Topos colloquium 16 May 2024

EFFECTFUL TRACE SEMANTICS VIA EFFECTFUL STREAMS

Filippo Bonchi
Università di Pisa

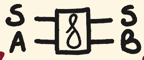
Elena Di Lavore
Università di Pisa

Mario Román
University of Oxford

MEALY MACHINES

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

state space



input / output alphabets

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 $f : S \to F(S)$

input/output

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

non-determinism

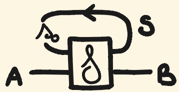
$S \to \mathcal{P}(S \times B)$

- bisimulation is equality in the final coalgebra

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

OVERVIEW

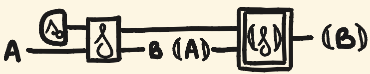
effectful Mealy machines



free construction

~ syntax

effectful streams



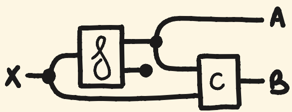
coalgebraic construction

~ semantics

STRING DIAGRAMS & DO-NOTATION

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

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

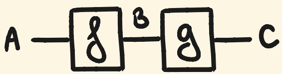


cond(x) = do
  f(x) → (a, b)
  c(a, x) → b'
  return (a, b')

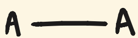
STRING DIAGRAMS & DO-NOTATION

- resources $A, B, \dots$ and processes $f : A \to B$, with possibly multiple inputs/outputs $h : A \to B \otimes B'$, $s : I \to B$

- sequential composition $f ; g : A \to C$ and identities $\mathbb{1}_A : A \to A$



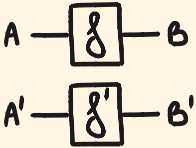

```
comp f g (a) = do
  f(a) → b
  g(b) → c
  return (c)
```




```
id (a) = do
  return (a)
```

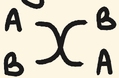
STRING DIAGRAMS & DO-NOTATION

- parallel composition $f \otimes f' : A \otimes A' \to B \otimes B'$

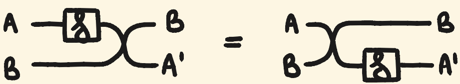



```
tensor f f' (a, a') = do
  f(a) → b
  f'(a') → b'
  return (b, b')
```

- permuting resources $\sigma_{A,B} : A \otimes B \to B \otimes A$

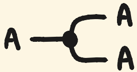



```
swap (a, b) = do
  return (b, a)
```




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

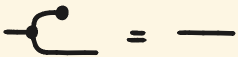
COPY AND DISCARD



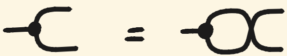

```
copy(a) = do
  return(a,a)
```


```
discard(a) = do
  return()
```

```
copyAssoc(a) = do
  return(a,a,a)
```



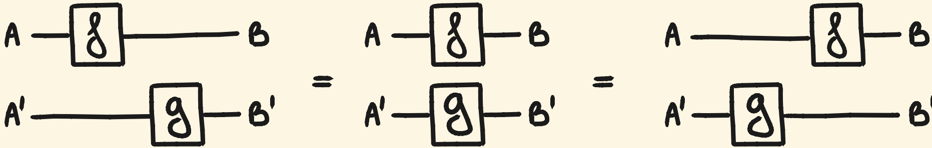
```
copyUnit(a) = do
  return(a)
```



```
copyCommut(a) = do
  return(a,a)
```

[Corradini & Gadducci 1999]

