Channel Synthesis for Finite Transducers

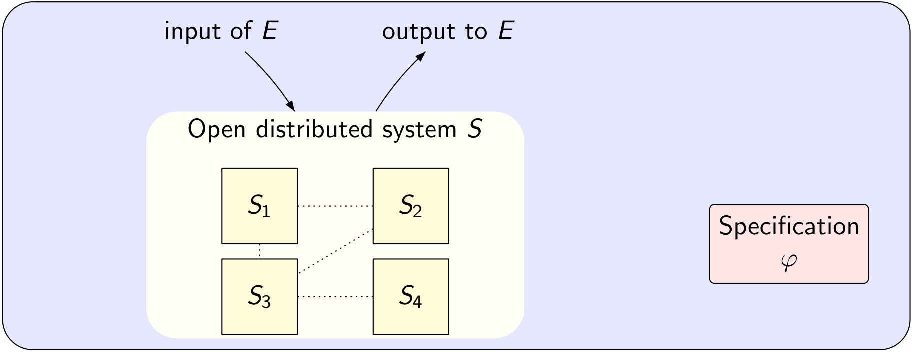
Gilles Benattar[1] Béatrice Bérard[2] Didier Lime[1]
John Mullins[3] Olivier H. Roux[1] Mathieu Sassolas[2]

[1]École Centrale de Nantes, IRCCyN, CNRS UMR 6597
[2]Université Pierre & Marie Curie, LIP6/MoVe, CNRS UMR 7606
[3]École Polytechnique de Montréal

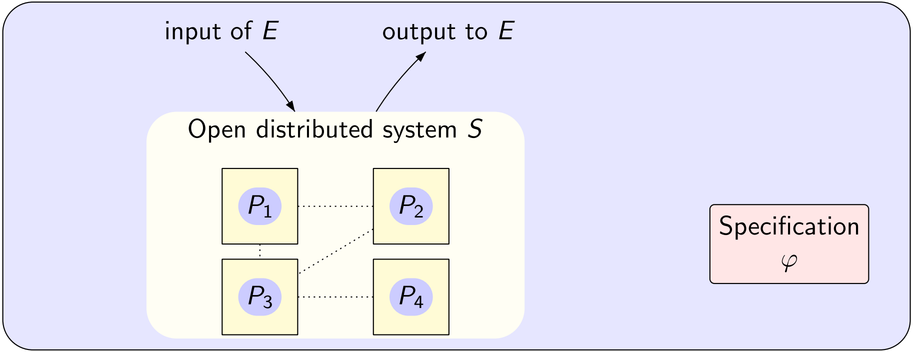
Work partially supported by projects DOTS (ANR-06-SETI-003), CoChaT (Digiteo-2009-HD27), NSERC discovery grant 13321-2007 (Govt of Canada)

13th International Conference on Automata and Formal Languages
August 19th, 2011

Distributed synthesis



Distributed synthesis



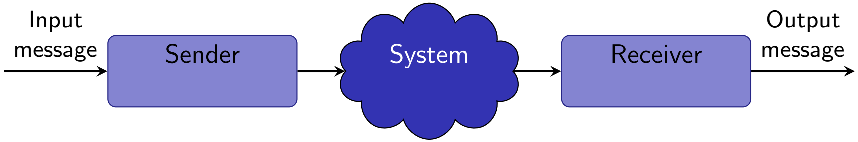
Two problems

- Decide the existence of a distributed program such that the joint behavior $P_1||P_2||P_3||P_4||E$ satisfies φ, for all E.
- Synthesis : If it exists, compute such a distributed program.

$\rightsquigarrow$ Undecidable for asynchronous communication with two processes and total LTL specifications [Schewe, Finkbeiner; 2006].

