A Contextual Formalization of Structural Coinduction

Paul Downen and Zena M. Ariola

ICFP — Monday, October 13, 2025

Interacting With Others

Induction has been the workhorse of PL in theory & practice

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

- Operating systems & User Interfaces
- Web servers & Networks
- Control software & robotics
- …

Coinduction also arises in semantics of languages

- Bisimulation & (potentially) infinite processes
- Interaction trees & effects
- Automata & formal languages

Coinduction for Modern Computer Science

Induction has been the workhorse of PL in theory & practice

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

- Operating systems & User Interfaces
- Web servers & Networks
- Control software & robotics
- ...

Coinduction also arises in semantics of languages

- Bisimulation & (potentially) infinite processes
- Interaction trees & effects
- Automata & formal languages

So let's just use coinduction like we do induction!

What's So Hard About Coinduction?

An Old-Fashioned Pen-and-Paper Proof

$$map : (a \to b) \to \text{Stream}\, a \to \text{Stream}\, b$$
$$map\ f\ xs = \text{More}\ (f\ (\text{Head}\, xs))\ (map\ f\ (\text{Tail}\, xs))$$

Theorem
For all $xs : \text{Stream}\, a$, $map\ id\ xs = xs$.

Proof. By general coinduction.
Assume the CoIH: $map\ id\ xs = xs$. …

An Old-Fashioned Pen-and-Paper Proof

The "Hello, World!" of coinduction

$$map : (a \to b) \to \text{Stream}\ a \to \text{Stream}\ b$$
$$map\ f\ xs = \text{More}\ (f\ (\text{Head}\ xs))\ (map\ f\ (\text{Tail}\ xs))$$

Theorem
For all $xs : \text{Stream}\ a$, *$map\ id\ xs = xs$.*

Proof. By general coinduction.
Assume the CoIH: $map\ id\ xs = xs$.

Then by CoIH, already know $map\ id\ xs = xs$. Easy! ☒

Obviously that won't do! Need to do some work…

An Old-Fashioned Pen-and-Paper Proof

$$map : (a \to b) \to \mathsf{Stream}\ a \to \mathsf{Stream}\ b$$
$$map\ f\ xs = \mathsf{More}\ (f\ (\mathsf{Head}\ xs))\ (map\ f\ (\mathsf{Tail}\ xs))$$

Theorem
For all $xs : \mathsf{Stream}\ a$, $map\ id\ xs = xs$.

Proof. By general coinduction.
Assume the CoIH: $map\ id\ xs = xs$.

$$\begin{aligned}
\underline{map\ id\ xs} &= \mathsf{More}\ (\underline{id(\mathsf{Head}\ xs)})\ (map\ id\ (\mathsf{Tail}\ xs)) && (map)\\
&= \mathsf{More}\ (\mathsf{Head}\ xs)\ (\underline{map\ id\ (\mathsf{Tail}\ xs)}) && (id)\\
&= \underline{\mathsf{More}\ (\mathsf{Head}\ xs)\ (\mathsf{Tail}\ xs)} && (CoIH)\\
&= xs && (\eta) \qquad \square
\end{aligned}$$

What's different this time?

An Old-Fashioned Pen-and-Paper Proof

$$map : (a \to b) \to \mathsf{Stream}\ a \to \mathsf{Stream}\ b$$
$$map\ f\ xs = \mathsf{More}\ (f\ (\mathsf{Head}\ xs))\ (map\ f\ (\mathsf{Tail}\ xs))$$

Theorem
For all $xs : \mathsf{Stream}\ a$, $map\ id\ xs = xs$.

Proof. By general coinduction.
Assume the CoIH: $map\ id\ xs = xs$.

$$\begin{aligned}
\underline{map\ id\ xs} &= \mathsf{More}\ (\underline{id(\mathsf{Head}\ xs)})\ (map\ id\ (\mathsf{Tail}\ xs)) && (map)\\
&= \mathsf{More}\ (\mathsf{Head}\ xs)\ (\underline{map\ id\ (\mathsf{Tail}\ xs)}) && (id)\\
&= \underline{\mathsf{More}\ (\mathsf{Head}\ xs)\ (\mathsf{Tail}\ xs)} && (CoIH)\\
&= xs && (\eta) \qquad \square
\end{aligned}$$

What's different this time? The CoIH is only used in a productive context.

