; similarly for $\mathsf{X} \underset{\mathsf{map}^*}{\rightsquigarrow} \mathsf{Y}$ and $\mathsf{X} \underset{\mathsf{pre}^*}{\rightsquigarrow} \mathsf{Y}$.

7.6 Correctness

Theorem 7.6.1 (natural transformation)**.** *Let* $\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{y} ::= \mathsf{AStore\ s}\ (\mathsf{x} \rightsquigarrow_{\mathsf{a}} \mathsf{y})$ *and* $\mathsf{x} \rightsquigarrow_{\mathsf{b}^*} \mathsf{y} ::= \mathsf{AStore\ s}\ (\mathsf{x} \rightsquigarrow_{\mathsf{b}^*} \mathsf{y})$*. Let* $\mathsf{lift_b} : (\mathsf{x} \rightsquigarrow_{\mathsf{a}} \mathsf{y}) \Rightarrow (\mathsf{x} \rightsquigarrow_{\mathsf{b}} \mathsf{y})$ *be an arrow homomorphism, and define*

$$\begin{aligned}
&\mathsf{lift}_{\mathsf{b}^*} : (\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{y}) \Rightarrow (\mathsf{x} \rightsquigarrow_{\mathsf{b}^*} \mathsf{y}) \\
&\mathsf{lift}_{\mathsf{b}^*}\ \mathsf{f\ j} \ := \ \mathsf{lift_b}\ (\mathsf{f\ j})
\end{aligned} \tag{44}$$

The following diagram commutes:

$$\begin{array}{ccc}
\mathsf{x} \rightsquigarrow_{\mathsf{a}} \mathsf{y} & \xrightarrow{\mathsf{lift_b}} & \mathsf{x} \rightsquigarrow_{\mathsf{b}} \mathsf{y} \\
{\scriptstyle \eta_{\mathsf{a}^*}} \big\downarrow & & \big\downarrow {\scriptstyle \eta_{\mathsf{b}^*}} \\
\mathsf{x} \rightsquigarrow_{\mathsf{a}^*} \mathsf{y} & \xrightarrow[\mathsf{lift}_{\mathsf{b}^*}]{} & \mathsf{x} \rightsquigarrow_{\mathsf{b}^*} \mathsf{y}
\end{array} \tag{45}$$

i.e. for all $\mathsf{f} : \mathsf{x} \rightsquigarrow_{\mathsf{a}} \mathsf{y}$, $\eta_{\mathsf{b}^*}\ (\mathsf{lift_b\ f}) \equiv \mathsf{lift}_{\mathsf{b}^*}\ (\eta_{\mathsf{a}^*}\ \mathsf{f})$*. Further,* $\mathsf{lift}_{\mathsf{b}^*}$ *is an arrow homomorphism.*

Proof. Starting from the right side of the equivalence, expand definitions and apply homomorphism identities (14) and (13) for $\mathsf{lift_b}$:

$$\begin{aligned}
\mathsf{lift}_{\mathsf{b}^*}\ (\eta_{\mathsf{a}^*}\ \mathsf{f}) \ &\equiv \ \lambda \mathsf{j}.\, \mathsf{lift_b}\ (\mathsf{arr_a\ snd} \ggg_{\mathsf{a}} \mathsf{f}) \\
&\equiv \ \lambda \mathsf{j}.\, \mathsf{lift_b}\ (\mathsf{arr_a\ snd}) \ggg_{\mathsf{b}} \mathsf{lift_b\ f} \\
&\equiv \ \lambda \mathsf{j}.\, \mathsf{arr_b\ snd} \ggg_{\mathsf{b}} \mathsf{lift_b\ f} \\
&\equiv \ \eta_{\mathsf{b}^*}\ (\mathsf{lift_b\ f})
\end{aligned}$$

Further, because η_{a^*}, η_{b^*}, and $\mathsf{lift_b}$ are homomorphisms, $\mathsf{lift}_{\mathsf{b}^*}$ is a homomorphism by composition.

