CALCO 17 June 2025

EFFECTFUL MEALY MACHINES

BISIMULATION & TRACES

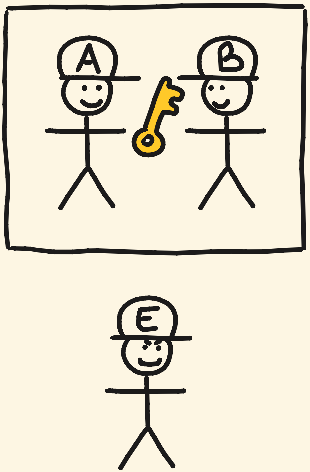
Filippo Bonchi
Università di Pisa

Elena Di Lavore
University of Oxford

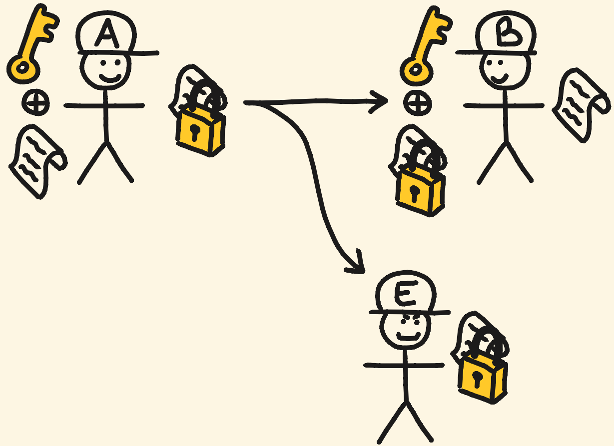
Mario Román
University of Oxford

ONE-TIME PAD PROTOCOL

1. share a key through a secure channel



2. send an encrypted message through a public channel



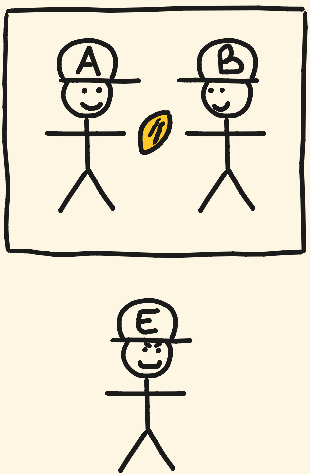
REPEATING THE ONE-TIME PAD

Sending n messages securely requires n private keys
↳ not very useful

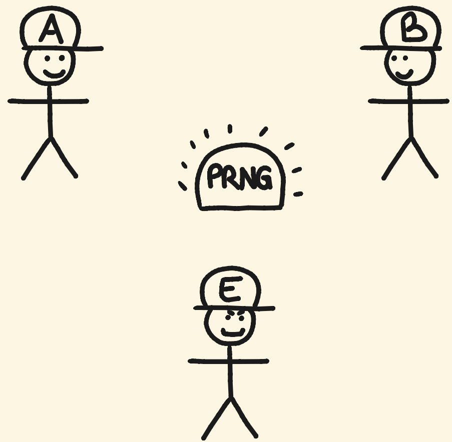
⇒ • privately share a seed 
• use identical pseudorandom number generator to obtain a new key for each message

STREAM CIPHER PROTOCOL (1)