A Miraculous Discovery!

$$\mathit{always} : a \to \mathsf{Stream}\, a \qquad\qquad \mathit{always}\ x = \mathsf{More}\ \ x\ (\mathit{always}\ x)$$

Theorem
$\mathsf{More}\, 0\ (\mathit{always}\ 1) = \mathit{always}\ 0.$ *Corollary:* $1 = 0.$

Proof. By general coinduction.
Assume the CoIH: $\mathsf{More}\, 0\ (\mathit{always}\ 1) = \mathit{always}\ 0.$ $\ldots$

A Miraculous Discovery!

$$always : a \to \text{Stream}\ a \qquad\qquad always\ x = \text{More}\ \ x\ (always\ x)$$

Theorem
More 0 $(always\ 1) = always\ 0.$ *Corollary:* $1 = 0.$

Proof. By general coinduction.
Assume the CoIH: More 0 $(always\ 1) = always\ 0$.

$$
\begin{aligned}
&\text{More}\,0\ (\underline{always\ 1}) \\
&= \text{More}\,0\ (\text{Tail}(\underline{\text{More}\,0\ (always\ 1)})) && (\text{Tail}^{-1}) \\
&= \text{More}\,0\ (\text{Tail}(\underline{always\ 0})) && (CoIH) \\
&= \text{More}\,0\ (\underline{\text{Tail}(\text{More}\,0\ (always\ 0))}) && (always) \\
&= \underline{\text{More}\,0\ (always\ 0)} && (\text{Tail}) \\
&= always\ 0 && (always^{-1}) \qquad \square
\end{aligned}
$$

What went wrong??

A Miraculous Discovery!

$$\mathit{always} : a \to \mathsf{Stream}\, a \qquad\qquad \mathit{always}\ x = \mathsf{More}\ \ x\ (\mathit{always}\ x)$$

Theorem
$\mathsf{More}\, 0\ (\mathit{always}\ 1) = \mathit{always}\ 0.$ *Corollary:* $1 = 0.$

Proof. By general coinduction.
Assume the CoIH: $\mathsf{More}\, 0\ (\mathit{always}\ 1) = \mathit{always}\ 0.$

$$\begin{aligned}
& \mathsf{More}\, 0\ (\underline{\mathit{always}\ 1}) \\
&= \mathsf{More}\, 0\ (\mathsf{Tail}(\underline{\mathsf{More}\, 0\ (\mathit{always}\ 1)})) && (\mathsf{Tail}^{-1}) \\
&= \mathsf{More}\, 0\ (\mathsf{Tail}(\underline{\mathit{always}\ 0})) && (\mathit{CoIH}) \\
&= \mathsf{More}\, 0\ (\underline{\mathsf{Tail}(\mathsf{More}\, 0\ (\mathit{always}\ 0))}) && (\mathit{always}) \\
&= \underline{\mathsf{More}\, 0\ (\mathit{always}\ 0)} && (\mathsf{Tail}) \\
&= \mathit{always}\ 0 && (\mathit{always}^{-1}) \qquad \square
\end{aligned}$$

What went wrong?? The CoIH looked productive, but it wasn't.

Coinduction via Productivity is Subtle

The coinductive hypothesis (CoIH) is too powerful

Status quo: avoid vicious cycles by using CoIH in good contexts

"Good" and "bad" contexts have subtle semantic content

Possible if your proof has a certain "shape"

- Calculations have obvious contexts around axiom use
- Good luck analyzing the "context" in a paragraph of prose

Proof assistants can help sort out good contexts from bad

Coinduction via Productivity is Subtle

The coinductive hypothesis (CoIH) is too powerful

Status quo: avoid vicious cycles by using CoIH in good contexts

"Good" and "bad" contexts have subtle semantic content

Possible if your proof has a certain "shape"

- Calculations have obvious contexts around axiom use
- Good luck analyzing the "context" in a paragraph of prose

Proof assistants can help sort out good contexts from bad

...using (rigidly) syntactic approximations of semantics

A Frustrating Proof in Rocq

I hope you like poring over auto-generated proof terms...

```
CoInductive Stream A : Type := More { Head : A ; Tail : Stream A }.

CoFixpoint map {A} {B} (f : A -> B) xs := More (f (Head xs)) (map f (Tail xs)).

CoInductive StreamEq {A} (xs ys : Stream A) : Prop :=
  MoreEq { HeadEq : Head xs = Head ys;
           TailEq : StreamEq (Tail xs) (Tail ys) }.
```

