ACT 2024 19 June 2024

# EFFECTFUL TRACE SEMANTICS VIA EFFECTFUL STREAMS

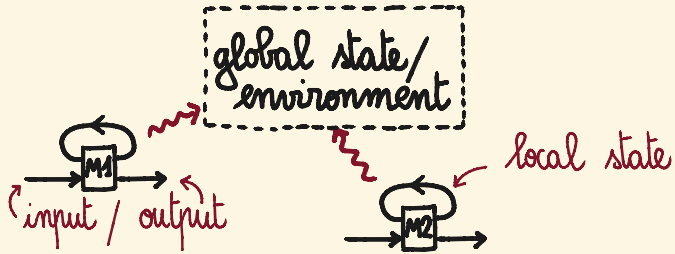
Filippo Bonchi
Università di Pisa

Elena Di Lavore
Università di Pisa

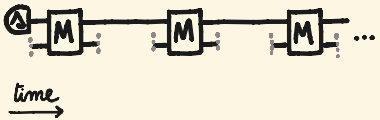
Mario Román
University of Oxford

# SEMANTICS OF EFFECTFUL MEALY MACHINES

- Mealy machines with global effects




- Trace semantics in streams



# EXAMPLES OF MEALY MACHINES

A classical Mealy machine is

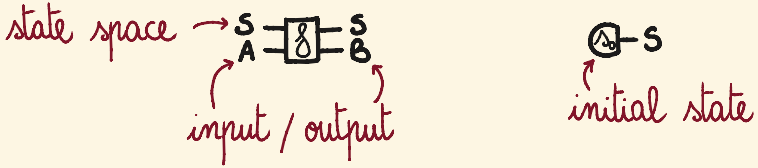
$$\begin{cases} t : S \times A \longrightarrow \mathcal{P}(S \times B) & \text{transition relation} \\ s_0 : 1 \longrightarrow \mathcal{P}S & \text{initial states} \end{cases}$$

A Markov decision process is

$$\begin{cases} t : S \times A \longrightarrow \mathcal{D}S & \text{transition probability} \\ r : S \times A \longrightarrow \mathcal{D}U & \text{reward} \\ s_0 : 1 \longrightarrow \mathcal{D}S & \text{initial distribution} \end{cases}$$

# MEALY MACHINES

Systems are $f : S \otimes A \to S \otimes B$ with $s_0 : I \to S$




- native sequential and parallel compositions
- parametric in the underlying process theory
- premonoidal categories for global effects

⇝ what is their behaviour ?
when are two of them equivalent ?

[ cf. Katis, Sabadini, Walters 1997 ]

# COALGEBRAIC SEMANTICS

Systems are coalgebras $f : S \to F(S)$

input / output

$S \to (S \times B)^A$

non-determinism

$S \to \mathcal{P}(S \times B)$

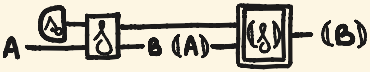
- bisimulation is equality in the final coalgebra

⇝ how do these compose ?
how to change the underlying process theory ?

# OVERVIEW

effectful Mealy machines


effectful streams



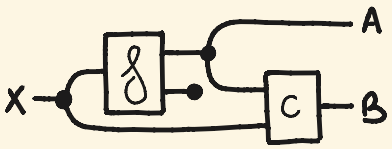

free construction
~ syntax

coalgebraic construction
~ semantics

# STRING DIAGRAMS & DO-NOTATION

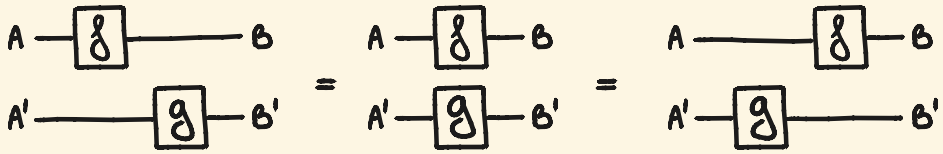
- Symmetric monoidal categories are theories of processes
- String diagrams and do-notation are convenient syntax

$$\nu_X ; ((f ; (\nu_A \otimes \varepsilon_B)) \otimes 1_X) ; (1_A \otimes c)$$




```
cond(x) = do
  f(x) → (a, b)
  c(a, x) → b'
  return (a, b')
```