1. share a seed through a secure channel

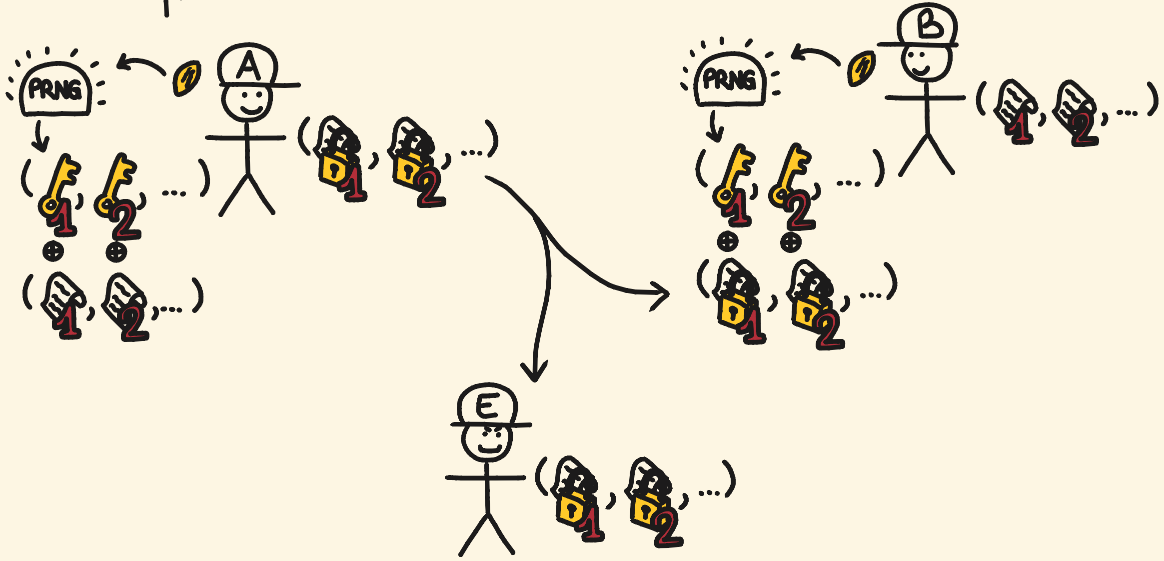


2. share a pseudorandom number generator



STREAM CIPHER PROTOCOL (2)

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

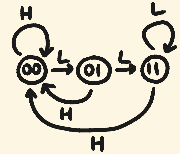


MEALY MACHINES

A classical Mealy machine is

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

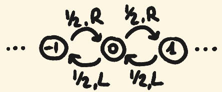
TEMPERATURE CONTROLLER



A Markov decision process is

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

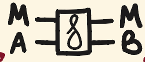
RANDOM WALK



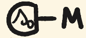
MEALY MACHINES

Systems are $\delta : M \otimes A \to M \otimes B$ with $s_0 : I \to M$

state space



input / output



initial state

- 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 $f : M \to F(M)$

input/output

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

non-determinism

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

- bisimulation is equality in the final coalgebra

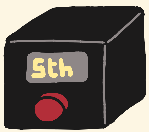
⇝ how do these compose?
how to change the underlying process theory?

MEALY MACHINES AND COALGEBRAS

Two faces of Mealy machines

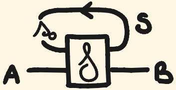
$$M \times A \to \mathcal{D}(M \times B) \qquad\qquad M \to \mathcal{D}(M \times B)^A$$

$$M \times A \to \mathcal{P}(M \times B) \qquad\qquad M \to \mathcal{P}(M \times B)^A$$



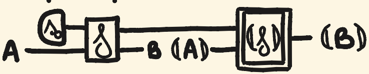
OVERVIEW

effectful Mealy machines



bisimilarity

effectful streams



[≃ causal processes]

free construction

~ syntax

uniformity

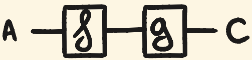
coalgebraic construction

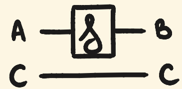
~ trace semantics

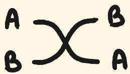
OUTLINE

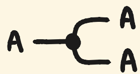
- Effectful copy-discard categories
- Effectful Mealy machines & bisimulations
- Coinductive traces
- Causal traces

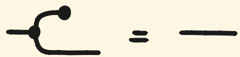
STRING DIAGRAMS

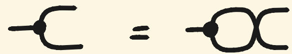




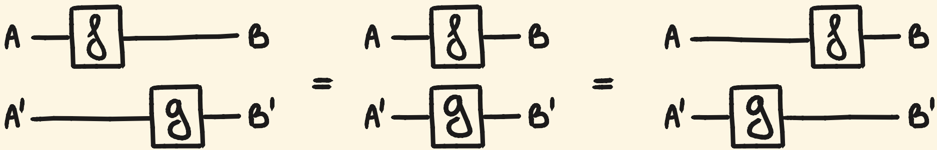








THE INTERCHANGE LAW



⇝ holds in monoidal categories

VALUES

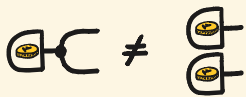
Values are both :

