Contextual Coinduction and Classical Logic

Or: Fearlessly Observing the Infinite

Paul Downen

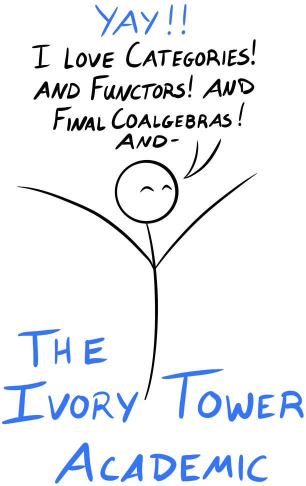
BU POPV: April 21, 2023

Coinduction, eh?

So when do we start talking about categories?

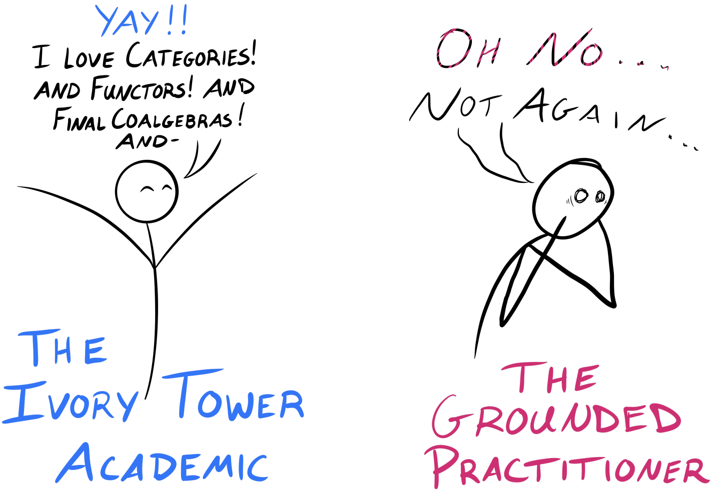
Coinduction, eh?

So when do we start talking about categories?



Coinduction, eh?

So when do we start talking about categories?



(Structural) Induction for Classic Algorithms

The Workhorse of Computer Science Theories A & B

Many classic (theory A) algorithms follow inductive structure:

- Sorting
- Searching
- Tree-based data structures

Language foundations (theory B): induction all the way down

- Syntax
- Semantics
- Compiliers
- Type systems

Proof assistants (the magnum opus of theory B) are effectively big induction engines.

Interacting With Others

Programs that need to interact with the outside world while they run are inherently coinductive:

- Operating systems & User Interfaces
- Web servers & Networks
- Distributed systems & IoT
- Real time & Embedded systems
- Control software & robotics

Coinduction is essiential to understand modern systems

Interacting With Others

Programs that need to interact with the outside world while they run are inherently coinductive:

- Operating systems & User Interfaces
- Web servers & Networks
- Distributed systems & IoT
- Real time & Embedded systems
- Control software & robotics

Coinduction is essiential to understand modern systems

So formal methods (type theory, proof assistants) have good support for coinduction, right?

Interacting With Others

Programs that need to interact with the outside world while they run are inherently coinductive:

- Operating systems & User Interfaces
- Web servers & Networks
- Distributed systems & IoT
- Real time & Embedded systems
- Control software & robotics

Coinduction is essiential to understand modern systems

So formal methods (type theory, proof assistants) have good support for coinduction, right?

...

Interacting With Others

Programs that need to interact with the outside world while they run are inherently coinductive:

- Operating systems & User Interfaces
- Web servers & Networks
- Distributed systems & IoT
- Real time & Embedded systems
- Control software & robotics

Coinduction is essiential to understand modern systems

So formal methods (type theory, proof assistants) have good support for coinduction, right?

…

…right …?

How To Coinduction?

Coinduction With Confidence

What is the Coinductive Hypothesis?

And When Can I Use It?

Coq's coinduction founded on begging the question

$cofix : (\forall x.P(x) \rightarrow P(x)) \rightarrow \forall x.P(x)$???

Viciously circular logic

Assume exactly what you are trying to prove …

…but only use it sometimes?

CIH should be guarded/inside a constructor

unless you eliminate it too soon …

CIH should be guarded/behind a projection

unless you use another projection in the "wrong spot" …

…or pass the result to another function (???)

"Guardedness" is trying to say something about the context's structure and how it shrinks

Principle (Induction on Natural Number Values)

Given property $P : \mathrm{Nat} \to \mathrm{Prop}$ *on natural numbers,*
$P(n)$ *holds for all numbers* $n : \mathrm{Nat}$ *if and only if*

$P(0)$ *holds, and*

for all $n : \mathrm{Nat}$, $P(n)$ *implies* $P(n+1)$.

Principle (Induction on Natural Number Values)

Given property $P : \mathrm{Nat} \to \mathrm{Prop}$ *on natural numbers,*
$P(n)$ *holds for all numbers* $n : \mathrm{Nat}$ *if and only if*

> $P(0)$ *holds, and*
>
> *for all* $n : \mathrm{Nat}$, $P(n)$ *implies* $P(n+1)$.

Principle (Coinduction on Stream Observations*)

Given property $P : (\mathrm{Stream}\ A \to B) \to \mathrm{Prop}$ *on stream observations,*
$P(f)$ *holds for all observations* $f : \mathrm{Stream}\ A \to B$ *if and only if*

> *for all* $g : A \to B$, $P(g \circ \mathrm{Head})$ *holds, and*
>
> *for all* $h : \mathrm{Stream}\ A \to B$, $P(h)$ *implies* $P(h \circ \mathrm{Tail})$.

Principle (Induction on Natural Number Values)

Given property $P : \mathrm{Nat} \to \mathrm{Prop}$ *on natural numbers,*
$P(n)$ *holds for all numbers* $n : \mathrm{Nat}$ *if and only if*

- $P(0)$ *holds, and*
- *for all* $n : \mathrm{Nat}$, $P(n)$ *implies* $P(n+1)$.