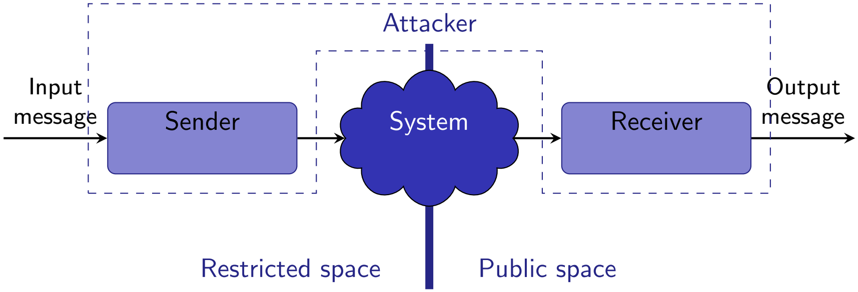
Channel synthesis

- Pipeline architecture with asynchronous transmission
- Simple external specification on finite binary messages :
  output message = input message (perfect data transmission)



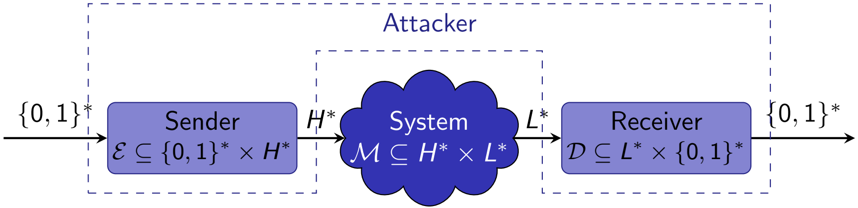
Channel synthesis

- Pipeline architecture with asynchronous transmission
- Simple external specification on finite binary messages :
  output message = input message (perfect data transmission)

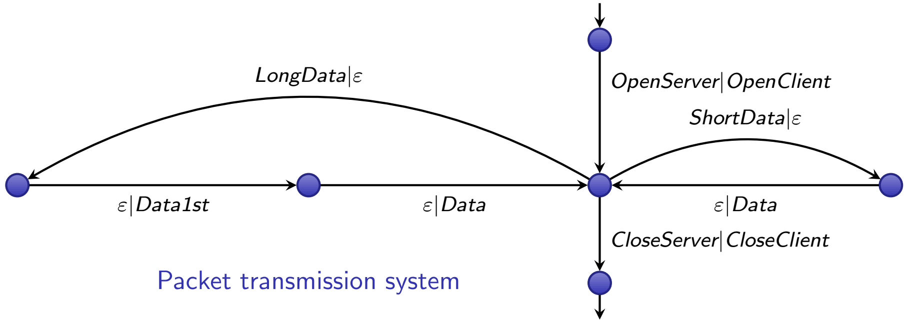


Channel synthesis

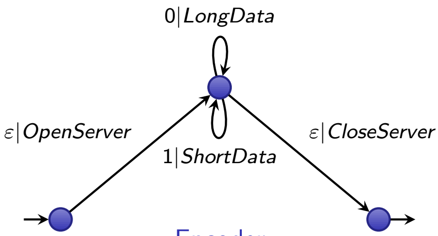
- Pipeline architecture with asynchronous transmission
- Simple external specification on finite binary messages :
  output message = input message (perfect data transmission)
- All processes are finite transducers



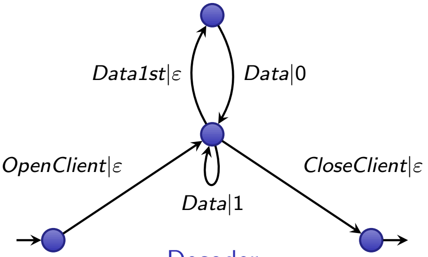
A small example of channel



Packet transmission system



Encoder



Decoder

Channels with transducers

- A transducer is a finite automaton with set of labels $Lab \subseteq A^* \times B^*$, it implements a rational relation.
- The identity relation on A^* is $Id(A^*) = \{(w,w) \mid w \in A^*\}$.
- Rational relations can be composed: $\mathcal{M} \cdot \mathcal{M}'$.