- deterministic

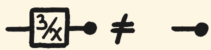
- total

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

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

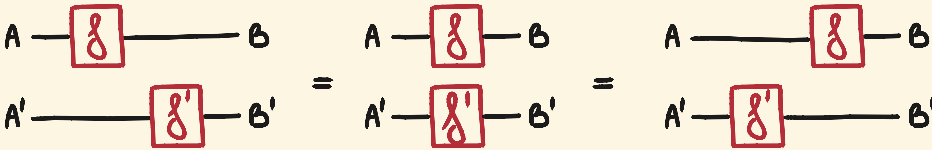


$(3/-) : \mathbb{R} \to \mathbb{R}$

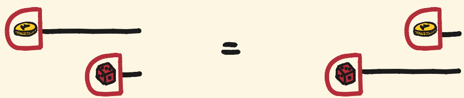


LOCAL COMPUTATIONS

Local computations interchange,

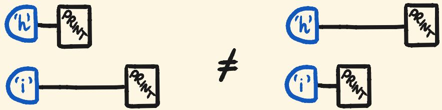


ex Stoch



EFFECTFUL COMPUTATIONS

Effectful computations may have global effects.



ex state promonads, IO monad

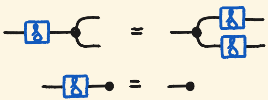
[Power and Robinson (1997)]

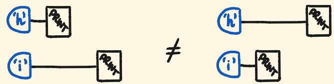
EFFECTFUL COPY-DISCARD CATEGORIES

Values can be copied and discarded (cartesian)

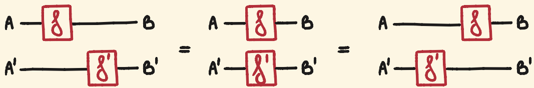
Effectful computations may have global effects (premonoidal)

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





Local computations interchange (monoidal)



[Jeffrey (1997), cf. Levy (2022), Power and Thielecke (1997)]

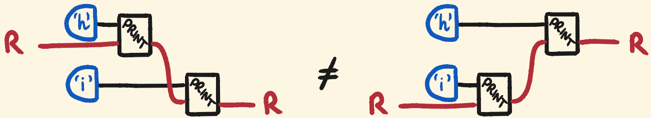
EXAMPLES OF EFFECTFUL TRIPLES

- $(\mathrm{cart}(\mathcal{C}), \mathcal{Z}(\mathcal{C}), \mathcal{C})$ for a cd-premonoidal $\mathcal{C}$
- $(\mathbf{Set}, \mathrm{Kl}(\mathcal{Z}(T)), \mathrm{Kl}(T))$ for a $\mathbf{Set}$-monad T
- $(\mathbf{Set}, \mathbf{Set}, \mathbf{Par})$
- $(\mathbf{Set}, \mathbf{Rel}_{TOT}, \mathbf{Rel})$
- $(\mathbf{Set}, \mathbf{Stoch}, \mathbf{Stoch}_{\leq})$
- $(\mathbf{Set}, \mathbf{Stoch}, \mathbf{State}_S)$

STRING DIAGRAMS FOR PREMONOIDAL CATEGORIES

Add a "runtime" wire to non-central morphisms

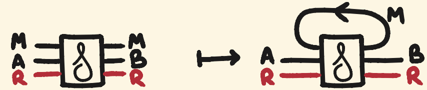
$f : A \to B$ is 

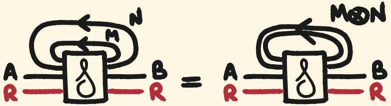


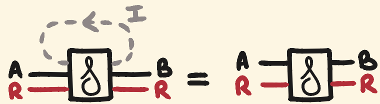
[Jeffrey (1997); Román (2022); Román, Sobociński (2025)]