Principle (Coinduction on Stream Observations*)

Given property $P : (\mathrm{Stream}\ A \to B) \to \mathrm{Prop}$ *on stream observations,*
$P(f)$ *holds for all observations* $f : \mathrm{Stream}\ A \to B$ *if and only if*

- *for all* $g : A \to B$, $P(g \circ \mathrm{Head})$ *holds, and*
- *for all* $h : \mathrm{Stream}\ A \to B$, $P(h)$ *implies* $P(h \circ \mathrm{Tail})$.

Coinductive Contextual Equivalence

Principle (Contextual Equivalence)
Given $x : A$ and $y : A$,

$$x = y$$

IF AND ONLY IF

$$\textit{for all } f,\ f(x) = f(y).$$

Principle (Contextual Equivalence)
Given $x : A$ and $y : A$,

$$x = y$$

IF AND ONLY IF

$$\textit{for all } f,\ f(x) = f(y).$$

Corollary (Contextual Stream Equality)
Given $xs : \mathrm{Stream}\ A$ and $ys : \mathrm{Stream}\ A$,

$$xs = ys$$

IF AND ONLY IF

$$\textit{for all } g,\ g(\mathrm{Head}(xs)) = g(\mathrm{Head}(ys))$$

AND

$$\textit{for all } h,\ h(xs) = h(ys)\ \textit{IMPLIES}\ h(\mathrm{Tail}(xs)) = h(\mathrm{Tail}(ys))$$

Coinductive Contextual Equivalence

Coinductive Hypothesis = Labeling the Observer

Principle (Contextual Equivalence)
Given $x : A$ *and* $y : A$,

$$x = y$$

IF AND ONLY IF

$$\textit{for all } f,\ f(x) = f(y).$$

Corollary (Contextual Stream Equality)
Given $xs : \mathrm{Stream}\ A$ *and* $ys : \mathrm{Stream}\ A$,

$$xs = ys$$

IF AND ONLY IF

$$\textit{for all } g,\ g(\mathrm{Head}(xs)) = g(\mathrm{Head}(ys))$$

AND

$$\textit{for all } h,\ h(xs) = h(ys)\ \textit{IMPLIES}\ h(\mathrm{Tail}(xs)) = h(\mathrm{Tail}(ys))$$

Proof.
Contextual Equivalence + Coinduction on Stream Observations,

where $P(f) = (f(xs) = f(ys))$. □

Principle (Contextual Equivalence)
Given $x : A$ and $y : A$,

$$x = y$$

IF AND ONLY IF

$$\text{for all } f, f(x) = f(y).$$

Corollary (Contextual Stream Equality)
Given $xs : \mathrm{Stream}\ A$ and $ys : \mathrm{Stream}\ A$,

$$xs = ys$$

IF AND ONLY IF

$$\mathrm{Head}(xs) = \mathrm{Head}(ys)$$

AND

$$\text{for all } h, h(xs) = h(ys) \text{ IMPLIES } h(\mathrm{Tail}(xs)) = h(\mathrm{Tail}(ys))$$

Proof.
Contextual Equivalence + Coinduction on Stream Observations,

where $P(f) = (f(xs) = f(ys))$. □

$$
\begin{aligned}
always\ x &= \mathrm{Cons}\ x\ (always\ x) \\
repeat\ f\ x &= \mathrm{Cons}\ x\ (repeat\ f\ (f\ x))
\end{aligned}
$$

Theorem
$repeat\ (\lambda y.y)\ x = always\ x$

Proof.
Assume coinductive hypothesis (CoIH): $repeat\ (\lambda y.y)\ x = always\ x$.
Now prove $repeat\ (\lambda y.y)\ x = always\ x$:

$$repeat\ (\lambda y.y)\ x = always\ x \qquad (CoIH?)$$

□

$repeat\ id = always$

$$
\begin{aligned}
always\ x &= \mathrm{Cons}\ x\ (always\ x) \\
repeat\ f\ x &= \mathrm{Cons}\ x\ (repeat\ f\ (f\ x))
\end{aligned}
$$

Theorem
$repeat\ (\lambda y.y)\ x = always\ x$

Proof.
Assume coinductive hypothesis (CoIH): $repeat\ (\lambda y.y)\ x = always\ x$.
Now prove $repeat\ (\lambda y.y)\ x = always\ x$:

$$
\begin{aligned}
repeat\ (\lambda y.y)\ x &= \mathrm{Cons}\ x\ (repeat\ (\lambda y.y)\ ((\lambda y.y)\ x)) && (def.\ repeat) \\
&= \mathrm{Cons}\ x\ (repeat\ (\lambda y.y)\ x) && (\beta) \\
&= \mathrm{Cons}\ x\ (always\ x) && (CoIH) \\
&= always\ x && (def.\ always)
\end{aligned}
$$

$\square$

repeat id = *always*

By Begging the Question (Boo...)

$$\begin{aligned} \mathit{always}\ x &= \mathrm{Cons}\ x\ (\mathit{always}\ x) \\ \mathit{repeat}\ f\ x &= \mathrm{Cons}\ x\ (\mathit{repeat}\ f\ (f\ x)) \end{aligned}$$

Theorem
$\mathit{repeat}\ (\lambda y.y)\ x = \mathit{always}\ x$

Proof.
Assume coinductive hypothesis (CoIH): $\mathit{repeat}\ (\lambda y.y)\ x = \mathit{always}\ x$.