XXX: not sure I'm allowed to invoke converse of composition of homomorphisms without extra conditions ∎

Corollary 7.6.2 (mapping* and preimage* arrow correctness)**.** *The following diagram commutes:*

$$\begin{array}{ccccc}
\mathsf{X} \rightsquigarrow_{\perp} \mathsf{Y} & \xrightarrow{\mathsf{lift_{map}}} & \mathsf{X} \underset{\mathsf{map}}{\rightsquigarrow} \mathsf{Y} & \xrightarrow{\mathsf{lift_{pre}}} & \mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Y} \\
{\scriptstyle \eta_{\perp^*}} \big\downarrow & & \big\downarrow {\scriptstyle \eta_{\mathsf{map}^*}} & & \big\downarrow {\scriptstyle \eta_{\mathsf{pre}^*}} \\
\mathsf{X} \rightsquigarrow_{\perp^*} \mathsf{Y} & \xrightarrow[\mathsf{lift}_{\mathsf{map}^*}]{} & \mathsf{X} \underset{\mathsf{map}^*}{\rightsquigarrow} \mathsf{Y} & \xrightarrow[\mathsf{lift}_{\mathsf{pre}^*}]{} & \mathsf{X} \underset{\mathsf{pre}^*}{\rightsquigarrow} \mathsf{Y}
\end{array} \tag{46}$$

Further, $\mathsf{lift}_{\mathsf{map}^*}$ *and* $\mathsf{lift}_{\mathsf{pre}^*}$ *are arrow homomorphisms.*

Corollary 7.6.3 (semantic correctness)**.** *If* $[\![e]\!]_{\perp *} : \mathsf{X} \rightsquigarrow_{\perp *} \mathsf{Y}$, *then* $\mathsf{lift}_{\mathsf{map}*}\ [\![e]\!]_{\perp *} \equiv [\![e]\!]_{\mathsf{map}*}$ *and* $\mathsf{lift}_{\mathsf{pre}*}\ [\![e]\!]_{\mathsf{map}*} \equiv [\![e]\!]_{\mathsf{pre}*}$.

Corollary 7.6.4 (semantic′ correctness)**.** *If* $[\![e]\!]'_{\perp *} : \mathsf{X} \rightsquigarrow_{\perp *} \mathsf{Y}$, *then* $\mathsf{lift}_{\mathsf{map}*}\ [\![e]\!]'_{\perp *} \equiv [\![e]\!]'_{\mathsf{map}*}$ *and* $\mathsf{lift}_{\mathsf{pre}*}\ [\![e]\!]'_{\mathsf{map}*} \equiv [\![e]\!]'_{\mathsf{pre}*}$.

In particular, $[\![e]\!]_{\mathsf{pre}*}$ and $[\![e]\!]'_{\mathsf{pre}*}$ correctly compute preimages under the interpretation of e as a function from an implicit random source. We will make stronger statements about $[\![\cdot]\!]'_{\mathsf{pre}*}$ after proving its computations always converge.

Theorem 7.6.5 (divergence implies error)**.** *Let* $\mathsf{f} := [\![e]\!]_{\perp *}$ *and* $\mathsf{f}' := [\![e]\!]'_{\perp *}$ *converge, where* $\mathsf{f} : \mathsf{x} \rightsquigarrow_{\perp *} \mathsf{y}$. *For all* $\mathsf{r} \in \mathsf{R}$, $\mathsf{t} \in \mathsf{T}$ *and* $\mathsf{a} : \mathsf{x}$,

1. *If* $\mathsf{f}\ \langle\langle \mathsf{r}, \mathsf{t}\rangle, \mathsf{a}\rangle = \mathsf{b}$, *then* $\mathsf{f}'\ \langle\langle \mathsf{r}, \mathsf{t}'\rangle, \mathsf{a}\rangle = \mathsf{b}$ *for some* $\mathsf{t}' \in \mathsf{T}$.
2. *If* $\mathsf{f}\ \langle\langle \mathsf{r}, \mathsf{t}\rangle, \mathsf{a}\rangle$ *diverges,* $\mathsf{f}'\ \langle\langle \mathsf{r}, \mathsf{t}'\rangle, \mathsf{a}\rangle = \perp$ *for all* $\mathsf{t}' \in \mathsf{T}$.