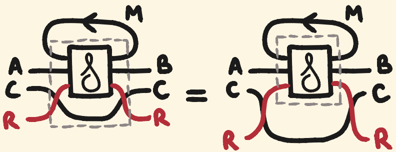
FEEDBACK EFFECTFUL CATEGORIES

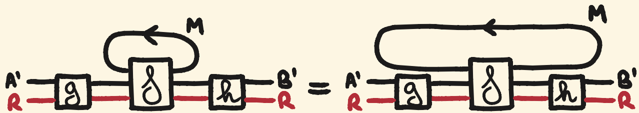
$\mathrm{Fbk}_M : \mathscr{C}(M \otimes A, M \otimes B) \to \mathscr{C}(A, B)$











$u : N \to M$ in $\mathscr{L}$

OUTLINE

- Effectful copy-discard categories
- [Effectful Mealy machines & bisimulations]
- Coinductive traces
- Causal traces

EFFECTFUL MEALY MACHINES

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

is a morphism

$f : M \otimes A \to M \otimes B$ in $\mathcal{C}$

with an initial state

$s_0 : I \to M$ in $\mathcal{L}$

ex $(\mathbf{Set}, \mathbf{Rel}_{TOT}, \mathbf{Rel})$

$$\begin{cases} f : M \times A \to \mathcal{P}(M \times B) \\ s_0 \subseteq M \end{cases}$$

ex $(\mathbf{Set}, \mathbf{Stoch}, \mathbf{Stoch}_{\leq})$

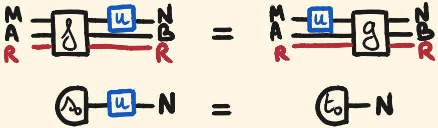
$$\begin{cases} f : M \times A \to \mathcal{D}(M \times B) \\ s_0 \in \mathcal{D}(M) \end{cases}$$

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

MORPHISMS OF MEALY MACHINES

A <u>morphism</u> of Mealy machines $u:(f,M,s_0)\to(g,N,t_0)$
is a value morphism $u: M\to N$ in $\mathcal{V}$

such that



<u>ex</u> $(\mathsf{Set}, \mathsf{Rel}_{TOT}, \mathsf{Rel})$

$\forall s\in M\ \forall a\in A\ \forall t\in N\ \forall b\in B$

$(t,b)\in g(u(s),a) \iff \exists s'\in M\ \ u(s')=t \wedge (s',b)\in f(s,a)$

<u>ex</u> $(\mathsf{Set}, \mathsf{Stoch}, \mathsf{Stoch}_{\leq})$

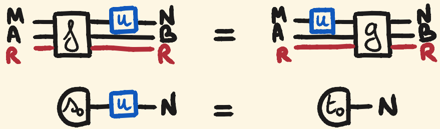
$\forall s\in M\ \forall a\in A\ \forall t\in N\ \forall b\in B$

$g(t,b\,|\,u(s),a) = \sum_{s':u(s')=t} f(s',b\,|\,s,a)$

EFFECTFUL CATEGORY OF MEALY MACHINES

Mealy is an effectful category where

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



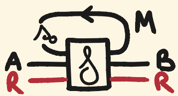
- composition tensors the state spaces ⇝ local states

MEALY MACHINES ARE FREE

THEOREM

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

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



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

COALGEBRAIC MEALY MACHINES

$T : \mathcal{S}et \to \mathcal{S}et$ monad

$$F_T : \mathcal{S}et \to \mathcal{S}et$$
$$X \mapsto T(X \times B)^A$$

A T-Mealy machine is an F_T-coalgebra

$$f : X \to T(X \times B)^A$$

$$\leftrightsquigarrow \quad \hat{f} : X \otimes A \to X \otimes B \quad \text{in } \mathcal{K}\ell\, T$$

$\leftrightsquigarrow$ effectful Mealy machine in $(\mathcal{S}et, \mathcal{K}\ell(Z(T)), \mathcal{K}\ell(T))$

COALGEBRAIC BISIMULATION

A bisimulation is a span of coalgebras.