Now prove $\mathit{repeat}\ (\lambda y.y)\ x = \mathit{always}\ x$:

$$\begin{aligned} \mathit{repeat}\ (\lambda y.y)\ x &= \mathrm{Cons}\ x\ (\mathit{repeat}\ (\lambda y.y)\ ((\lambda y.y)\ x)) && (\mathit{def.}\ \mathit{repeat}) \\ &= \mathrm{Cons}\ x\ (\mathit{repeat}\ (\lambda y.y)\ x) && (\beta) \\ &= \mathrm{Cons}\ x\ (\mathit{always}\ x) && (\mathit{CoIH}) \\ &= \mathit{always}\ x && (\mathit{def.}\ \mathit{always}) \end{aligned}$$

$\square$

$repeat\ id = always$

$$\mathrm{Head}(\mathit{always}\ x) = x \qquad \mathrm{Tail}(\mathit{always}\ x) = \mathit{always}\ x$$
$$\mathrm{Head}(\mathit{repeat}\ f\ x) = x \qquad \mathrm{Tail}(\mathit{repeat}\ f\ x) = \mathit{repeat}\ f\ (f\ x)$$

Theorem
$\mathit{repeat}\ (\lambda y.y)\ x = \mathit{always}\ x$

Proof. By contextual stream equality:

(Head) Show $\mathrm{Head}(\mathit{repeat}\ (\lambda y.y)\ x) = \mathrm{Head}(\mathit{always}\ x)$

$$\mathrm{Head}(\mathit{repeat}\ (\lambda y.y)\ x) = x = \mathrm{Head}(\mathit{always}\ x)$$

$\mathit{repeat}\ \mathit{id} = \mathit{always}$

By Contextual Stream Equality (No Guesswork!)

$$\text{Head}(\mathit{always}\ x) = x \qquad \text{Tail}(\mathit{always}\ x) = \mathit{always}\ x$$
$$\text{Head}(\mathit{repeat}\ f\ x) = x \qquad \text{Tail}(\mathit{repeat}\ f\ x) = \mathit{repeat}\ f\ (f\ x)$$

Theorem
$\mathit{repeat}\ (\lambda y.y)\ x = \mathit{always}\ x$

Proof. By contextual stream equality:

(Head) Show $\text{Head}(\mathit{repeat}\ (\lambda y.y)\ x) = \text{Head}(\mathit{always}\ x)$

$$\text{Head}(\mathit{repeat}\ (\lambda y.y)\ x) = x = \text{Head}(\mathit{always}\ x)$$

(Tail) Assume CoIH: $h(\mathit{repeat}\ (\lambda y.y)\ x) = h(\mathit{always}\ x)$.
Show $h(\text{Tail}(\mathit{repeat}\ (\lambda y.y)\ x)) = h(\text{Tail}(\mathit{always}\ x))$.

$$\begin{aligned}
h(\text{Tail}(\mathit{repeat}\ (\lambda y.y)\ x)) &= h(\mathit{repeat}\ (\lambda y.y)\ ((\lambda y.y)\ x)) && (\mathit{def.\ repeat}) \\
&= h(\mathit{repeat}\ (\lambda y.y)\ x) && (\beta) \\
&= h(\mathit{always}\ x) && (\mathit{CoIH}) \\
&= h(\text{Tail}(\mathit{always}\ x)) && (\mathit{def.\ always})
\end{aligned}$$

repeat id = *always*

By Contextual Stream Equality (No Guesswork!)

$$\mathrm{Head}(\mathit{always}\ x) = x \qquad \mathrm{Tail}(\mathit{always}\ x) = \mathit{always}\ x$$
$$\mathrm{Head}(\mathit{repeat}\ f\ x) = x \qquad \mathrm{Tail}(\mathit{repeat}\ f\ x) = \mathit{repeat}\ f\ (f\ x)$$

Theorem
$\mathit{repeat}\ (\lambda y.y)\ x = \mathit{always}\ x$

Proof. By contextual stream equality:

(Head) Show $\mathrm{Head}(\mathit{repeat}\ (\lambda y.y)\ x) = \mathrm{Head}(\mathit{always}\ x)$

$$\mathrm{Head}(\mathit{repeat}\ (\lambda y.y)\ x) = x = \mathrm{Head}(\mathit{always}\ x)$$

(Tail) Assume CoIH: $h(\mathit{repeat}\ (\lambda y.y)\ x) = h(\mathit{always}\ x)$.
Show $h(\mathrm{Tail}(\mathit{repeat}\ (\lambda y.y)\ x)) = h(\mathrm{Tail}(\mathit{always}\ x))$.

$$\begin{aligned} h(\mathrm{Tail}(\mathit{repeat}\ (\lambda y.y)\ x)) &= h(\mathit{repeat}\ (\lambda y.y)\ ((\lambda y.y)\ x)) && (\mathit{def.\ repeat}) \\ &= h(\mathit{repeat}\ (\lambda y.y)\ x) && (\beta) \\ &= h(\mathit{always}\ x) && (\mathit{CoIH}) \\ &= h(\mathrm{Tail}(\mathit{always}\ x)) && (\mathit{def.\ always}) \end{aligned}$$

$map\ f\ (repeat\ f\ x) = repeat\ f\ (f\ x)$

$$\text{Head}(map\ f\ xs) = f\ (\text{Head}\ xs) \qquad \text{Tail}(map\ f\ xs) = map\ f\ (\text{Tail}\ xs)$$

$$\text{Head}(repeat\ f\ x) = x \qquad \text{Tail}(repeat\ f\ x) = repeat\ f\ (f\ x)$$

Theorem

for all x, $map\ f\ (repeat\ f\ x) = repeat\ f\ (f\ x)$

Proof. By contextual stream equality:

(Head) Show $\forall x$, $\text{Head}(map\ f\ (repeat\ f\ x)) = \text{Head}(repeat\ f\ (f\ x))$.

$$\begin{aligned}\text{Head}(map\ f\ (repeat\ f\ x)) &= f(\text{Head}(repeat\ f\ x)) = f(x) \\ &= \text{Head}(repeat\ f\ (f\ x))\end{aligned}$$

$map\ f\ (repeat\ f\ x) = repeat\ f\ (f\ x)$

$$\mathrm{Head}(map\ f\ xs) = f\ (\mathrm{Head}\ xs) \qquad \mathrm{Tail}(map\ f\ xs) = map\ f\ (\mathrm{Tail}\ xs)$$

$$\mathrm{Head}(repeat\ f\ x) = x \qquad \mathrm{Tail}(repeat\ f\ x) = repeat\ f\ (f\ x)$$