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')
```

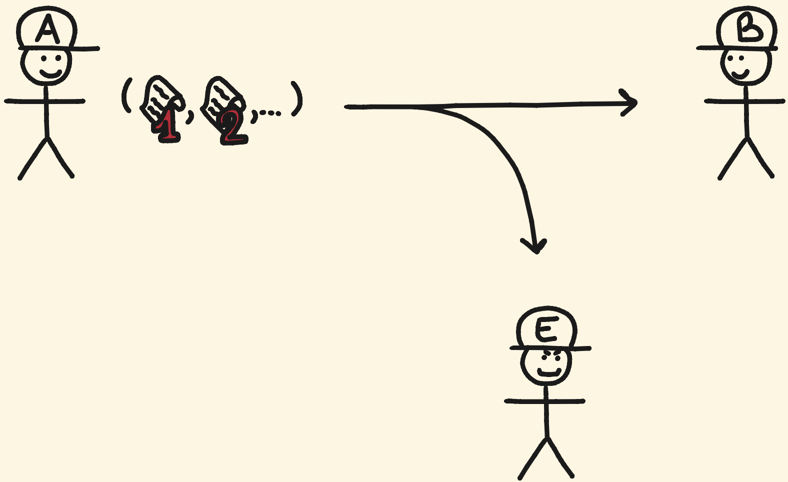
⇝ holds in monoidal categories

OUTLINE

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

A MOTIVATING EXAMPLE

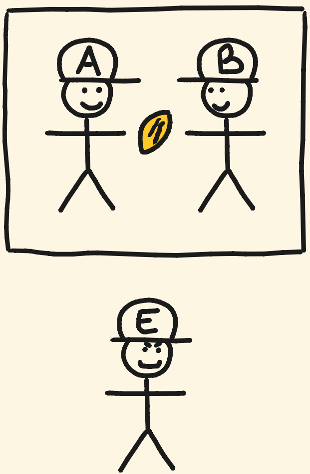
The stream cipher is a simple cryptographic protocol.



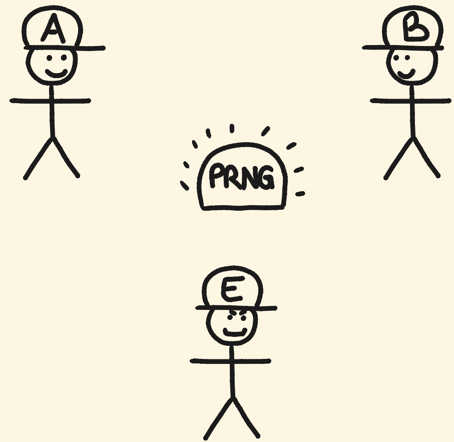
[cf. Broadbent, Karvonen 2022]

STREAM CIPHER PROTOCOL (1)

1. share a seed through a secure channel

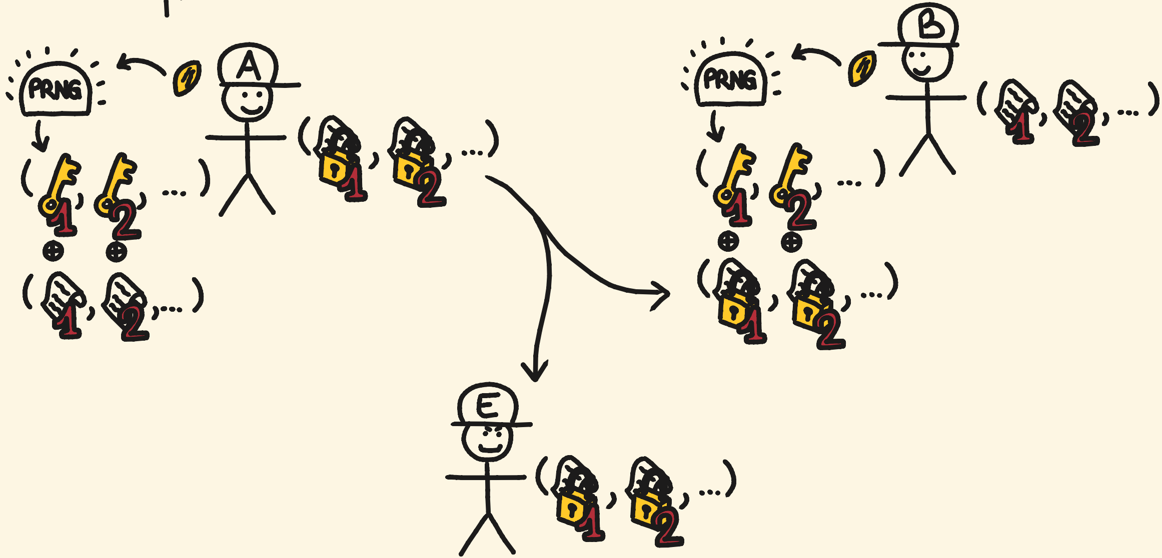


2. share a pseudorandom number generator



STREAM CIPHER PROTOCOL (2)

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



COMPUTATIONS WITH EFFECTS

- Stochastic effects: generating the seed

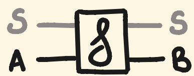
$\mathcal{D} : \mathbf{Set} \to \mathbf{Set}$ distribution monad

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

- Global state: sharing the seed

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

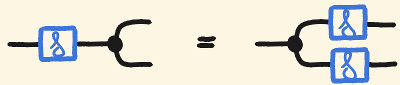
$\mathrm{State}_S(A,B) := \mathcal{C}(S \otimes A, S \otimes B)$



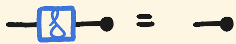
VALUES

Values are both :

- deterministic

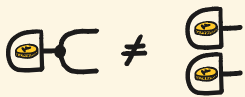


- total

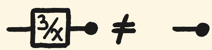


ex $(3\cdot -) : \mathbb{R} \longrightarrow \mathbb{R}$

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

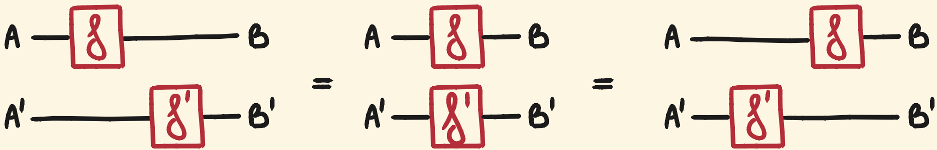


$(3/-) : \mathbb{R} \longrightarrow \mathbb{R}$



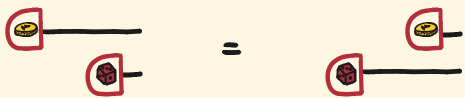
LOCAL COMPUTATIONS

local computations interchange,



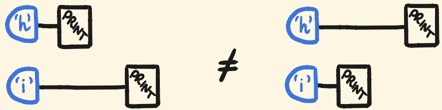
$$\mathrm{localF}(a, a') = \mathrm{do} \quad \begin{array}{|l} f(a) \to b \\ f'(a') \to b' \\ \mathrm{return}\,(b, b') \end{array} \quad = \quad \mathrm{localF}(a, a') = \mathrm{do} \quad \begin{array}{|l} f'(a') \to b' \\ f(a) \to b \\ \mathrm{return}\,(b, b') \end{array}$$