$$
\begin{tikzcd}
M \arrow[d, "f"'] & R \arrow[l, "\pi_1"'] \arrow[r, "\pi_2"] \arrow[d, "\alpha"] & N \arrow[d, "g"] \\
F_T(M) & F_T(R) \arrow[l, "F_T(\pi_1)"] \arrow[r, "F_T(\pi_2)"'] & F_T(N)
\end{tikzcd}
$$

THEOREM [Rutten (2000)]

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

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

BISIMULATION

For two effectful Mealy machines $(f, M, s), (g, N, t) : A \to B$, a <u>bisimulation</u> is a sequence of spans of morphisms.

$$(f, M, s) \xleftarrow{u_1} (h_1, R_1, r_1) \xrightarrow{v_1} (f_1, M_1, s_1) \xleftarrow{u_2} \cdots \quad (h_n, R_n, r_n) \xrightarrow{v_n} (g, N, t)$$

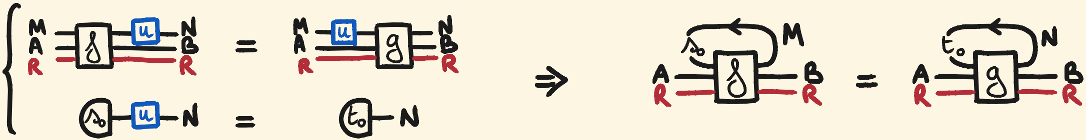
PROPOSITION

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

<u>ex</u> Set, Par, Rel, Stoch, pStoch

BISIMILARITY IS FREE

UNIFORM FEEDBACK [cf. Hasegawa (2002); Căzănescu, Ştefănescu (1994)]



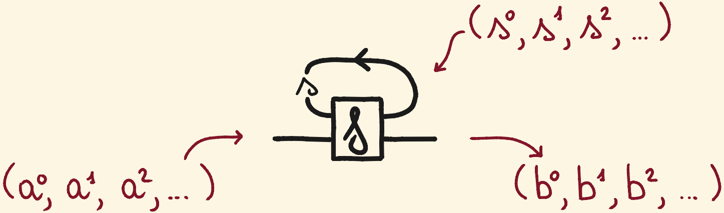
THEOREM

$\mathrm{Mealy}/_{\mathrm{bisim}}$ form the free uniform feedback structure over $(\mathcal{V}, \mathcal{L}, \mathcal{C})$.

OUTLINE

- Effectful copy-discard categories
- Effectful Mealy machines & bisimulations
- [Coinductive traces]
- Causal traces

EXECUTING MEALY MACHINES



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

STREAMS ARE COINDUCTIVE

A stream $(a^0, a^1, a^2, \dots)$ of elements of A is

- an element $a^0 \in A$
- a stream a^+ of elements of A

⇝ the set of streams is the final coalgebra of the functor

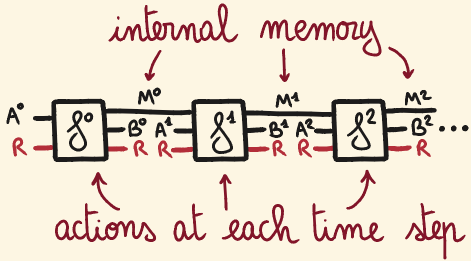
$$A \times (-) : \mathcal{S}et \to \mathcal{S}et$$

STREAM PROCESSES SHOULD BE COINDUCTIVE TOO

Objects are streams of objects of $(\mathcal{V}, \mathcal{L}, \mathcal{C})$

$$A = (A^0, A^1, A^2, \dots), \quad \mathbb{B} = (\mathbb{B}^0, \mathbb{B}^1, \mathbb{B}^2, \dots)$$

A stream process (= effectful stream) $\mathbb{F} : A \to \mathbb{B}$ is



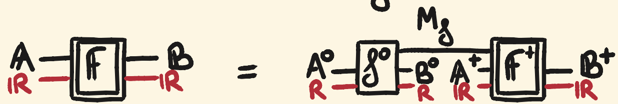
[cf. EDL, de Felice, Román (2022)]

EFFECTFUL STREAMS

$\mathbb{A} = (A^0, A^1, \dots)$, $\mathbb{B} = (B^0, B^1, \dots)$ streams of objects of $(\mathcal{V}, \mathcal{L}, \mathcal{C})$.