Theorem

for all x, $map\ f\ (repeat\ f\ x) = repeat\ f\ (f\ x)$

Proof. By contextual stream equality:

(Head) Show $\forall x, \mathrm{Head}(map\ f\ (repeat\ f\ x)) = \mathrm{Head}(repeat\ f\ (f\ x))$.

$$\begin{aligned}\mathrm{Head}(map\ f\ (repeat\ f\ x)) &= f(\mathrm{Head}(repeat\ f\ x)) = f(x)\\ &= \mathrm{Head}(repeat\ f\ (f\ x))\end{aligned}$$

(Tail) Assume CoIH: $\forall x, h(map\ f\ (repeat\ f\ x)) = h(repeat\ f\ (f\ x))$.
Show $\forall x, h(\mathrm{Tail}(map\ f\ (repeat\ f\ x))) = h(\mathrm{Tail}(repeat\ f\ (f\ x)))$.

$$\begin{aligned}h(\mathrm{Tail}(map\ f\ (repeat\ f\ x))) &= h(map\ f\ (\mathrm{Tail}(repeat\ f\ x)))\\ &= h(map\ f\ (repeat\ f\ (f\ x))) && (CoIH[(f\ x)/x])\\ &= h(repeat\ f\ (f\ (f\ x)))\\ &= h(\mathrm{Tail}(repeat\ f\ (f\ x)))\end{aligned}$$

Mutual Coinduction

$$
\begin{aligned}
evens\,(x_0, x_1, x_2, x_3, x_4, x_5, \ldots) &= x_0, x_2, x_4, \ldots \\
odds\,(x_0, x_1, x_2, x_3, x_4, x_5, \ldots) &= x_1, x_3, x_5, \ldots \\
merge\,(x_0, x_1, x_2, \ldots)\,(y_0, y_1, y_2, \ldots) &= x_0, y_0, x_1, y_1, x_2, y_2, \ldots
\end{aligned}
$$

$$evens\ (x_0, x_1, x_2, x_3, x_4, x_5, \ldots) = x_0, x_2, x_4, \ldots$$
$$odds\ (x_0, x_1, x_2, x_3, x_4, x_5, \ldots) = x_1, x_3, x_5, \ldots$$
$$merge\ (x_0, x_1, x_2, \ldots)\ (y_0, y_1, y_2, \ldots) = x_0, y_0, x_1, y_1, x_2, y_2, \ldots$$

$$\begin{aligned}
\mathrm{Head}(evens\ xs) &= \mathrm{Head}\ xs \\
\mathrm{Tail}(evens\ xs) &= odds\ (\mathrm{Tail}\ xs) \\
odds\ xs &= evens\ (\mathrm{Tail}\ xs)
\end{aligned}$$

$$\begin{aligned}
\mathrm{Head}(merge\ xs\ ys) &= \mathrm{Head}\ xs \\
\mathrm{Head}(\mathrm{Tail}(merge\ xs\ ys)) &= \mathrm{Head}\ ys \\
\mathrm{Tail}(\mathrm{Tail}(merge\ xs\ ys)) &= merge\ (\mathrm{Tail}\ xs)\ (\mathrm{Tail}\ ys)
\end{aligned}$$

Proof By Mutual Coinduction

Theorem

for all xs and ys, $\mathit{evens}\ (\mathit{merge}\ \mathit{xs}\ \mathit{ys}) = \mathit{xs}$ *AND* $\mathit{odds}\ (\mathit{merge}\ \mathit{xs}\ \mathit{ys}) = \mathit{ys}$

Proof. By mutual contextual stream equality:

$$
\begin{aligned}
\text{(Head)}\quad \mathrm{Head}(\mathit{evens}\ (\mathit{merge}\ \mathit{xs}\ \mathit{ys})) &= \mathrm{Head}(\mathit{merge}\ \mathit{xs}\ \mathit{ys}) = \mathrm{Head}\ \mathit{xs} \\
\mathrm{Head}(\mathit{odds}\ (\mathit{merge}\ \mathit{xs}\ \mathit{ys})) &= \mathrm{Head}(\mathit{evens}\ (\mathrm{Tail}(\mathit{merge}\ \mathit{xs}\ \mathit{ys}))) \\
&= \mathrm{Head}(\mathrm{Tail}(\mathit{merge}\ \mathit{xs}\ \mathit{ys})) = \mathrm{Head}\ \mathit{ys}
\end{aligned}
$$

Proof By Mutual Coinduction

Theorem

for all xs and ys, $evens\ (merge\ xs\ ys) = xs$ *AND* $odds\ (merge\ xs\ ys) = ys$

Proof. By mutual contextual stream equality:

(Head) $\mathrm{Head}(evens\ (merge\ xs\ ys)) = \mathrm{Head}(merge\ xs\ ys) = \mathrm{Head}\ xs$

$$\begin{aligned}\mathrm{Head}(odds\ (merge\ xs\ ys)) &= \mathrm{Head}(evens\ (\mathrm{Tail}(merge\ xs\ ys)))\\ &= \mathrm{Head}(\mathrm{Tail}(merge\ xs\ ys)) = \mathrm{Head}\ ys\end{aligned}$$

(Tail) $\forall xs, ys,\ CoIH_1 : h(evens(merge\ xs\ ys)) = h(xs)$, AND

$CoIH_2 : h(odds(merge\ xs\ ys)) = h(ys)$.