Definition

A channel for a transducer $\mathcal{M}$ is a pair $(\mathcal{E}, \mathcal{D})$ of transducers such that
$$\mathcal{E} \cdot \mathcal{M} \cdot \mathcal{D} = Id(\{0,1\}^*).$$

The definition can be relaxed to take into account bounded delays or errors: existence of such a channel implies existence of a perfect channel.

Decision problems:

- Verification: Given $\mathcal{M}$ and the pair $(\mathcal{E}, \mathcal{D})$, is $(\mathcal{E}, \mathcal{D})$ a channel for $\mathcal{M}$?
- Synthesis: Given $\mathcal{M}$, does there exist a channel $(\mathcal{E}, \mathcal{D})$ for $\mathcal{M}$?

Outline

Results and tools

Verification problem

A necessary condition for synthesis

The synthesis problem

The general case

The case of functional transducers

Conclusion

Results

Theorem

- The channel verification problem is decidable.
- The channel synthesis problem is undecidable.
- If $\mathcal{M}$ is a functional transducer, the synthesis problem is decidable in polynomial time. Moreover, if a channel exists, it can be computed.

Results

Theorem

- The channel verification problem is decidable.
- The channel synthesis problem is undecidable.
- If $\mathcal{M}$ is a functional transducer, the synthesis problem is decidable in polynomial time. Moreover, if a channel exists, it can be computed.

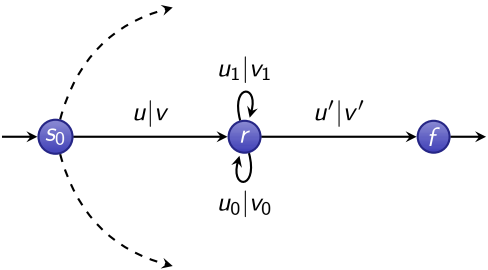
Decision for the verification problem: given $\mathcal{E}$, $\mathcal{M}$ and $\mathcal{D}$

1. Decide whether $\mathcal{E} \cdot \mathcal{M} \cdot \mathcal{D}$ is functional [Schützenberger; 1975], [Béal, Carton, Prieur, Sakarovitch; 2000].
2. If not, it cannot be $Id(\{0,1\}^*)$ which is a functional relation.
3. Otherwise decide whether $\mathcal{E} \cdot \mathcal{M} \cdot \mathcal{D} = Id(\{0,1\}^*)$, which can be done since both relations are functional.

A necessary condition for the existence of a channel

An encoding state in a transducer is a (useful) state r such that:

- there exist cycling pathes: $r \xrightarrow{u_0|v_0} r$ and $r \xrightarrow{u_1|v_1} r$,
- the labels form codes: $u_0 u_1 \neq u_1 u_0$ and $v_0 v_1 \neq v_1 v_0$.