Proof. Let $\mathsf{m} : \mathsf{J} \Rightarrow \mathsf{J}$ invertibly map sub-computation indexes in f' to corresponding sub-computation indexes in f. (Defining m formally is tedious and unilluminating.)

Case 1. Define $\mathsf{t}' \in \mathsf{J} \to \mathsf{Bool}_\perp$ such that $\mathsf{t}'\ \mathsf{j} = \mathsf{z}$ if the sub-computation with index $\mathsf{m}\ \mathsf{j}$ in f is an if condition that returns z, otherwise $\mathsf{t}'\ \mathsf{j} = \perp$. Because $\mathsf{f}\ \langle\langle \mathsf{r}, \mathsf{t}\rangle, \mathsf{a}\rangle$ converges, $\mathsf{t}'\ \mathsf{j} \neq \perp$ for at most finitely many j, so $\mathsf{t}' \in \mathsf{T}$. Exists t'.

Case 2. Let $\mathsf{t}' \in \mathsf{T}$. There exists an infinite *suffix* $\mathsf{J}' \subset \mathsf{J}$ closed under left and right, such that for all $\mathsf{j}' \in \mathsf{J}'$, $\mathsf{t}'\ \mathsf{j}' = \perp$. Because $\mathsf{f}\ \langle\langle \mathsf{r}, \mathsf{t}\rangle, \mathsf{a}\rangle$ diverges, the indexes of its if conditions are unbounded; there is therefore a condition with index j such that $\mathsf{m}^{-1}\ \mathsf{j} \in \mathsf{J}'$. It returns $\perp$, so $\mathsf{f}'\ \langle\langle \mathsf{r}, \mathsf{t}'\rangle, \mathsf{a}\rangle = \perp$. ☐

Definition 7.6.6 (halting set)**.** *A halting set* A^* *can be defined for any bottom*, mapping* or preimage* arrow computation. In all cases,* $\mathsf{A}^* \subseteq (\mathsf{R} \times \mathsf{T}) \times \mathsf{X}$, *defined by*

- $\mathsf{f} : \mathsf{X} \rightsquigarrow_{\perp *} \mathsf{Y}$*: largest* A^* *for which* $\mathsf{f}\ \mathsf{j}_0\ \mathsf{x} \neq \perp$ *(which implies convergence) for all* $\mathsf{x} \in \mathsf{A}^*$.
- $\mathsf{g} : \mathsf{X} \underset{\mathsf{map}*}{\rightsquigarrow} \mathsf{Y}$*: largest* A^* *for which* $\mathsf{domain}\ (\mathsf{g}\ \mathsf{j}_0\ \mathsf{A}^*) = \mathsf{A}^*$ *(which implies convergence).*
- $\mathsf{h} : \mathsf{X} \underset{\mathsf{pre}*}{\rightsquigarrow} \mathsf{Y}$*: largest* A^* *for which* $\mathsf{pre\text{-}ap}\ (\mathsf{h}\ \mathsf{j}_0\ \mathsf{A}^*)\ \mathsf{Y} = \mathsf{A}^*$.

That $\mathsf{lift}_{\mathsf{map}*}$ and $\mathsf{lift}_{\mathsf{pre}*}$ are arrow homomorphisms allows transporting halting set definitions and theorems between arrow types.