$$\begin{aligned}h(\mathrm{Tail}(evens\ (merge\ xs\ ys))) &= h(evens\ (\mathrm{Tail}(\mathrm{Tail}(merge\ xs\ ys))))\\ &= h(evens\ (merge\ (\mathrm{Tail}\ xs)\ (\mathrm{Tail}\ ys)))\\ &= h(\mathrm{Tail}\ xs) \qquad (CoIH_1[(\mathrm{Tail}\ xs)/xs, (\mathrm{Tail}\ ys)/ys])\end{aligned}$$

$$\begin{aligned}h(\mathrm{Tail}(odds\ (merge\ xs\ ys))) &= h(odds\ (\mathrm{Tail}(\mathrm{Tail}(merge\ xs\ ys))))\\ &= h(odds\ (merge\ (\mathrm{Tail}\ xs)\ (\mathrm{Tail}\ ys)))\\ &= h(\mathrm{Tail}\ ys) \qquad (CoIH_2[(\mathrm{Tail}\ xs)/xs, (\mathrm{Tail}\ ys)/ys])\end{aligned}$$

Proof By Strong Coinduction

Theorem

for all xs, $merge\ (evens\ xs)\ (odds\ xs) = xs.$

Proof. By strong contextual stream equality:

$$\text{(Head)} \quad \mathrm{Head}(merge\ (evens\ xs)\ (odds\ xs)) = \mathrm{Head}\ xs$$

$$\begin{aligned} \mathrm{Head}(merge\ (evens\ xs)\ (odds\ xs)) &= \mathrm{Head}(evens\ xs) \\ &= \mathrm{Head}\ xs \end{aligned}$$

Theorem

for all xs, $\mathit{merge}\ (\mathit{evens}\ \mathit{xs})\ (\mathit{odds}\ \mathit{xs}) = \mathit{xs}$.

Proof. By strong contextual stream equality:

(Head) $\quad \mathrm{Head}(\mathit{merge}\ (\mathit{evens}\ \mathit{xs})\ (\mathit{odds}\ \mathit{xs})) = \mathrm{Head}\ \mathit{xs}$

$$\begin{aligned}\mathrm{Head}(\mathit{merge}\ (\mathit{evens}\ \mathit{xs})\ (\mathit{odds}\ \mathit{xs})) &= \mathrm{Head}(\mathit{evens}\ \mathit{xs}) \\ &= \mathrm{Head}\ \mathit{xs}\end{aligned}$$

(Head ∘ Tail) $\quad \mathrm{Head}(\mathrm{Tail}(\mathit{merge}\ (\mathit{evens}\ \mathit{xs})\ (\mathit{odds}\ \mathit{xs}))) = \mathrm{Head}(\mathrm{Tail}\ \mathit{xs})$

$$\begin{aligned}\mathrm{Head}(\mathrm{Tail}(\mathit{merge}\ (\mathit{evens}\ \mathit{xs})\ (\mathit{odds}\ \mathit{xs}))) &= \mathrm{Head}(\mathit{odds}\ \mathit{xs}) \\ &= \mathrm{Head}(\mathit{evens}\ (\mathrm{Tail}\ \mathit{xs})) \\ &= \mathrm{Head}(\mathrm{Tail}\ \mathit{xs})\end{aligned}$$

Proof By Strong Coinduction

Theorem

for all xs, $merge\ (evens\ xs)\ (odds\ xs) = xs$.

Proof. By strong contextual stream equality:

(Tail ∘ Tail) Assume $CoIH : \forall xs,\ h(merge\ (evens\ xs)\ (odds\ xs)) = h(xs)$.

Show $\forall xs,\ h(\mathrm{Tail}(\mathrm{Tail}(merge\ (evens\ xs)\ (odds\ xs)))) = h(\mathrm{Tail}(\mathrm{Tail}\ xs))$.

$$
\begin{aligned}
& h(\mathrm{Tail}(\mathrm{Tail}(merge\ (evens\ xs)\ (odds\ xs)))) \\
&= h(merge\ (\mathrm{Tail}(evens\ xs))\ (\mathrm{Tail}(odds\ xs))) \\
&= h(merge\ (evens\ (\mathrm{Tail}(\mathrm{Tail}\ xs)))\ (odds\ (\mathrm{Tail}(\mathrm{Tail}\ xs))))
\end{aligned}
$$

□

Proof By Strong Coinduction

Theorem

for all xs, $merge\ (evens\ xs)\ (odds\ xs) = xs$.

Proof. By strong contextual stream equality:

(Tail ∘ Tail) Assume *CoIH* : $\forall xs,\ h(merge\ (evens\ xs)\ (odds\ xs)) = h(xs)$.

Show $\forall xs,\ h(\mathrm{Tail}(\mathrm{Tail}(merge\ (evens\ xs)\ (odds\ xs)))) = h(\mathrm{Tail}(\mathrm{Tail}\ xs))$.

$$\begin{aligned} & h(\mathrm{Tail}(\mathrm{Tail}(merge\ (evens\ xs)\ (odds\ xs)))) \\ &= h(merge\ (\mathrm{Tail}(evens\ xs))\ (\mathrm{Tail}(odds\ xs))) \\ &= h(merge\ (evens\ (\mathrm{Tail}(\mathrm{Tail}\ xs)))\ (odds\ (\mathrm{Tail}(\mathrm{Tail}\ xs)))) \end{aligned}$$

□

Proof By Strong Coinduction

...CONTINUED

Theorem

for all xs, $merge\ (evens\ xs)\ (odds\ xs) = xs.$

Proof. By strong contextual stream equality:

$(\mathrm{Tail} \circ \mathrm{Tail})$ Assume $\mathit{CoIH} : \forall xs,\ h(merge\ (evens\ xs)\ (odds\ xs)) = h(xs).$

Show $\forall xs,\ h(\mathrm{Tail}(\mathrm{Tail}(merge\ (evens\ xs)\ (odds\ xs)))) = h(\mathrm{Tail}(\mathrm{Tail}\ xs)).$

$$
\begin{aligned}
& h(\mathrm{Tail}(\mathrm{Tail}(merge\ (evens\ xs)\ (odds\ xs)))) \\
&= h(merge\ (\mathrm{Tail}(evens\ xs))\ (\mathrm{Tail}(odds\ xs))) \\
&= h(merge\ (evens\ (\mathrm{Tail}(\mathrm{Tail}\ xs)))\ (odds\ (\mathrm{Tail}(\mathrm{Tail}\ xs)))) \\
&= h(\mathrm{Tail}(\mathrm{Tail}\ xs)) && (\mathit{CoIH}[(\mathrm{Tail}(\mathrm{Tail}\ xs))/xs])
\end{aligned}
$$

$\square$

Coinductive Rules in Classical Logic

Consider property $P : \mathrm{Bool} \to \mathrm{Prop}$

Is $P(x)$ **true** for any value $x : \mathrm{Bool}$?