<u>ex</u> Stoch



EFFECTFUL COMPUTATIONS

Effectful computations may have global effects.

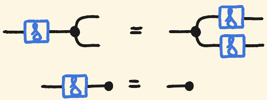


$$
\begin{array}{l}
\mathrm{printHI}(\,) = \mathrm{do} \\
\quad \text{'h'}(\,) \to c_1 \\
\quad \text{'i'}(\,) \to c_2 \\
\quad \mathrm{print}(c_1) \rightsquigarrow (\,) \\
\quad \mathrm{print}(c_2) \rightsquigarrow (\,) \\
\quad \mathrm{return}\ (\,)
\end{array}
\quad \neq \quad
\begin{array}{l}
\mathrm{printIH}(\,) = \mathrm{do} \\
\quad \text{'h'}(\,) \to c_1 \\
\quad \text{'i'}(\,) \to c_2 \\
\quad \mathrm{print}(c_2) \rightsquigarrow (\,) \\
\quad \mathrm{print}(c_1) \rightsquigarrow (\,) \\
\quad \mathrm{return}\ (\,)
\end{array}
$$

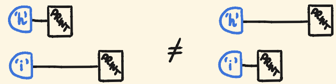
ex state promonads, IO monad

EFFECTFUL COPY-DISCARD CATEGORIES

Values can be copied and discarded (cartesian)

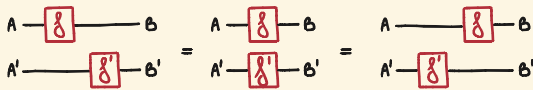


Effectful computations may have global effects (premonoidal)



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

Local computations interchange (monoidal)



ex ($\mathcal{S}et$, $\mathcal{S}toch$, $\mathcal{S}tate_S$)

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

OUTLINE

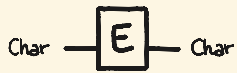
- effectful copy-discard categories
- effectful Mealy machines
- effectful streams
- trace semantics
- causal processes
- bisimulation

STREAM CIPHER COMPONENTS

Encryption protocol

Decryption protocol

Attacker protocol



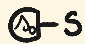
EFFECTFUL MEALY MACHINES

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

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

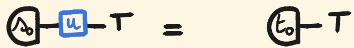
with an initial state

$$s_0 : I \to S$$



A <u>morphism</u> 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