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

- a memory $M_f \in \mathcal{L}$
- a first action $f^0 : A^0 \to M_f \otimes B^0$ in $\mathcal{C}$
- the rest of the action $\mathbb{F}^+ : M_f \cdot \mathbb{A}^+ \to \mathbb{B}^+$



quotiented by sliding: for $r : M_g \to M_f$ in $\mathcal{L}$

$$f^0 = g^0 ; (r \otimes 1) \qquad\qquad g^+ = r \cdot \mathbb{F}^+$$

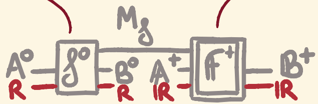
EFFECTFUL STREAMS

The profunctor Stream $: \mathcal{C}^{\mathbb{N}^{op}} \times \mathcal{C}^{\mathbb{N}} \to \mathbf{Set}$ is the final coalgebra of the functor

$$F : [\mathcal{C}^{\mathbb{N}^{op}} \times \mathcal{C}^{\mathbb{N}}, \mathbf{Set}] \to [\mathcal{C}^{\mathbb{N}^{op}} \times \mathcal{C}^{\mathbb{N}}, \mathbf{Set}]$$

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

quotient by sliding on the memory



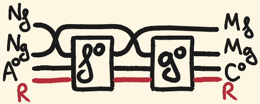
[cf. EDL, de Felice, Román (2022)]

COMPOSITIONAL STRUCTURE OF STREAMS

THEOREM

Effectful streams form an effectful category Stream.

- composition and monoidal actions are defined coinductively: for $\mathbb{F} : N_f \cdot \mathbb{A} \to \mathbb{B}$ and $\mathbb{g} : N_g \cdot \mathbb{B} \to \mathbb{C}$,

$(\mathbb{F} ;_N \mathbb{g})^\circ :=$ 

$(\mathbb{F} ;_N \mathbb{g})^+ := \mathbb{F}^+ ;_M \mathbb{g}^+$

$(\mathbb{X} \otimes_N \mathbb{F})^\circ :=$ 

$(\mathbb{X} \otimes_N \mathbb{F})^+ := \mathbb{X}^+ \otimes_M \mathbb{F}^+$

FEEDBACK ON EFFECTFUL STREAMS

$\partial : \mathsf{Stream} \to \mathsf{Stream}$ $\qquad\qquad \partial(A) := (I, A^0, A^1, \dots)$

THEOREM

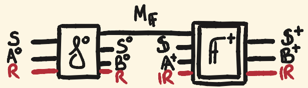
Stream has ∂-feedback.

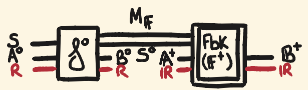
- feedback is defined coinductively

$$\mathbb{F} : (S \cdot \partial \mathbb{S}) \otimes A \to \mathbb{S} \otimes B$$

$$\mathsf{Fbk}_{\mathbb{S}} \mathbb{F} : S \cdot A \to B$$

$$M(\mathsf{Fbk}^S_{\mathbb{S}} \mathbb{F}) := M(\mathbb{F}) \otimes \mathbb{S}^0$$
$$(\mathsf{Fbk}^S_{\mathbb{S}} \mathbb{F})^0 := f^0$$
$$(\mathsf{Fbk}^S_{\mathbb{S}} \mathbb{F})^+ := \mathsf{Fbk}^{S^0}_{\mathbb{S}^+}(\mathbb{F}^+)$$