# THE INTERCHANGE LAW




```
par f g (a, a') = do
  | f(a) → b
  | g(a') → b'
  | return (b, b')
```

=

```
par f g (a, a') = do
  | g(a') → b'
  | f(a) → b
  | return (b, b')
```

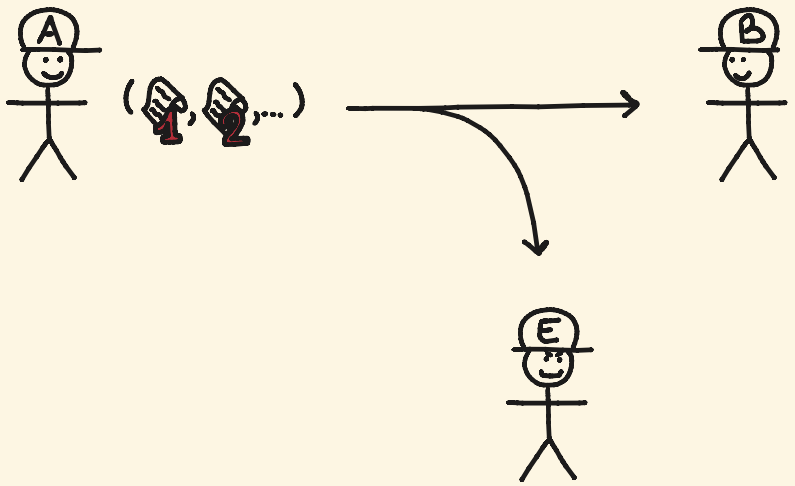
⇝ holds in monoidal categories

# OUTLINE

- [ effectful copy-discard categories ]
- effectful Mealy machines
- effectful streams
- causal processes
- bisimulation

# A MOTIVATING EXAMPLE

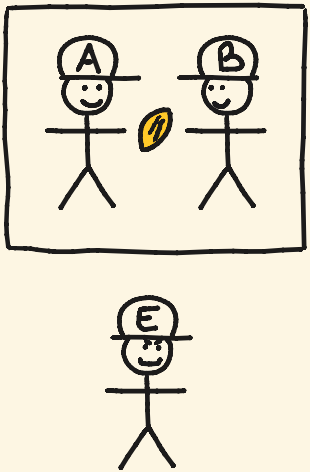
The stream cipher is a simple cryptographic protocol.



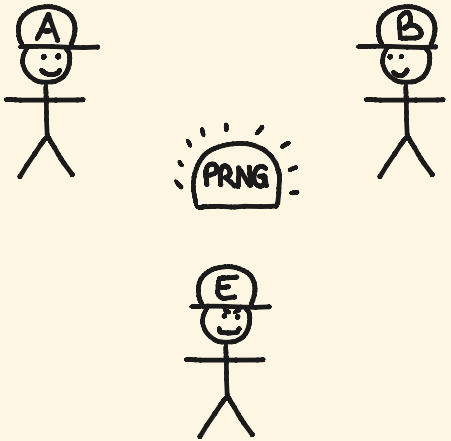

[cf. Broadbent, Karvonen 2022]