A Frustrating Proof in Rocq

I hope you like poring over auto-generated proof terms...

```
CoInductive Stream A : Type := More { Head : A ; Tail : Stream A }.

CoFixpoint map {A} {B} (f : A -> B) xs := More (f (Head xs)) (map f (Tail xs)).

CoInductive StreamEq {A} (xs ys : Stream A) : Prop :=
  MoreEq { HeadEq : Head xs = Head ys;
           TailEq : StreamEq (Tail xs) (Tail ys) }.
```

```
Theorem map_id1
  : forall {A} (xs : Stream A),
    StreamEq (map id xs) xs.
Proof.
  intro A.
  intro xs.
  cofix CoIH.
  apply MoreEq.
  * reflexivity.
  * apply CoIH.
Qed.
```

```
Theorem map_id2
  : forall {A} (xs : Stream A),
    StreamEq (map id xs) xs.
Proof.
  intro A.
  cofix CoIH.
  intro xs.
  apply MoreEq.
  * reflexivity.
  * apply CoIH.
Qed.
```

A Frustrating Proof in Rocq

I hope you like poring over auto-generated proof terms...

```
CoInductive Stream A : Type := More { Head : A ; Tail : Stream A }.

CoFixpoint map {A} {B} (f : A -> B) xs := More (f (Head xs)) (map f (Tail xs)).

CoInductive StreamEq {A} (xs ys : Stream A) : Prop :=
  MoreEq { HeadEq : Head xs = Head ys;
           TailEq : StreamEq (Tail xs) (Tail ys) }.
```

```
Theorem map_id1
  : forall {A} (xs : Stream A),
    StreamEq (map id xs) xs.
Proof.
  intro A.
  intro xs.
  cofix CoIH.
  apply MoreEq.
  * reflexivity.
  * apply CoIH.
Qed.
```

No more goals.

```
Theorem map_id2
  : forall {A} (xs : Stream A),
    StreamEq (map id xs) xs.
Proof.
  intro A.
  cofix CoIH.
  intro xs.
  apply MoreEq.
  * reflexivity.
  * apply CoIH.
Qed.
```

No more goals.

A Frustrating Proof in Rocq

I hope you like poring over auto-generated proof terms...

```
CoInductive Stream A : Type := More { Head : A ; Tail : Stream A }.

CoFixpoint map {A} {B} (f : A -> B) xs := More (f (Head xs)) (map f (Tail xs)).

CoInductive StreamEq {A} (xs ys : Stream A) : Prop :=
  MoreEq { HeadEq : Head xs = Head ys;
           TailEq : StreamEq (Tail xs) (Tail ys) }.
```

```
Theorem map_id1
  : forall {A} (xs : Stream A),
    StreamEq (map id xs) xs.
Proof.
  intro A.
  intro xs.
  cofix CoIH.
  apply MoreEq.
  * reflexivity.
  * apply CoIH.
Qed.
```

No more goals.

Error: …CoIH is ill-formed…

```
Theorem map_id2
  : forall {A} (xs : Stream A),
    StreamEq (map id xs) xs.
Proof.
  intro A.
  cofix CoIH.
  intro xs.
  apply MoreEq.
  * reflexivity.
  * apply CoIH.
Qed.
```

No more goals.

Ok. ◡̈

Liberating Structural Coinduction from Syntax

Making coinduction as straightforward as induction outside a proof assistant

Want: A coinduction principle useful for informal proofs, pen-and-paper prose style, with the same confidence as structural induction

No question when the Inductive Hypothesis applies, even in informal contexts:

$$\text{assume } \mathit{IH} : P(n) \qquad\qquad \text{prove } \mathit{Goal} : P(n+1)$$

The usual basis of coinduction is begging the question:

$$\text{assume } \mathit{CoIH} : P(xs) \qquad\qquad \text{prove } \mathit{Goal} : P(xs)$$

Need: A re-formulation of the CoInductive Hypothesis that

(1) Can be checked for valid applications immediately
(2) Is not dependent on a particular syntax / proof context
(3) Gives an axiom that is sound by definition without secondary syntactic checks

Coinduction With Confidence

What is the Principle Behind Copatterns?