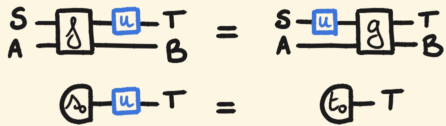


[cf. Katis, Sabadini, Walters 1997 ; EDL, Gianola, Román, Sabadini, Sobociński 2022]

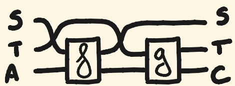
EFFECTFUL CATEGORY OF MEALY MACHINES

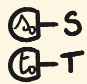
Mealy is an effectful category where

- 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



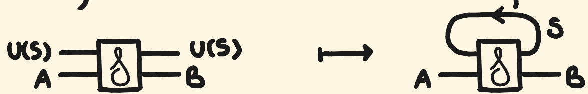


FEEDBACK EFFECTFUL CATEGORIES

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

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

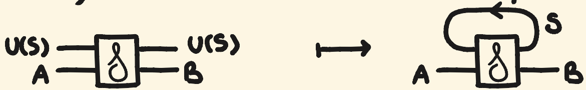


+ axioms

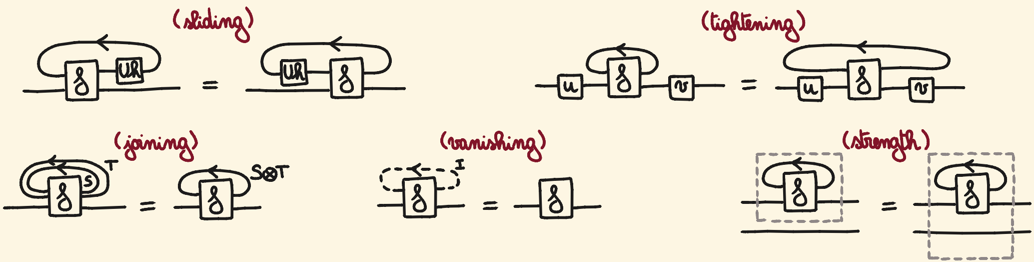
FEEDBACK EFFECTFUL CATEGORIES

U-FEEDBACK

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



satisfying



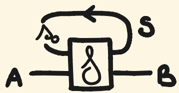
EFFECTFUL CATEGORY OF MEALY MACHINES

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

THEOREM

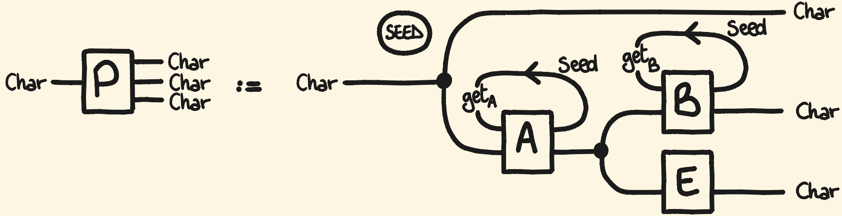
Mealy is the free pointed-feedback category over $\mathcal{C}$.

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



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

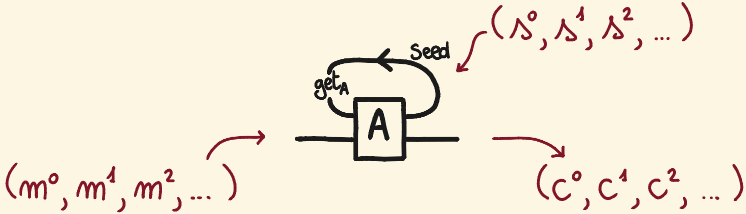
ASSEMBLING THE STREAM CIPHER



OUTLINE

- effectful copy-discard categories
- effectful Mealy machines
- [• effectful streams]
- trace semantics
- 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 $a^0 \in A$
- a stream a^+ of elements of A

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

$$A \times (-) : \mathbf{Set} \to \mathbf{Set}$$

PRACTICAL COINDUCTION

Final coalgebras allow

- coinductive definitions

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

$$\begin{tikzcd} X \arrow[r, dashed, "\exists! h"] \arrow[d, "(f^\circ, f^+)"'] & \mathrm{stream}_A \arrow[d, "(\_^\circ, \_^+)"] \\ A \times X \arrow[r, dashed, "A \times h"'] & A \times \mathrm{stream}_A \end{tikzcd}$$