# STREAM CIPHER PROTOCOL (1)

1. share a seed through a secure channel

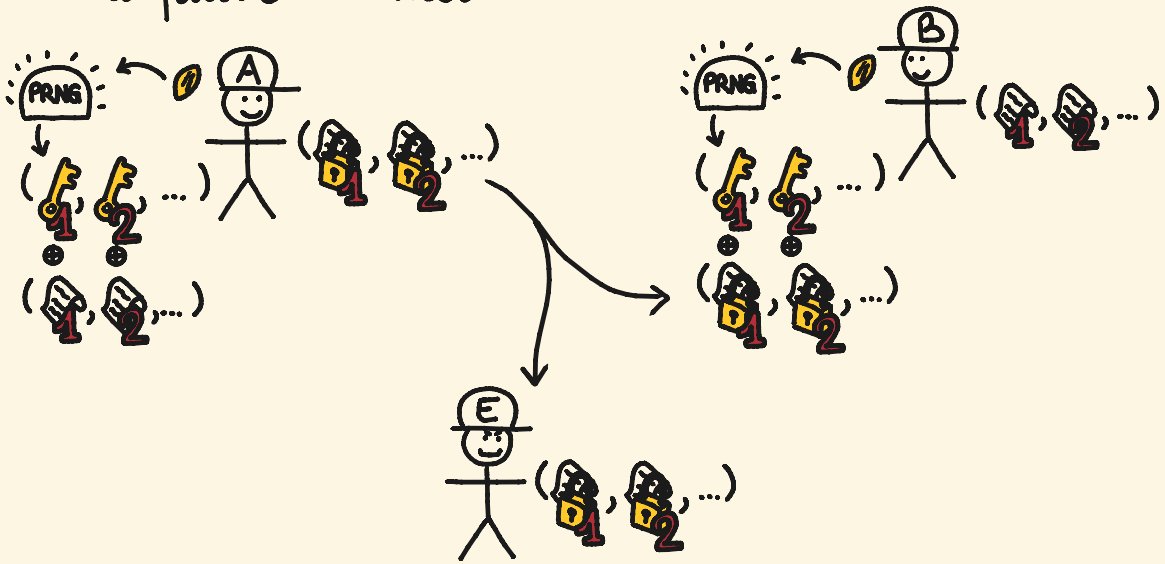



2. share a pseudorandom number generator



# STREAM CIPHER PROTOCOL (2)

3. send a stream of encrypted messages through a public channel



# COMPUTATIONS WITH EFFECTS

- Stochastic effects: generating the seed

$\mathcal{D} : \mathbf{Set} \to \mathbf{Set}$ distribution monad

$\mathcal{D}(A) := \{ \sigma : A \to [0,1] \mid \mathrm{supp}\, \sigma \text{ is finite} \wedge \sum_{a \in A} \sigma(a) = 1 \}$

- Global state: sharing the seed

$\mathbf{State}_S : \mathcal{C}^{op} \times \mathcal{C} \to \mathbf{Set}$ state promonad

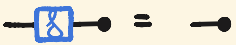
$\mathbf{State}_S(A,B) := \mathcal{C}(S \otimes A, S \otimes B)$

# VALUES

Values are both :

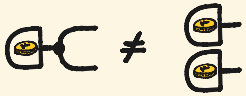
- deterministic

- total

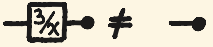


ex $(3 \cdot -) : \mathbb{R} \to \mathbb{R}$

NON-ex $\mathrm{Flip} : 1 \to \mathcal{D}(\{H,T\})$

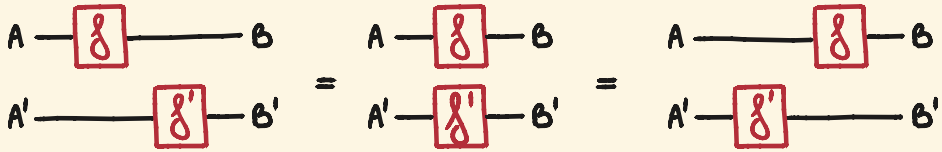


$(3/-) : \mathbb{R} \to \mathbb{R}$



# LOCAL COMPUTATIONS

Local computations interchange,




```
localF (a, a') = do
  f (a) → b
  f'(a') → b'
  return (b, b')
```

=

```
localF (a, a') = do
  f'(a') → b'
  f (a) → b
  return (b, b')
```

ex Stoch

# EFFECTFUL COMPUTATIONS

Effectful computations may have global effects.


```
printHI() = do
  'h'() → c1
  'i'() → c2
  print(c1) ⇝ ()
  print(c2) ⇝ ()
  return ()
```

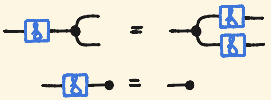
≠

```
printIH() = do
  'h'() → c1
  'i'() → c2
  print(c2) ⇝ ()
  print(c1) ⇝ ()
  return ()
```

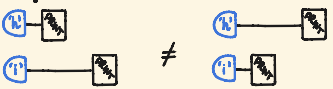
ex state promonads, IO monad

# EFFECTFUL COPY-DISCARD CATEGORIES

Values can be copied and discarded (cartesian)

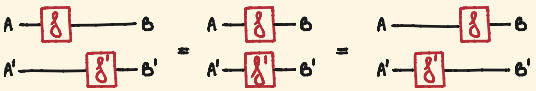


Effectful computations may have global effects (premonoidal)