Restoring the structure to structural (co)induction

```
record Stream (A : Set) : Set where
  coinductive
  field Head : A
        Tail : Stream A

map : ∀ {A B} → (A → B) → Stream A → Stream B
map f xs .Head = f (xs .Head)
map f xs .Tail = map f (xs .Tail)

record Stream_≈_ {A} (xs ys : Stream A) : Set where
  coinductive
  field Head : xs .Head ≡ ys .Head
        Tail : Stream xs .Tail ≈ ys .Tail

map-id : ∀ {A} (xs : Stream A) → Stream map id xs ≈ xs
map-id xs .Head = refl
map-id xs .Tail = map-id (xs .Tail)
```

Principle (Induction on Natural Number Values)

Property P holds on all natural number values $n : \mathrm{Nat}$ (i.e., $P(n)$) if and only if

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

Main idea 1: Coinduction = Induction on the Observing Context

Principle (Induction on Natural Number Values)

Property P holds on all natural number values $n : \mathrm{Nat}$ (i.e., $P(n)$) if and only if

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

Principle (Coinduction on Stream Observations*)

Property P holds on all stream observations $f : \mathrm{Stream}\, A \rightsquigarrow B$ (i.e., $P(f)$) if and only if

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

Principle (Induction on Natural Number Values)

Property P holds on all natural number values $n : \mathrm{Nat}$ (i.e., $P(n)$) if and only if

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

Principle (Coinduction on Stream Observations*)**

Property P holds on all stream observations $f : \mathrm{Stream}\ A \rightsquigarrow B$ (i.e., $P(f)$) if and only if

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

Coinductive Contextual Equivalence

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

$$x = y$$

if and only if

for all observations f, $f(x) = f(y)$.

Coinductive Contextual Equivalence

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

$$x = y$$

if and only if

for all observations f, $f(x) = f(y)$.

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

$$xs = ys$$

if and only if

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

and

for all obs. h, $h(xs) = h(ys)$ implies $h(\mathrm{Tail}(xs)) = h(\mathrm{Tail}(ys))$

Coinductive Contextual Equivalence

Main idea 2: Sound Coinductive Hypothesis = Labeling the Observer

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

$$x = y$$

if and only if

for all observations f, $f(x) = f(y)$.

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

$$xs = ys$$

if and only if

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

and

for all obs. h, $h(xs) = h(ys)$ implies $h(\mathrm{Tail}(xs)) = h(\mathrm{Tail}(ys))$

Proof. By Contextual Equivalence + Coinduction on Stream Observations, where $P(f) = (f(xs) = f(ys))$. □

Coinductive Contextual Equivalence

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

$$x = y$$

$$\textit{if and only if}$$

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

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

$$xs = ys$$

$$\textit{if and only if}$$

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

$$\textit{and}$$

$$\textit{for all obs. } h,\ h(xs) = h(ys)\ \textit{implies}\ h(\mathsf{Tail}(xs)) = h(\mathsf{Tail}(ys))$$

Proof. By Contextual Equivalence + Coinduction on Stream Observations, where $P(f) = (f(xs) = f(ys))$. □

An Informal Proof By Contextual Stream Equality

Now with more confidence!

$$\mathrm{Head}(\mathit{map}\, f\ x) = f\ (\mathrm{Head}\, x) \qquad \mathrm{Tail}(\mathit{map}\, f\ x) = \mathit{map}\, f\ (\mathrm{Tail}\, x)$$

Theorem
map id xs $=$ *map id xs*

Proof. By contextual stream equality:

(Head) Show $\mathrm{Head}(\mathit{map}\ \mathit{id}\ \mathit{xs}) = \mathrm{Head}(\mathit{xs})$

$$\mathrm{Head}(\mathit{map}\ \mathit{id}\ \mathit{xs}) = \mathit{id}(\mathrm{Head}(\mathit{xs})) = \mathrm{Head}(\mathit{xs}) \qquad (\mathrm{Head} \circ \mathit{map}, \mathit{id})$$

An Informal Proof By Contextual Stream Equality

Now with more confidence!