Corollary 7.6.7 (halting set equality)**.** *Let* $\mathsf{f} : \mathsf{X} \rightsquigarrow_{\perp *} \mathsf{Y}$, *and* $\mathsf{g} : \mathsf{X} \underset{\mathsf{map}*}{\rightsquigarrow} \mathsf{Y}$ *and* $\mathsf{h} : \mathsf{X} \underset{\mathsf{pre}*}{\rightsquigarrow} \mathsf{Y}$ *such that* $\mathsf{g} \equiv \mathsf{lift}_{\mathsf{map}*}\ \mathsf{f}$ *and* $\mathsf{h} \equiv \mathsf{lift}_{\mathsf{pre}*}\ \mathsf{g}$. *Then* f, g *and* h *have the same halting set.*

Definition 7.6.8 (halting probability)**.** *Let* $\mathsf{f} : \mathsf{X} \rightsquigarrow_{\perp *} \mathsf{Y}$ *and* A^* *be its halting set. Let* $\mathsf{P} \in \mathcal{P}\ \mathsf{R} \rightharpoonup [0,1]$ *be a probability measure over random stores. The* ***halting probability*** *of* f *is* $\mathsf{P}\ (\mathsf{image}\ (\mathsf{fst} \ggg \mathsf{fst})\ \mathsf{A}^*)$.

Corollary 7.6.9 (computed halting set)**.** *Let* $[\![e]\!]_{\perp *} : \mathsf{X} \rightsquigarrow_{\perp *} \mathsf{Y}$ *converge. Then* $\mathsf{A}^* = \mathsf{pre\text{-}ap}\ ([\![e]\!]'_{\mathsf{pre}*}\ \mathsf{j}_0\ (\mathsf{S} \times \mathsf{X}))\ \mathsf{Y}$.

Corollary 7.6.10 (semantic correctness (final))**.** *Let* $[\![e]\!]_{\perp *} : \mathsf{X} \rightsquigarrow_{\perp *} \mathsf{Y}$ *converge, with halting set* A^*. *For* $\mathsf{A} \subseteq \mathsf{X}$ *and* $\mathsf{B} \subseteq \mathsf{Y}$, $\mathsf{pre\text{-}ap}\ ([\![e]\!]'_{\mathsf{pre}*}\ \mathsf{j}_0\ \mathsf{A})\ \mathsf{B} = \mathsf{preimage}\ ([\![e]\!]_{\mathsf{map}*}\ \mathsf{j}_0\ (\mathsf{A} \cap \mathsf{A}^*))\ \mathsf{B}$.

In other words, preimages computed using $[\![\cdot]\!]'_{\mathsf{pre}*}$ always converge and never include inputs that give rise to errors or divergence.

8. Implementable Approximation

XXX: $\mathsf{arr}_{\mathsf{pre}}$ is generally uncomputable, but we don't need that many lifts; Figure 8 has the rest of the non-arithmetic ones we'll need

XXX: figure out a good way to present the following info

Figure 4:

- pre: can't implement
- $\mathsf{pre\text{-}ap}$: need $\cap$
- $\langle\cdot,\cdot\rangle_{\mathsf{pre}}$: approximate; need $\times$ and $\cap$
- $\circ_{\mathsf{pre}}$: no change
- $\uplus_{\mathsf{pre}}$: approximate; need join

Figure 6:

- $\mathsf{arr}_{\mathsf{pre}}$ (and $\mathsf{lift}_{\mathsf{pre}}$): can't implement
- $\ggg_{\mathsf{pre}}$: no change
- $\&\&\&_{\mathsf{pre}}$: use approximating $\langle\cdot,\cdot\rangle_{\mathsf{pre}}$
- $\mathsf{ifte}_{\mathsf{pre}}$: need $\{\mathsf{true}\}$ and $\{\mathsf{false}\}$; use approximating $\uplus_{\mathsf{pre}}$
- $\mathsf{lazy}_{\mathsf{pre}}$: need $(= \varnothing)$, $(\mathsf{pre}\ \varnothing)$

Figure 8:

- $\mathsf{id}_{\mathsf{pre}}$: no change
- $\mathsf{const}_{\mathsf{pre}}$: need $\{\mathsf{y}\}$, $(= \varnothing)$, $\varnothing$
- $\mathsf{fst}_{\mathsf{pre}}$ and $\mathsf{snd}_{\mathsf{pre}}$: need projections, i, $\times$
- π_{pre}: need projections, $\cap$, arbitrary products

9. Computable Approximation

References

[1] J. Hughes. Programming with arrows. In *5th International Summer School on Advanced Functional Programming*, pages 73–129, 2005.