$\mathcal{V} \longrightarrow \mathcal{L} \longrightarrow \mathcal{C}$

Local computations interchange (monoidal)



ex $(\mathbf{Set}, \mathbf{Stoch}, \mathbf{State}_S)$

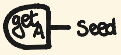
$(\mathrm{cart}(\mathcal{C}), \mathcal{Z}(\mathcal{C}), \mathcal{C})$ for a CD-premonoidal $\mathcal{C}$

# OUTLINE

- effectful copy-discard categories
- [ effectful Mealy machines ]
- effectful streams
- causal processes
- bisimulation

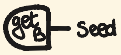
# STREAM CIPHER COMPONENTS

Encryption protocol





Decryption protocol





Attacker protocol

# EFFECTFUL MEALY MACHINES

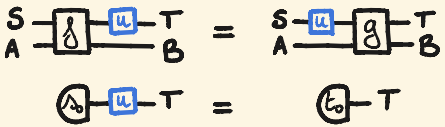
A Mealy machine $(f, S, s_0) : A \to B$ in $(\mathcal{V}, \mathcal{L}, \mathcal{C})$ is a morphism

$$f : S \otimes A \to S \otimes B$$


with an initial state

$$s_0 : I \to S$$


A morphism of Mealy machines $u : (f, S, s_0) \to (g, T, t_0)$ is a value morphism $u : S \to T$ in $\mathcal{V}$ such that

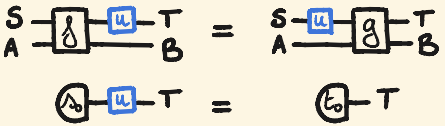



[cf. Katis, Sabadini, Walters 1997 ; EDL, Gianola, Román, Sabadini, Sobociński 2022]

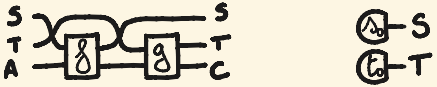
# EFFECTFUL CATEGORY OF MEALY MACHINES

Mealy is an effectful category where

- objects are the objects of $\mathcal{C}$
- morphisms $(f, S, s_0) : A \to B$ are Mealy machines quotiented by value isomorphisms $u : S \xrightarrow{\cong} T$




- composition tensors the state spaces



# FEEDBACK EFFECTFUL CATEGORIES

A feedback effectful category $\mathcal{C}$ is a premonoidal category $\mathcal{C}$ with

- a monoidal category $\mathcal{S}$
- a premonoidal functor $U : \mathcal{S} \to \mathcal{C}$
- an operation

$$\mathrm{FbK} : \mathcal{C}(U(S) \otimes A, U(S) \otimes B) \longrightarrow \mathcal{C}(A, B)$$

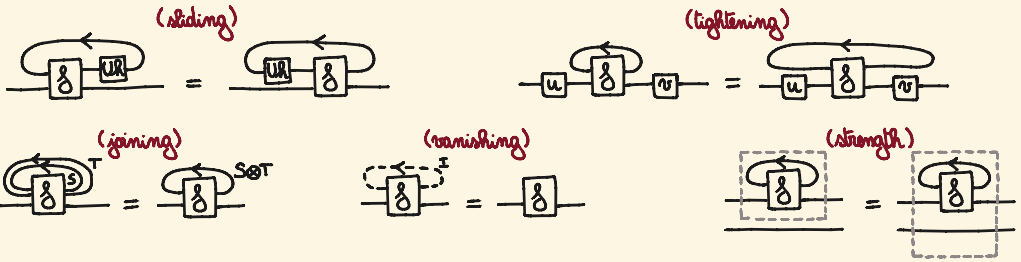

+ axioms

# FEEDBACK EFFECTFUL CATEGORIES

## U-FEEDBACK

$$\mathrm{Fbk} : \mathcal{C}(U(S) \otimes A, U(S) \otimes B) \longrightarrow \mathcal{C}(A, B)$$


satisfying



# EFFECTFUL CATEGORY OF MEALY MACHINES

$\mathcal{S} := \mathrm{pt}\mathcal{C}_{\mathrm{iso}}$

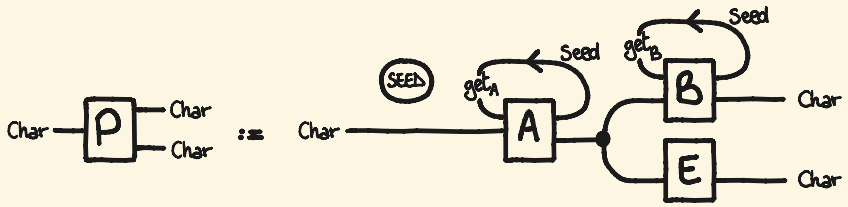
**THEOREM**

Mealy is the free pointed-feedback category over $\mathcal{C}$.