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

Theorem
map id xs $=$ *map id xs*

Proof. By contextual stream equality:

(Head) Show $\text{Head}(map\ id\ xs) = \text{Head}(xs)$

$$\text{Head}(map\ id\ xs) = id(\text{Head}(xs)) = \text{Head}(xs) \qquad (\text{Head} \circ map,\ id)$$

(Tail) Assume CoIH: $h(map\ id\ xs) = h(xs)$.
Show $h(\text{Tail}(map\ id\ xs)) = h(\text{Tail}(xs))$.

$$\begin{aligned} h(\underline{\text{Tail}(map\ id\ xs)}) &= \underline{h(map\ id\ (\text{Tail}(xs)))} && (\text{Tail} \circ map) \\ &= h(\text{Tail}(xs)) && (\mathit{CoIH}) \end{aligned}$$

$\square$

An Informal Proof By Contextual Stream Equality

Now with more confidence!

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

Theorem
$\mathit{map}\ \mathit{id}\ \mathit{xs} = \mathit{map}\ \mathit{id}\ \mathit{xs}$

Proof. By contextual stream equality:

(Head) Show $\mathrm{Head}(\mathit{map}\ \mathit{id}\ \mathit{xs}) = \mathrm{Head}(\mathit{xs})$

$$\mathrm{Head}(\mathit{map}\ \mathit{id}\ \mathit{xs}) = \mathit{id}(\mathrm{Head}(\mathit{xs})) = \mathrm{Head}(\mathit{xs}) \qquad (\mathrm{Head} \circ \mathit{map}, \mathit{id})$$

(Tail) Assume CoIH: $h(\mathit{map}\ \mathit{id}\ \mathit{xs}) = h(\mathit{xs})$.
Show $h(\mathrm{Tail}(\mathit{map}\ \mathit{id}\ \mathit{xs})) = h(\mathrm{Tail}(\mathit{xs}))$.

$$\begin{aligned} h(\underline{\mathrm{Tail}(\mathit{map}\ \mathit{id}\ \mathit{xs})}) &= \underline{h(\mathit{map}\ \mathit{id}\ (\mathrm{Tail}(\mathit{xs})))} && (\mathrm{Tail} \circ \mathit{map}) \\ &= h(\mathrm{Tail}(\mathit{xs})) && (\mathit{CoIH}) \qquad \square \end{aligned}$$

The "guard" is now <u>explicitly</u> part of CoIH! It <u>can't</u> be misapplied!

Stopping Incorrect Steps As Soon As They Happen

Can't use the CoIH in the wrong context!

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

Theorem
$\mathrm{More}\,0\ (\mathit{always}\ 1) = \mathit{always}\ 0$

Proof (attempt). By contextual stream equality:

(Head) Show $\mathrm{Head}(\mathrm{More}\,0\ (\mathit{always}\ 1)) = \mathrm{Head}(\mathit{always}\ 0)$.

$$\begin{aligned} \mathrm{Head}(\mathrm{More}\,0\ (\mathit{always}\ 1)) &= 0 && (\mathrm{Head} \circ \mathrm{More}) \\ &= \mathrm{Head}(\mathit{always}\ 0) && (\mathrm{Head} \circ \mathit{always}^{-1}) \end{aligned}$$

Stopping Incorrect Steps As Soon As They Happen

Can't use the CoIH in the wrong context!

$$\text{Head}(\textit{always}\ x) = x \qquad\qquad \text{Tail}(\textit{always}\ x) = \textit{always}\ x$$

Theorem
$\text{More}\,0\ (\textit{always}\ 1) = \textit{always}\ 0$

Proof (attempt). By contextual stream equality:

(Head) Show $\text{Head}(\text{More}\,0\ (\textit{always}\ 1)) = \text{Head}(\textit{always}\ 0)$.

$$\begin{aligned} \text{Head}(\text{More}\,0\ (\textit{always}\ 1)) &= 0 && (\text{Head} \circ \text{More}) \\ &= \text{Head}(\textit{always}\ 0) && (\text{Head} \circ \textit{always}^{-1}) \end{aligned}$$

(Tail) Assume CoIH: $h(\text{More}\,0\ (\textit{always}\ 1)) = h(\textit{always}\ 0)$.
Show $h(\text{Tail}(\text{More}\,0\ (\textit{always}\ 1))) = h(\text{Tail}(\textit{always}\ 0))$.

$$\begin{aligned} & h(\text{Tail}(\text{More}\,0\ (\underline{\textit{always}\ 1}))) \\ &= h(\text{Tail}(\text{More}\,0\ (\text{Tail}(\underline{\text{More}\,0\ (\textit{always}\ 1)})))()) && (\text{Tail} \circ \text{More}^{-1}) \\ &\neq \ldots && (\textit{CoIH}) \qquad \boxtimes \end{aligned}$$

Stopping Incorrect Steps As Soon As They Happen

Can't use the CoIH in the wrong context!