All the cases of x:

$$x = \mathrm{tt}$$

$$x = \mathrm{ff}$$

Consider property $P : \mathrm{Bool} \to \mathrm{Prop}$

Is $P(x)$ **true** for any value $x : \mathrm{Bool}$?

All the cases of x:

$x = \mathrm{tt}$

$x = \mathrm{ff}$

$$\frac{\Gamma \vdash P(\mathrm{tt}) \qquad \bullet \vdash P(\mathrm{ff})}{\Gamma, x : \mathrm{Bool} \vdash P(x)}\ \mathrm{Bool}\ \mathit{Ind}$$

$$\approx$$

$$P(\mathrm{tt}) \implies P(\mathrm{ff}) \implies \forall x : \mathrm{Bool} . P(x)$$

Consider property $P : \mathrm{Nat} \to \mathrm{Prop}$

Is $P(x)$ **true** for any value $x : \mathrm{Nat}$?

All the cases of x:

$$x = 0$$

$$x = 1$$

$$x = 2$$

$$\ldots$$

Consider property $P : \mathrm{Nat} \to \mathrm{Prop}$

Is $P(x)$ **true** for any value $x : \mathrm{Nat}$?

All the cases of x:

$x = 0$

$x = 1$

$x = 2$

$\dots$

$$\frac{\Gamma \vdash P(0) \quad \Gamma \vdash P(1) \quad \Gamma \vdash P(2) \quad \dots}{\Gamma, x : \mathrm{Nat} \vdash P(x)}$$

Consider property $P : \mathrm{Nat} \to \mathrm{Prop}$

Is $P(x)$ **true** for any value $x : \mathrm{Nat}$?

All the cases of x:

$x = 0$

$x = y + 1$ for some other $y : \mathrm{Nat}$

$$\frac{\Gamma \vdash P(0) \qquad \Gamma, y : \mathrm{Nat}, P(y) \vdash P(y+1)}{\Gamma, x : \mathrm{Nat} \vdash P(x)}\ \mathrm{Nat}\ \mathit{Ind}$$

$$P(0) \implies (\forall y : \mathrm{Nat}\,.\,P(y) \implies P(y+1)) \implies \forall x : \mathrm{Nat}\,.\,P(x)$$

Making Coinduction Less Vicious

$$\frac{\Gamma, xs : \mathrm{Stream}\ A,\ P(xs) \vdash P(xs)}{\Gamma, xs : \mathrm{Stream}\ A \vdash P(xs)}\ \textit{vicious}!$$

$$\frac{\Gamma, xs : \mathrm{Stream}\ A, P(xs) \vdash P(xs)}{\Gamma, xs : \mathrm{Stream}\ A \vdash P(xs)}\ \textit{vicious!}$$

$$\frac{xs : \mathrm{Stream}\ A \vdash P\left(\begin{array}{l}\mathrm{Head}\ xs, \mathrm{Head}(\mathrm{Tail}\ xs),\\ \mathrm{Head}(\mathrm{Tail}(\mathrm{Tail}\ xs)), \ldots\end{array}\right)}{xs : \mathrm{Stream}\ A \vdash P(xs)}$$

$$\frac{\Gamma, xs : \text{Stream}\ A, P(xs) \vdash P(xs)}{\Gamma, xs : \text{Stream}\ A \vdash P(xs)}\ \textit{vicious!}$$

$$\frac{xs : \text{Stream}\ A \vdash P\begin{pmatrix}\text{Head}\ xs, \text{Head}(\text{Tail}\ xs),\\ \text{Head}(\text{Tail}(\text{Tail}\ xs)), \ldots\end{pmatrix}}{xs : \text{Stream}\ A \vdash P(xs)}$$

Key Idea: Move focus away from stream values $xs : \text{Stream}\ A$, and consider the cases for any observation $\alpha \div \text{Stream}\ A$ that might look at xs

The Structure of Observations

And observation $\alpha \div \mathit{StreamA}$ of streams might be:

$$
\begin{aligned}
\alpha &= \mathsf{Head} && \text{(observe element 0)} \\
\alpha &= \mathsf{Head} \circ \mathsf{Tail} && \text{(observe element 1)} \\
\alpha &= \mathsf{Head} \circ \mathsf{Tail} \circ \mathsf{Tail} && \text{(observe element 2)} \\
\alpha &= \mathsf{Head} \circ \mathsf{Tail} \circ \mathsf{Tail} \circ \mathsf{Tail} && \text{(observe element 3)} \\
&\dots \\
\alpha &= \mathsf{Head} \circ \mathsf{Tail}^{i} && \text{(observe element } i\text{)} \\
&\dots
\end{aligned}
$$

And observation $\alpha \div \mathit{StreamA}$ of streams might be:

$$
\begin{aligned}
\alpha &= \mathsf{Head} && \text{(observe element 0)} \\
\alpha &= \mathsf{Head} \circ \mathsf{Tail} && \text{(observe element 1)} \\
\alpha &= \mathsf{Head} \circ \mathsf{Tail} \circ \mathsf{Tail} && \text{(observe element 2)} \\
\alpha &= \mathsf{Head} \circ \mathsf{Tail} \circ \mathsf{Tail} \circ \mathsf{Tail} && \text{(observe element 3)} \\
&\ldots \\
\alpha &= \mathsf{Head} \circ \mathsf{Tail}^{i} && \text{(observe element } i\text{)} \\
&\ldots
\end{aligned}
$$