$$\mathrm{Mealy}(A,B) = \int^{(s_0,S)\in \mathrm{pt}\mathcal{C}_{\mathrm{iso}}} \mathcal{C}(S\otimes A, S\otimes B)$$


[cf. Katis, Sabadini, Walters 1997 ; EDL, Gianola, Román, Sabadini, Sobociński 2022]

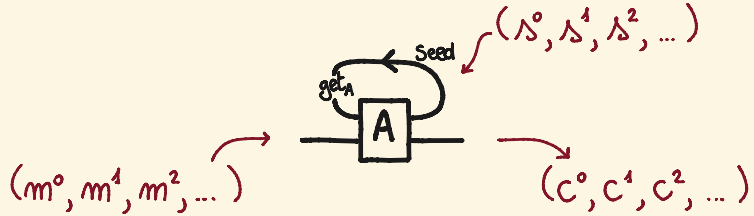
# ASSEMBLING THE STREAM CIPHER



# OUTLINE

- effectful copy-discard categories
- effectful Mealy machines
- [ effectful streams ]
- causal processes
- bisimulation

# EXECUTING MEALY MACHINES




↝ what should the semantic universe be?
when do two Mealy machines have the same executions?

# STREAMS ARE COINDUCTIVE

A stream of elements of $A$ is

- an element $a^\circ \in A$
- a stream $a^+$ of elements of $A$

$\rightsquigarrow$ the set of streams is the final coalgebra of the functor

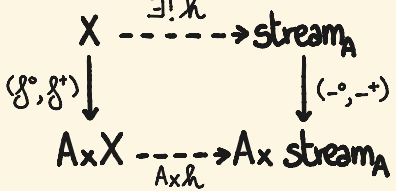
$$A \times (-) : \mathcal{S}et \longrightarrow \mathcal{S}et$$

# PRACTICAL COINDUCTION

Final coalgebras allow

- coinductive definitions

$$\begin{cases} h(x)^{\circ} := g^{\circ}(x) \\ h(x)^{+} := h(g^{+}(x)) \end{cases}$$



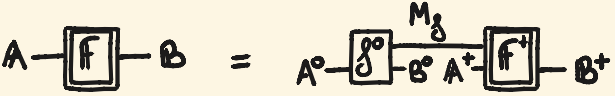

- coinductive proofs

[ Kozen & Silva (2017) Practical coinduction ]

# EFFECTFUL STREAMS

An effectful stream $F : A \to B$ on $(\mathcal{V}, \mathcal{L}, \mathcal{C})$ is

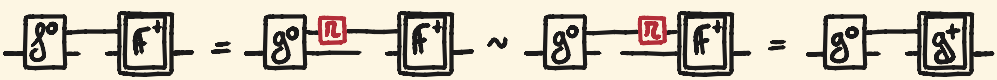
- a memory $M_g \in \mathcal{L}$
- a first action $g^\circ : A^\circ \to M_g \otimes B^\circ$ in $\mathcal{C}$
- the rest of the action $F^+ : M_g \cdot A^+ \to B^+$




quotiented by sliding

$$\begin{cases} g^\circ ; (r \otimes 1) = g^\circ \\ F^+ = r \cdot g^+ \end{cases}$$

for $r : M_g \to M_g$ in $\mathcal{L}$



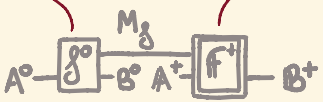
# EFFECTFUL STREAMS

The profunctor $\mathrm{Stream} : \mathcal{C}^{\mathbb{N}^{op}} \times \mathcal{C}^{\mathbb{N}} \longrightarrow \mathcal{S}et$ is the final coalgebra of the functor

$$F : [\mathcal{C}^{\mathbb{N}^{op}} \times \mathcal{C}^{\mathbb{N}}, \mathcal{S}et] \longrightarrow [\mathcal{C}^{\mathbb{N}^{op}} \times \mathcal{C}^{\mathbb{N}}, \mathcal{S}et]$$

$$F(Q)(A,B) := \int^{M \in \mathcal{C}} \mathcal{C}(A^\circ, M \otimes B^\circ) \times Q(M \cdot A^+, B^+)$$

quotient by sliding on the memory



# COMPOSITIONAL STRUCTURE OF STREAMS

**THEOREM**

Effectful streams form an effectful category Stream.