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

Theorem
$\mathrm{More}\,0\ (\mathit{always}\ 1) = \mathit{always}\ 0$

Proof (attempt). By contextual stream equality:

(Head) Show $\mathrm{Head}(\mathrm{More}\,0\ (\mathit{always}\ 1)) = \mathrm{Head}(\mathit{always}\ 0)$.

$$\begin{aligned}
\mathrm{Head}(\mathrm{More}\,0\ (\mathit{always}\ 1)) &= 0 && (\mathrm{Head} \circ \mathrm{More}) \\
&= \mathrm{Head}(\mathit{always}\ 0) && (\mathrm{Head} \circ \mathit{always}^{-1})
\end{aligned}$$

(Tail) Assume CoIH: $h(\mathrm{More}\,0\ (\mathit{always}\ 1)) = h(\mathit{always}\ 0)$.
Show $h(\mathrm{Tail}(\mathrm{More}\,0\ (\mathit{always}\ 1))) = h(\mathrm{Tail}(\mathit{always}\ 0))$.

$$\begin{aligned}
h(\underline{\mathrm{Tail}(\mathit{always}\ 0)}) &= \underline{h(\mathit{always}\ 0)} && (\mathrm{Tail} \circ \mathit{always}) \\
&= h(\mathrm{More}\,0\ (\mathit{always}\ 1)) && (\mathit{CoIH}^{-1}) \\
&\neq h(\mathrm{Tail}(\mathrm{More}\,0\ (\mathit{always}\ 1))) && (???) \qquad \boxtimes
\end{aligned}$$

Coinductive Rules in Classical Logic

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

$$\langle x \| \alpha \rangle$$

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

A producer $x : A$ gives an answer of type A

A consumer $\alpha \div A$ asks a question of type A

A command $\langle x \| \alpha \rangle$ is an interaction at a type

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

An Formal Induction Principle

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 $y : \mathrm{Nat}$

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

The sound axiom of primitive induction on Nat:

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

A Classical Coinduction Principle

Summarizing infinite cases of observers

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 $\delta \div \mathsf{Stream}\ A$

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

A Classical Coinduction Principle

Summarizing infinite cases of observers

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

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

All the cases of α:

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

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

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

The sound axiom of primitive corecursion on Stream A:

$$\begin{aligned} &(\forall \beta \div A.\ P(\beta \circ \text{Head})) \implies \\ &(\forall \delta \div \text{Stream } A.\ P(\delta) \implies P(\delta \circ \text{Tail})) \implies \\ &\ \forall \alpha \div \text{Stream } A.\ P(\alpha) \end{aligned}$$

Coinductive Principles for Other Types

```
record River (A : Set) : Set where
  coinductive
  field Curr : A
        Fork : River A × River A
```

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

All the cases of α:

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

$\alpha = \delta \circ \pi_1 \circ \mathsf{Fork}$ for some other $\delta \div \mathsf{Stream}\, A$

$\alpha = \delta \circ \pi_2 \circ \mathsf{Fork}$ for some other $\delta \div \mathsf{Stream}\, A$

The sound axiom of primitive corecursion on River A:

$$
\begin{aligned}
(\forall \beta \div A.\ P(\beta \circ \mathsf{Head})) &\implies (\forall \delta \div \mathsf{River}\, A.\ P(\delta) \implies P(\delta \circ \pi_1 \circ \mathsf{Tail})) \\
&\implies (\forall \delta \div \mathsf{River}\, A.\ P(\delta) \implies P(\delta \circ \pi_2 \circ \mathsf{Tail})) \\
&\implies \forall \alpha \div \mathsf{River}\, A.\ P(\alpha)
\end{aligned}
$$

Computing With Contextual Coinduction

Consistency of Equality

Theorem
If $\Gamma \vdash \langle v \| e \rangle = \langle v' \| e' \rangle$, *then* $\langle v \| e \rangle$ *and* $\langle v' \| e' \rangle$ *are contextually equivalent.*

Proof.
By a logical relation based on orthogonal fixed points in a subtyping lattice.