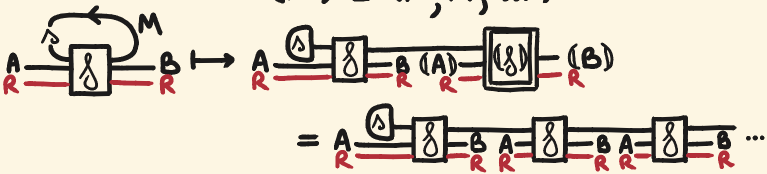
COMPOSITIONAL TRACE SEMANTICS

THEOREM

There is an effectful functor

$$\mathrm{Tr} : \mathrm{Mealy} \to \mathrm{Stream}$$

$$A \mapsto \llparenthesis A \rrparenthesis = (A, A, \dots)$$



TRACE IS UNIVERSAL

THEOREM

The trace functor $\mathrm{Tr} : \mathbf{Mealy} \to \mathbf{Stream}$ is the unique feedback effectful functor determined by freeness of $\mathbf{Mealy}$.

$$\begin{tikzcd} \mathbf{FbkEffCat} \arrow[d, bend left] \\ \mathbf{EffCat} \arrow[u, bend left, "\mathbf{Mealy}"] \arrow[u, phantom, "\dashv"] \end{tikzcd} \quad \Rightarrow \quad \exists!\ \mathrm{Tr} : \begin{tikzcd} \mathbf{Mealy}_{(\mathcal{V},\mathcal{L},\mathcal{C})} \arrow[rr] \arrow[dr] & {} \arrow[d, phantom, "="] & \mathbf{Stream}_{(\mathcal{V},\mathcal{L},\mathcal{C})} \\ & \mathbf{Mealy}_{(\mathcal{V},\mathcal{L},\mathcal{C})}/\mathrm{bisim} \arrow[ur] & \end{tikzcd}$$

COROLLARY

Bisimilarity implies trace equivalence.

OUTLINE

- Effectful copy-discard categories
- Effectful Mealy machines & bisimulations
- Coinductive traces

[• Causal traces]

STREAM COMPUTATIONS

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

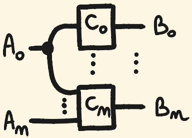
  [Raney (1958)] shows that they are
  the executions of deterministic Mealy machines

⇝ is there a similar explicit form for effectful streams ?

CAUSAL STREAM FUNCTIONS

Stream computations $(c_n)_{n \in \mathbb{N}} : A \to B$ in a cartesian category are families $c_n : A_0 \times \cdots \times A_n \longrightarrow B_n$.

⇝ $c_n(a_0, \ldots, a_n) \in B_n$ is the output at time n



reconstructs the outputs <u>until</u> time n

[Sprunger & Katsumata (2019), Uustalu & Vene (2008)]

STOCHASTIC PROCESSES

Stochastic stream computations $(p_n)_{n\in\mathbb{N}} : \mathbb{A} \to \mathbb{B}$
are families $p_n : A_0 \times \dots \times A_n \longrightarrow \mathcal{D}(B_0 \times \dots \times B_n)$
such that $p_n(a_0, \dots, a_n) = \sum_{a \in A_{n+1}} p_{n+1}(a_0, \dots, a_n, a)$.

⇝ $p_n(a_0, \dots, a_n) \in \mathcal{D}(B_0 \times \dots \times B_n)$ is the distribution of the outputs <u>until</u> time n

↳ the outputs may be correlated

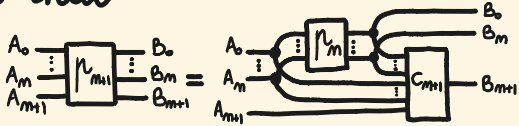
Is there a monoidal version of causal stream functions?

CAUSAL PROCESSES

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

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

such that



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

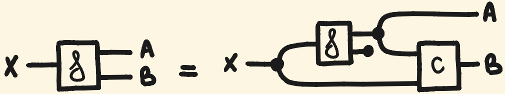
⇝ p_n determines the input-output behaviour <u>until</u> time n

COMPOSING CAUSAL PROCESSES

$\mathcal{C}$ copy-discard

CONDITIONALS [Cho & Jacobs (2017), Fritz (2020), EDL & Román (2023)]