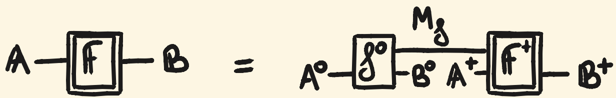
- coinductive proofs

[Kozen & Silva (2017) Practical coinduction]

EFFECTFUL STREAMS

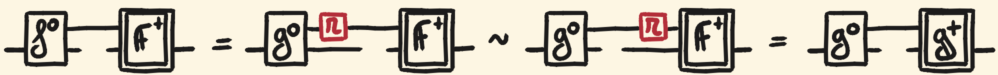
An <u>effectful stream</u> $F : A \to B$ on $(\mathcal{V}, \mathcal{L}, \mathcal{C})$ is

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



quotiented by sliding

$$\begin{cases} f^\circ ; (r \otimes 1) = g^\circ \\ F^+ = r \cdot g^+ \end{cases} \qquad \text{for } r : M_f \to M_g \text{ in } \mathcal{L}$$



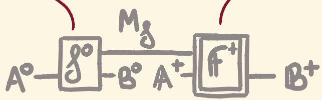
EFFECTFUL STREAMS

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

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

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

quotient by sliding on the memory



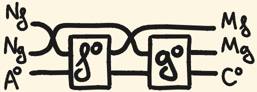
COMPOSITIONAL STRUCTURE OF STREAMS

THEOREM

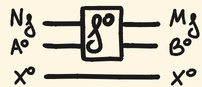
Effectful streams form an effectful category **Stream**.

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

$$\begin{cases} (\mathbb{f} ;_N \mathbb{g})^\circ := \\ (\mathbb{f} ;_N \mathbb{g})^+ := \mathbb{f}^+ ;_M \mathbb{g}^+ \end{cases}$$



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



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

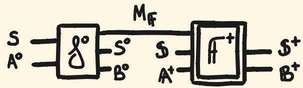
$$\mathbb{F} : (S \cdot \partial \mathbb{S}) \otimes A \longrightarrow \mathbb{S} \otimes \mathbb{B}$$

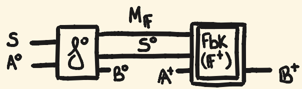
$$\mathsf{Fbk}_{\mathbb{S}} \mathbb{F} : S \cdot A \longrightarrow \mathbb{B}$$

$$M(\mathsf{Fbk}^{S}_{\mathbb{S}} \mathbb{F}) := M(\mathbb{F}) \otimes \mathbb{S}^{\circ}$$

$$(\mathsf{Fbk}^{S}_{\mathbb{S}} \mathbb{F})^{\circ} := f^{\circ}$$

$$(\mathsf{Fbk}^{S}_{\mathbb{S}} \mathbb{F})^{+} := \mathsf{Fbk}^{S^{\circ}}_{\mathbb{S}^{+}} (\mathbb{F}^{+})$$