Key idea: Knaster-Tarski and Kleene fixed points defining types coincide. $\square$

Consistency of Equality

Theorem
If $\Gamma \vdash \langle v \| e \rangle = \langle v' \| e' \rangle$*, then* $\langle v \| e \rangle$ *and* $\langle v' \| e' \rangle$ *are contextually equivalent.*

Proof.
By a logical relation based on orthogonal fixed points in a subtyping lattice.

Key idea: Knaster-Tarski and Kleene fixed points defining types coincide. □

Corollary
If $\alpha \div \mathrm{Bool} \vdash \langle v \| e \rangle = \langle v' \| e' \rangle$*, then either*

$$\langle v \| e \rangle \mapsto\!\!\!\!\twoheadrightarrow \langle \mathrm{tt} \| \alpha \rangle \twoheadleftarrow\!\!\!\!\leftarrow \langle v' \| e' \rangle \textit{ or}$$

$$\langle v \| e \rangle \mapsto\!\!\!\!\twoheadrightarrow \langle \mathrm{ff} \| \alpha \rangle \twoheadleftarrow\!\!\!\!\leftarrow \langle v' \| e' \rangle.$$

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

Surprising wrinkle: 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

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

- Fully consistent under call-by-value evaluation
- Safe for strict properties in call-by-name evaluation

$$\textit{Strict on } x \ni \qquad \Psi(x) ::= \langle x \| E \rangle = \langle x \| E' \rangle \qquad (E, E' \in \textit{Eval.Cxt.})$$
$$\mid \ldots$$

(Co)Induction and Evaluation Strategy

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

- Fully consistent under call-by-value evaluation
- Safe for strict properties in call-by-name evaluation

$$\textit{Strict on } x \ni \qquad \Psi(x) ::= \langle x \| E \rangle = \langle x \| E' \rangle \qquad (E, E' \in \textit{Eval.Cxt.})$$
$$\mid \ldots$$

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

- Fully consistent under call-by-name evaluation
- Safe for productive properties in call-by-value evaluation

$$\textit{Productive on } \alpha \ni \qquad \Psi(\alpha) ::= \langle V \| \alpha \rangle = \langle V' \| \alpha \rangle \qquad (V, V' \in \textit{Value})$$
$$\mid \ldots$$

Other Reasoning Principles

Other reasoning principles like...

Mutual (co)induction: Multiple (Co)IHs over multiple goals

Strong (co)induction: Assume (Co)IH over <u>all</u> smaller structures

Bisimulation: Proof by relationship preservation

...are all derivable from structural (co)induction.

Other Reasoning Principles

Other reasoning principles like...

Mutual (co)induction: Multiple (Co)IHs over multiple goals

Strong (co)induction: Assume (Co)IH over all smaller structures

Bisimulation: Proof by relationship preservation

...are all derivable from structural (co)induction.

Caveat: Bisimulation & strong coinduction requires unrestricted CBN rule

Dual caveat: strong induction requires unrestricted CBV rule

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

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

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

What’s So Hard About Coinduction?

Coinduction With Confidence

Coinductive Rules in Classical Logic

Computing With Contextual Coinduction

References

[1] **Downen & Ariola, A Contextual Formalization of Structural Coinduction, Journal of Funcional Programming ’25.**

[2] Downen & Ariola, Classical (Co)Recursion: Mechanics, Journal of Functional Programming ’23.

[3] Downen & Ariola, Classical (Co)Recursion: Programming, ArXiv ’21.

[4] Downen & Ariola, A Computational Understanding of Classical (Co)Recursion, PPDP ’20.

[5] Downen & Ariola, Structures for Structural Recursion, ICFP ’16. (extended version)

Bonus

Mutual Coinduction

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

Mutual Coinduction

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

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

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

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:

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

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

$$\text{(Tail)}\quad \forall xs, ys,\ CoIH_1 : h(evens(merge\ xs\ ys)) = h(xs), \quad \text{AND } CoIH_2 : h(odds(merge\ xs\ ys)) = h(ys).$$

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

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

$\square$

Proof By Strong Coinduction

Theorem

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

Proof. By strong contextual stream equality:

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

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

Proof By Strong Coinduction

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

Proof. By strong contextual stream equality:

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

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

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

$\square$

Proof By Strong Coinduction

Theorem

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

Proof. By strong contextual stream equality:

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

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

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

$\square$

Proof By Strong Coinduction

Theorem

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

Proof. By strong contextual stream equality:

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

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

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

$\square$