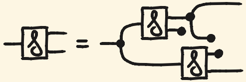
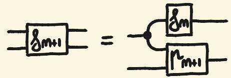
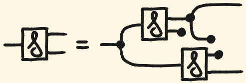
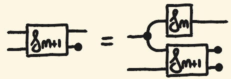
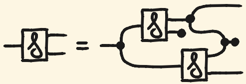
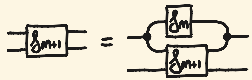
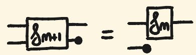
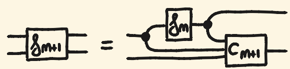
For all $f : X \to A \otimes B$ there is $c : A \otimes X \to B$ st



THEOREM

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

CAUSAL PROCESSES : EXAMPLES

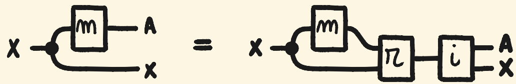
	CONDITIONALS	CAUSALITY CONDITION
Set		
Par		
Rel		
Stoch		
pStoch		

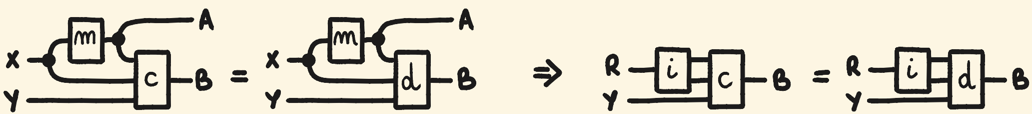
CAUSAL PROCESSES ARE STREAMS

$\mathcal{C}$ copy-discard

RANGES

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





THEOREM

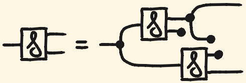
Consider $({\color{blue}\mathrm{fun}\mathcal{C}}, {\color{red}\mathrm{tot}\,\mathcal{C}}, \mathcal{C})$.
If $\mathcal{C}$ has conditionals and ranges,

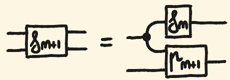
$$\mathrm{Proc} \simeq \mathrm{Stream}.$$

TRACES ARE EFFECTFUL TRACES

CONDITIONALS | CAUSALITY CONDITION | TRACE PREDICATE

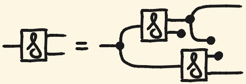
Set

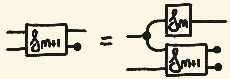




$s_0 = s \wedge \forall i \leq n$
$(s_{i+1}, b_i) = f(s_i, a_i)$

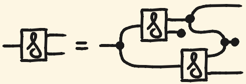
Par

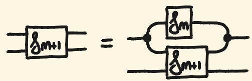




$s_0 = s \wedge \forall i \leq n$
$(s_{i+1}, b_i) = f(s_i, a_i)$

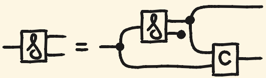
Rel

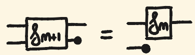




$\exists s_0, \dots, s_{n+1} \quad s_0 \in s$
$\wedge \forall i \leq n \ (s_{i+1}, b_i) \in f(s_i, a_i)$

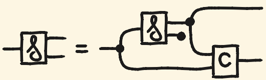
Stoch

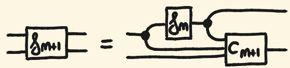




$\sum_{s_0, \dots, s_{n+1}} s(s_0)$
$\cdot \prod_{i \leq n} f(s_{i+1}, b_i \mid s_i, a_i)$

pStoch





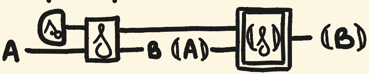
$\sum_{s_0, \dots, s_{n+1}} s(s_0)$
$\cdot \prod_{i \leq n} f(s_{i+1}, b_i \mid s_i, a_i)$

SUMMARY

effectful Mealy machines

bisimilarity

effectful streams



[≃ causal processes]

free construction
~ syntax

uniformity

coalgebraic construction
~ trace semantics

FUTURE WORK

- Adding choice, iteration and higher-order
- Behavioural metrics, metric enrichment
- Coinduction up-to dinaturality
- Tree-like behaviour via final coalgebra of an appropriate φ

[Filippo Bonchi, EDL, Mario Román
Effectful Mealy machines: bisimulation and trace (2025) LiCS]