[2] N. Toronto and J. McCarthy. Computing in Cantor's paradise with λ-ZFC. In *Functional and Logic Programming Symposium (FLOPS)*, pages 290–306, 2012.

$$\mathsf{id_{pre}} : \mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{X}$$
$$\mathsf{id_{pre}}\ \mathsf{A} \ := \ \langle \mathsf{A}, \lambda \mathsf{B}.\, \mathsf{B} \rangle$$

$$\mathsf{const_{pre}} : \mathsf{Y} \Rightarrow \mathsf{X} \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Y}$$
$$\mathsf{const_{pre}}\ \mathsf{y}\ \mathsf{A} \ := \ \langle \{\mathsf{y}\}, \lambda \mathsf{B}.\, \mathsf{if}\ (\mathsf{B} = \varnothing)\ \varnothing\ \mathsf{A} \rangle$$

$$\pi_{\mathsf{pre}} : \mathsf{J} \Rightarrow (\mathsf{J} \to \mathsf{X}) \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{X}$$
$$\begin{aligned} \pi_{\mathsf{pre}}\ \mathsf{j}\ \mathsf{A} \ := \ \mathsf{let}\ \ & \mathsf{A_j} := \mathsf{proj}\ \mathsf{j}\ \mathsf{A} \\ & \mathsf{p} := \lambda \mathsf{B}.\, \mathsf{A} \cap \textstyle\prod_{\mathsf{i} \in \mathsf{J}} \mathsf{if}\ (\mathsf{j} = \mathsf{i})\ \mathsf{B}\ (\mathsf{proj}\ \mathsf{i}\ \mathsf{A}) \\ \mathsf{in}\ \ & \langle \mathsf{A_j}, \mathsf{p} \rangle \end{aligned}$$

$$\mathsf{fst_{pre}} : \langle \mathsf{X}, \mathsf{Y} \rangle \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{X}$$
$$\begin{aligned} \mathsf{fst_{pre}}\ \mathsf{A} \ := \ \mathsf{let}\ \ & \mathsf{A_1} := \mathsf{image}\ \mathsf{fst}\ \mathsf{A} \\ & \mathsf{A_2} := \mathsf{image}\ \mathsf{snd}\ \mathsf{A} \\ \mathsf{in}\ \ & \langle \mathsf{A_1}, \lambda \mathsf{B}.\, \mathsf{A} \cap (\mathsf{B} \times \mathsf{A_2}) \rangle \end{aligned}$$

$$\mathsf{snd_{pre}} : \langle \mathsf{X}, \mathsf{Y} \rangle \underset{\mathsf{pre}}{\rightsquigarrow} \mathsf{Y}$$
$$\begin{aligned} \mathsf{snd_{pre}}\ \mathsf{A} \ := \ \mathsf{let}\ \ & \mathsf{A_1} := \mathsf{image}\ \mathsf{fst}\ \mathsf{A} \\ & \mathsf{A_2} := \mathsf{image}\ \mathsf{snd}\ \mathsf{A} \\ \mathsf{in}\ \ & \langle \mathsf{A_2}, \lambda \mathsf{B}.\, \mathsf{A} \cap (\mathsf{A_1} \times \mathsf{B}) \rangle \end{aligned}$$

Figure 8: Specific instances of $\mathsf{arr_{pre}}\ \mathsf{f}$