ALL stream observations $\alpha \div \mathit{StreamA}$ are one of:

$$
\begin{aligned}
\alpha &= \beta \circ \mathsf{Head} && \text{for some observation } \beta \div A\text{, or} \\
\alpha &= \delta \circ \mathsf{Tail} && \text{for some other } \delta \div \mathsf{Stream}\, A
\end{aligned}
$$

A Coinduction Principle

Consider property $P : -\ \mathsf{Stream}\ A \to \mathsf{Prop}$

Is $P(\alpha)$ **true** for any observation $\alpha \div \mathsf{Stream}\ A$

All the cases of α:

$\alpha = \beta \circ \mathsf{Head}$ for some observation $\beta \div A$

$\alpha = \delta \circ \mathsf{Tail}$ for some other $\delta \div \mathsf{Stream}\ A$

$$\frac{\Gamma, \beta \div A \vdash P(\beta \circ \mathsf{Head}) \qquad \Gamma, \delta \div \mathsf{Stream}\ A, P(\delta) \vdash P(\delta \circ \mathsf{Tail})}{\Gamma, \alpha \div \mathsf{Stream}\ A \vdash P(\alpha)}\ \mathsf{Stream}\ \mathit{CoInd}$$

$$\begin{array}{l}(\forall \beta \div A.\ P(\beta \circ \mathsf{Head})) \implies \\ (\forall \delta \div \mathsf{Stream}\ A.\ P(\delta) \implies P(\delta \circ \mathsf{Tail})) \implies \\ \forall \alpha \div \mathsf{Stream}\ A.\ P(\alpha)\end{array}$$

But What About Bisimulation?

Given any binary relation $R : \mathsf{Stream}\, A \times \mathsf{Stream}\, A \to \mathsf{Prop}$,

$$
\begin{aligned}
&(\forall xs, ys : \mathsf{Stream}\, A.\ R(xs, ys) \implies \mathsf{Head}\, xs = \mathsf{Head}\, ys) \implies \\
&(\forall xs, ys : \mathsf{Stream}\, A.\ R(xs, ys) \implies R(\mathsf{Tail}\, xs, \mathsf{Tail}\, ys)) \implies \\
&\ \forall xs, ys.\ R(xs, ys) \implies xs = ys
\end{aligned}
$$

But What About Bisimulation?

Given any binary relation $R : \text{Stream}\,A \times \text{Stream}\,A \to \text{Prop}$,

$$(\forall xs, ys : \text{Stream}\,A.\ R(xs, ys) \implies \text{Head}\,xs = \text{Head}\,ys) \implies$$
$$(\forall xs, ys : \text{Stream}\,A.\ R(xs, ys) \implies R(\text{Tail}\,xs, \text{Tail}\,ys)) \implies$$
$$\forall xs, ys.\ R(xs, ys) \implies xs = ys$$

Bisimulation is derivable from Stream *CoInd* with help from observational equivalence:

$$\frac{\Gamma, \alpha \div A \vdash \langle v \| \alpha \rangle = \langle w \| \alpha \rangle}{\Gamma \vdash v = w : A}\ \mathit{Obs.Equiv.}$$

$\langle v \| \alpha \rangle$ is a computation where α observes v:

$$\frac{\Gamma \vdash v : A \quad \Gamma \vdash \alpha \div A}{\Gamma \vdash \langle v \| \alpha \rangle}\ \mathit{Cut}$$

Computing With Contextual Coinduction

Dualities of Computation

Embodying the Context

$$\xRightarrow{\text{Answers}}$$

$$\langle v \| e \rangle$$

$$\xLeftarrow[\text{Questions}]{}$$

A producer v gives an answer

A consumer e asks a question

A command $\langle v \| e \rangle$ is an interaction

- One side moves first in a predictable <u>pattern</u>
- The other side <u>responds</u> to first move

Data = patterns of answers

Codata = patterns of questions

A call stack $\boxed{x \cdot \alpha}$ contains an:

argument x

return pointer α

map is well-founded because its argument shrinks:

$$
\begin{aligned}
\langle map \| f \cdot \mathsf{Nil} \cdot \alpha \rangle &= \langle \mathsf{Nil} \| \alpha \rangle \\
\langle map \| f \cdot \boxed{\mathsf{Cons}\; x\; xs} \cdot \alpha \rangle &= \langle map \| f \cdot \boxed{xs} \cdot \alpha \circ \mathsf{Cons}(f\; x) \rangle
\end{aligned}
$$

repeat is well-founded because its return pointer shrinks:

$$
\begin{aligned}
\langle repeat \| f \cdot x \cdot \alpha \circ \mathsf{Head} \rangle &= \langle x \| \alpha \rangle \\
\langle repeat \| f \cdot x \cdot \boxed{\alpha \circ \mathsf{Tail}} \rangle &= \langle repeat \| f \cdot f\; x \cdot \boxed{\alpha} \rangle
\end{aligned}
$$