- composition and monoidal actions are defined coinductively: for $f : N_g \cdot A \to B$ and $g : N_g \cdot B \to C$,

$$\begin{cases} (f \fatsemi_N g)^\circ := \\ (f \fatsemi_N g)^+ := f^+ \fatsemi_M g^+ \end{cases}$$


$$\begin{cases} (X \otimes_N f)^\circ := \\ (X \otimes_N f)^+ := X^+ \otimes_M f^+ \end{cases}$$

# FEEDBACK ON EFFECTFUL STREAMS

$\partial : \text{Stream} \longrightarrow \text{Stream} \qquad \partial(A) := (I, A^\circ, A^1, \dots)$

**THEOREM**

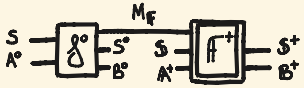
Stream has $\partial$-feedback.

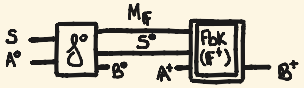
- feedback is defined coinductively

$$ff : (S \cdot \partial S) \otimes A \longrightarrow S \otimes B$$

$$\mathrm{FbK}_S\, ff : S \cdot A \longrightarrow B$$

$$M(\mathrm{FbK}^S_S\, ff) := M(ff) \otimes S^\circ$$
$$(\mathrm{FbK}^S_S\, ff)^\circ := f^\circ$$
$$(\mathrm{FbK}^S_S\, ff)^+ := \mathrm{FbK}^{S^\circ}_{S^+}(ff^+)$$



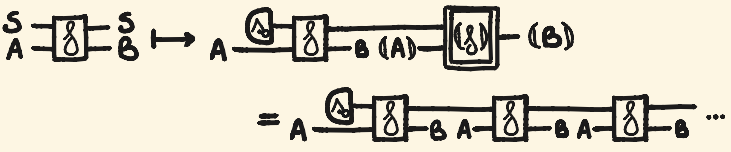
# COMPOSITIONAL TRACE SEMANTICS

**THEOREM**

There is a feedback effectful functor

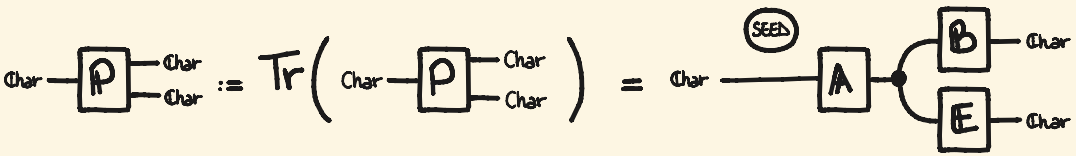
$$\mathrm{Tr} : \mathbf{Mealy} \longrightarrow \mathbf{Stream}$$

$$A \longmapsto (\!|A|\!) = (A, A, \dots)$$

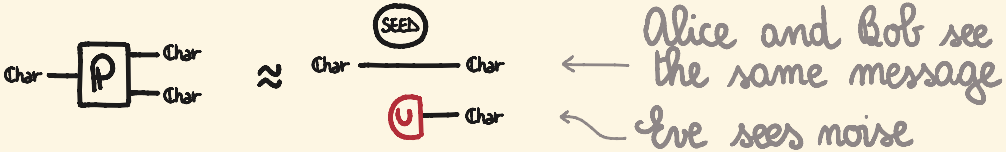



⇝ in **Rel** these traces coincide with the classical traces

# SEMANTICS FOR THE STREAM CIPHER PROTOCOL




## SECURITY OF THE PROTOCOL



# OUTLINE

- effectful copy-discard categories
- effectful Mealy machines
- effectful streams
- causal processes
- bisimulation

# STREAM COMPUTATIONS

- Sliding equivalence might be difficult to handle
- Causal stream functions are old :

  [Raney 1958] shows that they are
  the executions of deterministic Mealy machines

⇝ is there a similar explicit form for effectful streams ?