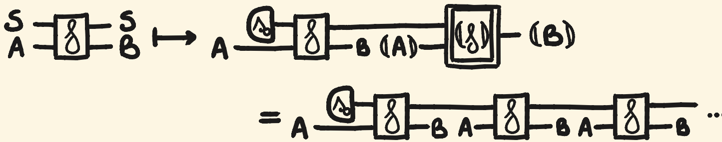
COMPOSITIONAL TRACE SEMANTICS

THEOREM

There is a feedback effectful functor

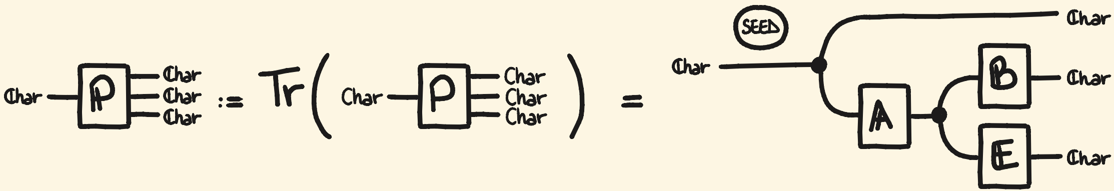
$$Tr : \mathsf{Mealy} \to \mathsf{Stream}$$

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

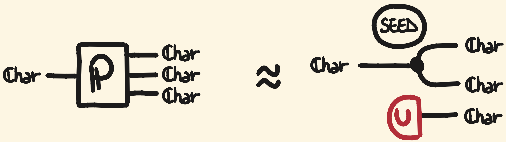


⇝ in Rel these traces coincide with the classical traces

SEMANTICS FOR THE STREAM CIPHER PROTOCOL



SECURITY OF THE PROTOCOL



Alice and Bob see the same message

Eve sees noise

OUTLINE

- effectful copy-discard categories
- effectful Mealy machines
- effectful streams
- trace semantics
- [• 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 $(p_n)_{n \in \mathbb{N}} : \mathbb{A} \to \mathbb{B}$ in a cartesian category are families $p_n : A_0 \times \cdots \times A_n \longrightarrow B_n$.

STOCHASTIC PROCESSES

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

$\rightsquigarrow$ is there a monoidal version ?

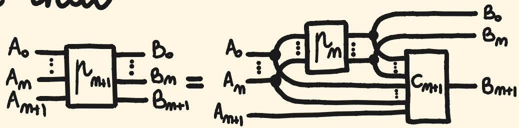
[Sprunger & Katsumata (2019), Uustalu & Vene (2008)]

CAUSAL PROCESSES

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

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

such that



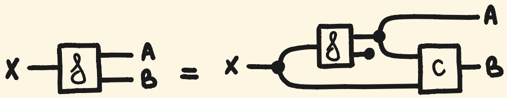
for some $c_{n+1} : B_0 \otimes \cdots \otimes B_n \otimes A_0 \otimes \cdots \otimes A_n \otimes A_{n+1} \to B_{n+1}$

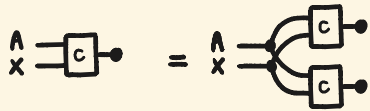
COMPOSING CAUSAL PROCESSES

$\mathcal{C}$ 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

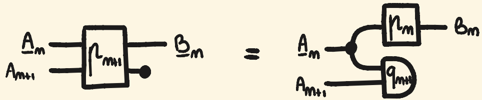
Set

$$p_n : A_0 \times \cdots \times A_n \longrightarrow B_n$$

Par

$$p_n : A_0 \times \cdots \times A_n \longrightarrow (B_0 \times \cdots \times B_n) + 1$$

st



Stoch

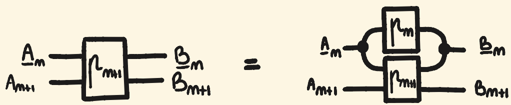
$$p_n : A_0 \times \cdots \times A_n \longrightarrow \mathcal{D}(B_0 \times \cdots \times B_n)$$