More Adventurous Structural (Co)Recursion

evens and *odds* are mutually well-founded because *even*'s return pointer always shrinks and *odds* return pointer stays the same:

$$\begin{aligned}
\langle \mathit{evens} \| \mathit{xs} \cdot \alpha \circ \mathrm{Head} \rangle &= \langle \mathit{xs} \| \alpha \circ \mathrm{Head} \rangle \\
\left\langle \mathit{evens} \middle\| \mathit{xs} \cdot \boxed{\alpha \circ \mathrm{Tail}} \right\rangle &= \langle \mathit{odds} \| \mathrm{Tail}\ \mathit{xs} \cdot \boxed{\alpha} \rangle \\
\langle \mathit{odds} \| \mathit{xs} \cdot \boxed{\alpha} \rangle &= \langle \mathit{evens} \| \mathrm{Tail}\ \mathit{xs} \cdot \boxed{\alpha} \rangle
\end{aligned}$$

merge is well-founded by strong corecursion because its return pointer shrinks by 2, and the first 2 base cases are covered:

$$\begin{aligned}
\langle \mathit{merge} \| \mathit{xs} \cdot \mathit{ys} \cdot \alpha \circ \mathrm{Head} \rangle &= \langle \mathit{xs} \| \alpha \circ \mathrm{Head} \rangle \\
\langle \mathit{merge} \| \mathit{xs} \cdot \mathit{ys} \cdot \alpha \circ \mathrm{Head} \circ \mathrm{Tail} \rangle &= \langle \mathit{ys} \| \alpha \circ \mathrm{Head} \rangle \\
\left\langle \mathit{merge} \middle\| \mathit{xs} \cdot \mathit{ys} \cdot \boxed{\alpha \circ \mathrm{Tail} \circ \mathrm{Tail}} \right\rangle &= \langle \mathit{merge} \| \mathrm{Tail}\ \mathit{xs} \cdot \mathrm{Tail}\ \mathit{ys} \cdot \boxed{\alpha} \rangle
\end{aligned}$$

Theorem
If $\Gamma \vdash \langle v_1 \| e_1 \rangle = \langle v_2 \| e_2 \rangle$, *then* $\langle v_1 \| e_1 \rangle$ *and* $\langle v_2 \| e_2 \rangle$ *are contextually equivalent (as usual, per the operational semantics).*

Proof.
By a logical relation based on orthogonal fixed points in a subtyping lattice. Key: Knaster-Tarski and Kleene fixed points coincide. □

Consistency of Equality

Theorem
If $\Gamma \vdash \langle v_1 \| e_1 \rangle = \langle v_2 \| e_2 \rangle$*, then* $\langle v_1 \| e_1 \rangle$ *and* $\langle v_2 \| e_2 \rangle$ *are contextually equivalent (as usual, per the operational semantics).*

Proof.
By a logical relation based on orthogonal fixed points in a subtyping lattice. Key: Knaster-Tarski and Kleene fixed points coincide. □

Corollary
If $\alpha \div \mathrm{Bool} \vdash \langle v_1 \| e_2 \rangle = \langle v_2 \| e_2 \rangle$*, then either*

$$\langle v_1 \| e_2 \rangle \mapsto\!\!\!\!\twoheadrightarrow \langle \mathrm{tt} \| \alpha \rangle \twoheadleftarrow\!\!\!\!\leftarrowtail \langle v_2 \| e_2 \rangle \text{ or}$$

$$\langle v_1 \| e_2 \rangle \mapsto\!\!\!\!\twoheadrightarrow \langle \mathrm{ff} \| \alpha \rangle \twoheadleftarrow\!\!\!\!\leftarrowtail \langle v_2 \| e_2 \rangle.$$

Corollary
$\bullet \vdash \mathrm{tt} = \mathrm{ff} : \mathrm{Bool}$ *is not derivable.*

What about effects?

Programs can do some funny things

Conventional side effects

- Mutable state / references
- Input / Output
- Exceptions and Jumps
- Infinite loops

Suprising wringle: Information effects

- Dual to control effects (manipulating control flow)
- Erasing answers
- Duplicating answers

Both can cause (co)inductive reasoning principles to go awry

- For example, they can cause inconsistency

(Co)Induction and Evaluation Strategy

Adjusting Strength to Save Consistency

Induction principles (like Nat *Ind*) + Effects are

Fully consistent under call-by-value evaluation

Safe for strict properties in call-by-name evaluation

$$\begin{array}{lll} \mathit{Strict\ on}\ x \ni \quad \Psi(x) ::= \langle x \| E \rangle = \langle x \| E' \rangle & & (E, E' \in \mathit{Eval.Cxt.}) \\ \qquad\qquad\qquad\qquad \mid \forall y : A.\ \Psi(x) & & (x \neq y) \\ \qquad\qquad\qquad\qquad \mid P \implies \Psi(x) & & (x \notin FV(P)) \\ \qquad\qquad\qquad\qquad \mid \dots & & \end{array}$$

Induction principles (like Nat *Ind*) + Effects are

Fully consistent under call-by-value evaluation

Safe for strict properties in call-by-name evaluation

$$\begin{array}{llr} \textit{Strict on } x \ni \quad \Psi(x) ::= \langle x \| E \rangle = \langle x \| E' \rangle & & (E, E' \in \mathit{Eval.Cxt.}) \\ \qquad\qquad \mid \forall y : A.\ \Psi(x) & & (x \neq y) \\ \qquad\qquad \mid P \implies \Psi(x) & & (x \notin FV(P)) \\ \qquad\qquad \mid \ldots & & \end{array}$$

Coinduction principles (like Stream *CoInd*) + Effects are

Fully consistent under call-by-name evaluation

Safe for productive properties in call-by-value evaluation

$$\begin{array}{llr} \textit{Productive on } \alpha \ni \quad \Psi(\alpha) ::= \langle V \| \alpha \rangle = \langle V' \| \alpha \rangle & & (V, V' \in \mathit{Value}) \\ \qquad\qquad \mid \forall \beta \div A.\ \Psi(\alpha) & & (\alpha \neq \beta) \\ \qquad\qquad \mid P \implies \Psi(\alpha) & & (\alpha \notin FV(P)) \\ \qquad\qquad \mid \ldots & & \end{array}$$

Answers

$$\Longrightarrow$$

$$\langle \mathit{Me} \| \mathit{You} \rangle$$

$$\Longleftarrow$$

Questions

Downen & Ariola, Structures for Structural Recursion, ICFP '16.

Downen & Ariola, A Computational Understanding of Classical (Co)Recursion, PPDP '20.

Downen & Ariola, Classical (Co)Recursion: Programming, ArXiv '21.

Downen & Ariola, Classical (Co)Recursion: Mechanics, Journal of Func. Prog. '23.

Table of Contents