# STREAM COMPUTATIONS

## CAUSAL STREAM FUNCTIONS

Stream computations $(p_m)_{m \in \mathbb{N}} : \mathbb{A} \to \mathbb{B}$ in a cartesian category are families $p_m : A_0 \times \cdots \times A_m \longrightarrow B_m$ .

## STOCHASTIC PROCESSES

Stochastic stream computations $(p_m)_{m \in \mathbb{N}} : \mathbb{A} \to \mathbb{B}$ are families $p_m : A_0 \times \cdots \times A_m \longrightarrow \mathcal{D}(B_0 \times \cdots \times B_m)$ such that $p_m(a_0, \ldots, a_m) = \sum_{a \in A_{m+1}} p_{m+1}(a_0, \ldots, a_m, a)$ .

⇝ is there a monoidal version ?

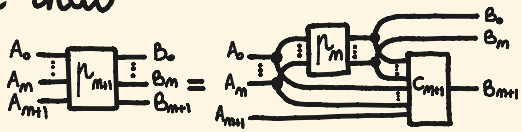
[Sprunger & Katsumata (2019), Ulustalu & Veme (2008)]

# CAUSAL PROCESSES

A causal process $p : A \to B$ in a copy-discard category $\mathcal{C}$ is a family of morphisms

$$p_n : A_0 \otimes \cdots \otimes A_n \longrightarrow B_0 \otimes \cdots \otimes B_n$$

such that



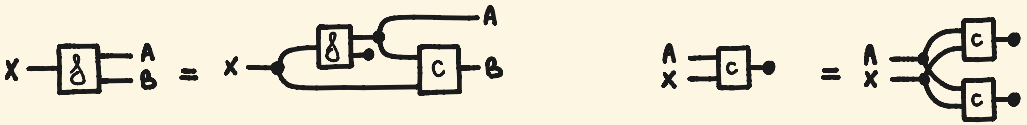

for some $C_{n+1} : B_0 \otimes \cdots \otimes B_n \otimes A_0 \otimes \cdots \otimes A_n \otimes A_{n+1} \to B_{n+1}$

# COMPOSING CAUSAL PROCESSES

$\mathcal{C}$ copy-discard

**QUASI-TOTAL CONDITIONALS** [Fritz (2020), EDL & Román (2023)]

For all $f : X \to A \otimes B$ there is $c : A \otimes X \to B$ st




**THEOREM**

Causal processes form a monoidal category Proc when $\mathcal{C}$ has quasi-total conditionals.

# CAUSAL PROCESSES : EXAMPLES

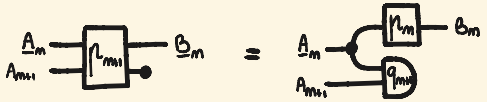
**Set**

$$f_m : A_0 \times \cdots \times A_m \longrightarrow B_m$$

**Par**

$$f_m : A_0 \times \cdots \times A_m \longrightarrow (B_0 \times \cdots \times B_m) + 1$$

st




**Stoch**

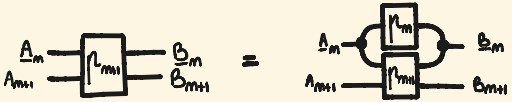
$$f_m : A_0 \times \cdots \times A_m \longrightarrow \mathcal{D}(B_0 \times \cdots \times B_m)$$

st


**Rel**

$$f_m : A_0 \times \cdots \times A_m \longrightarrow \mathcal{P}(B_0 \times \cdots \times B_m)$$

st

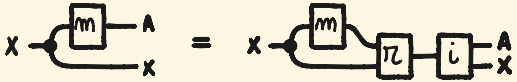


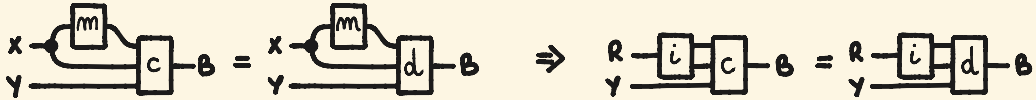
# CAUSAL PROCESSES ARE STREAMS

$\mathcal{C}$ copy-discard

## RANGES

For all $m : X \to A$ there are $\begin{cases} r : A \otimes X \to R & \text{deterministic} \\ i : R \to A \otimes X & \text{total} \end{cases}$




## THEOREM

Consider $(\mathrm{fun}\mathcal{C}, \mathrm{tot}\mathcal{C}, \mathcal{C})$.