st

Rel

$$p_n : A_0 \times \cdots \times A_n \longrightarrow \mathcal{P}(B_0 \times \cdots \times B_n)$$

st

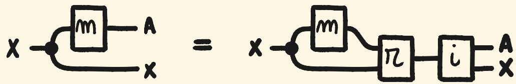


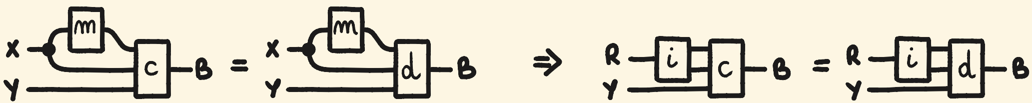
CAUSAL PROCESSES ARE STREAMS

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

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

OUTLINE

- effectful copy-discard categories
- effectful Mealy machines
- effectful streams
- trace semantics
- causal processes

[• bisimulation]

COALGEBRAIC BISIMULATION

A bisimulation is a span of coalgebras.

$$\begin{tikzcd} S \arrow[d, "f"'] & R \arrow[l, "\pi_1"'] \arrow[r, "\pi_2"] \arrow[d, "\alpha"] & T \arrow[d, "g"] \\ F(S) & F(R) \arrow[l, "F(\pi_1)"] \arrow[r, "F(\pi_2)"'] & F(T) \end{tikzcd}$$

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

$$\begin{tikzcd}
& (h_1, R_1, r_1) \arrow[dl, "u_1"'] \arrow[dr, "v_1"] & & \cdots \arrow[dl, "u_2"'] & (h_n, R_n, r_n) \arrow[dr, "v_n"] & \\
(f, S, s) & & (f_1, S_1, s_1) & & & (g, T, t)
\end{tikzcd}$$

THEOREM

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

PROOF: By coinduction. $\square$

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
$$\begin{tikzcd}
 & (h, R, r) \arrow[dl, "u"'] \arrow[dr, "v"] & \\
(f, S, s) & & (g, T, t)
\end{tikzcd}$$

EXAMPLES

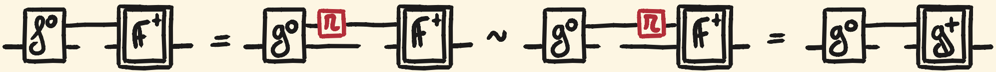
- Set
- Rel
- Stoch
- Par
- pStoch

SUMMARY

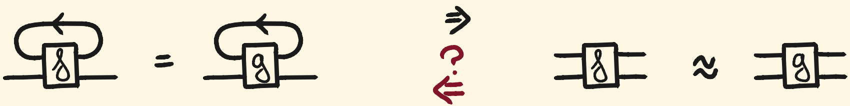
- formal compositional semantics for effectful stream computations
- trace equivalence and bisimulation of effectful Mealy machines
- characterisation as causal stream processes

FUTURE WORK

- coinduction up-to dinaturality



- Rel with explicit failure
- equality in St$\mathcal{C}$ implies bisimulation



- distance instead of equivalence relation for security