If $\mathcal{C}$ has quasi-total conditionals and ranges,

$$\mathrm{Proc} \simeq \mathrm{Stream} .$$

# TRACES ARE EFFECTFUL TRACES

Compute the traces of a Mealy machine

$$(f, S, s) : A \to B$$

in some known cases.

$(b_0, \dots, b_n)$ is a trace of $(a_0, \dots, a_n)$

**Set** if $s_0 = s$ and $\forall k \leq n \ (s_{k+1}, b_k) = f(s_k, a_k)$

**Rel** if $\exists (s_0, \dots, s_{n+1}) \quad s_0 \in s$
and $\forall k \leq n \ (s_{k+1}, b_k) \in f(s_k, a_k)$

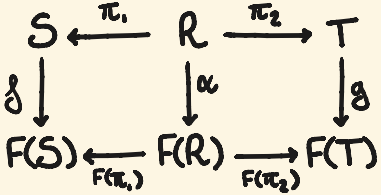
**pStoch** with probability $\sum_{(s_0, \dots, s_{n+1})} s(s_0 \mid *) \cdot \prod_{k \leq n} f(s_{k+1}, b_k \mid s_k, a_k)$

# OUTLINE

- effectful copy-discard categories
- effectful Mealy machines
- effectful streams
- causal processes
- [ bisimulation ]

# COALGEBRAIC BISIMULATION

A bisimulation is a span of coalgebras.



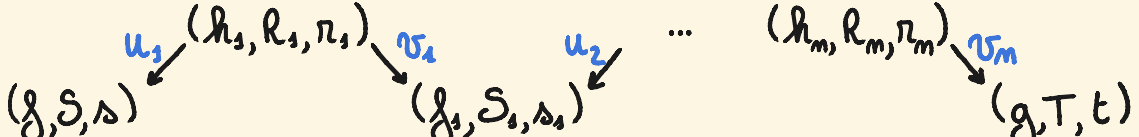

**THEOREM** [Rutten (2000)]

When $F : \mathbf{Set} \to \mathbf{Set}$ preserves weak pullbacks, bisimularity is an equivalence relation.

[Aczel & Mendler (1989), Rutten (2000)]

# BISIMULATION

Two effectful Mealy machines $(g, S, s), (g, T, t) : A \to B$ are <u>bisimilar</u> if they belong to the same connected component in $\mathrm{Mealy}(A, B)$:




**THEOREM**

For Mealy machines in $(\mathcal{V}, \mathcal{L}, \mathcal{C})$, bisimulation implies trace equivalence.

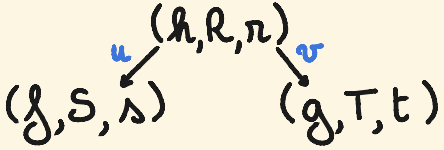
PROOF: By coinduction. □

# COALGEBRAIC BISIMULATION

**PROPOSITION**

When $\mathcal{C} = \mathrm{Kl}(M)$, for a commutative monad preserving weak pullbacks, effectful bisimulation coincides with coalgebraic bisimulation.

$(f, S, s) \approx (g, T, t)$ iff




**EXAMPLES**

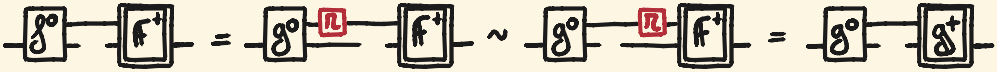
- Set
- Rel
- Stoch
- Par
- pStoch

# SUMMARY

- formal compositional semantics for effectful stream computations
- trace equivalence and bisimulation of effectful Mealy machines
- characterisation as causal stream processes

# FUTURE WORK

- coinduction up-to dinaturality




- Rel with explicit failure
- equality in St-C implies bisimulation


- distance instead of equivalence relation for security