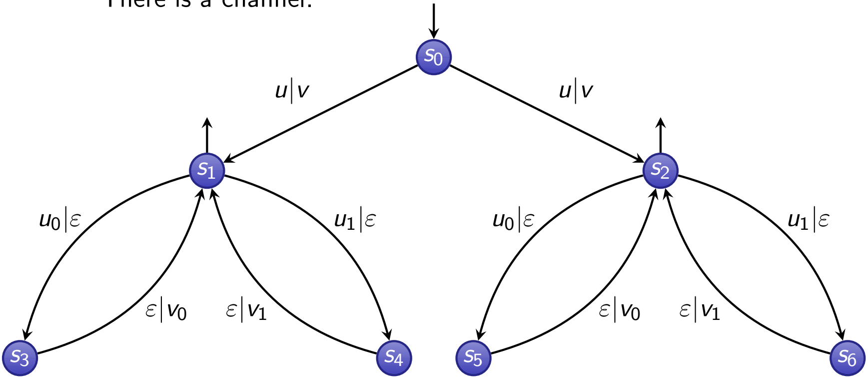


If a transducer admits a channel, then it has an encoding state

An encoding state is not enough

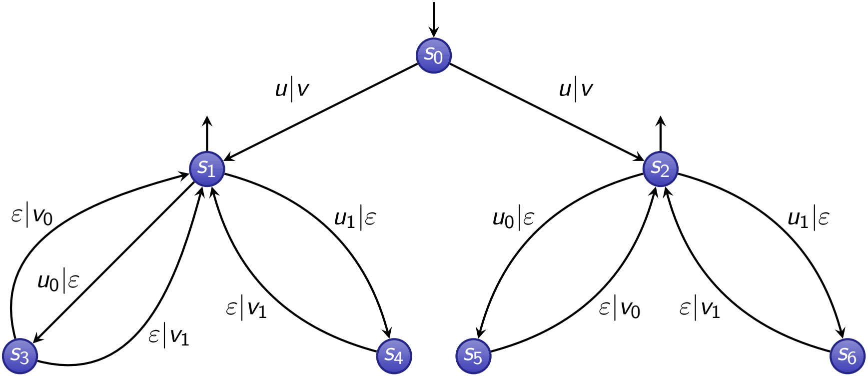
s_1 and s_2 are encoding states.

There is a channel.



An encoding state is not enough

s_1 introduces errors.

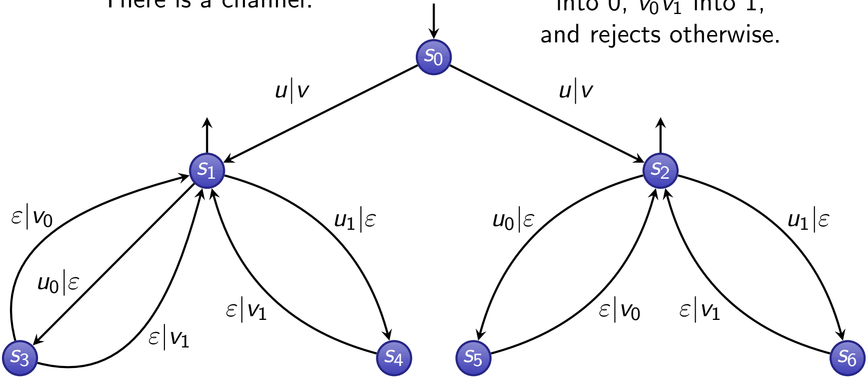


An encoding state is not enough

s_1 introduces errors.

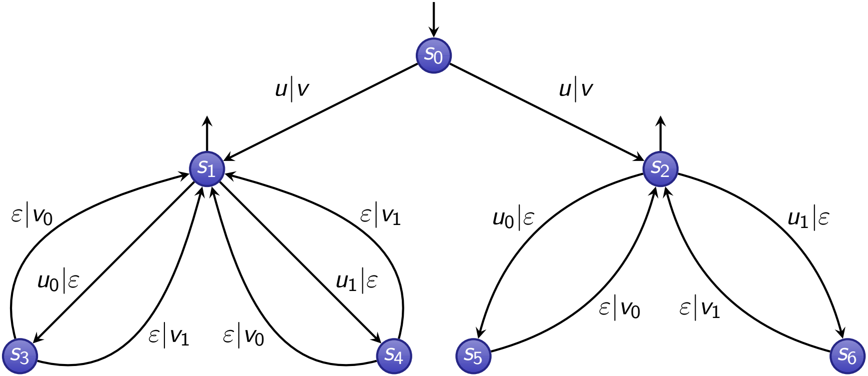
There is a channel.

Encode 0 with $u_1 u_0$ and 1 with $u_0 u_1$. The decoder decodes $v_1 v_0$ into 0, $v_0 v_1$ into 1, and rejects otherwise.



An encoding state is not enough

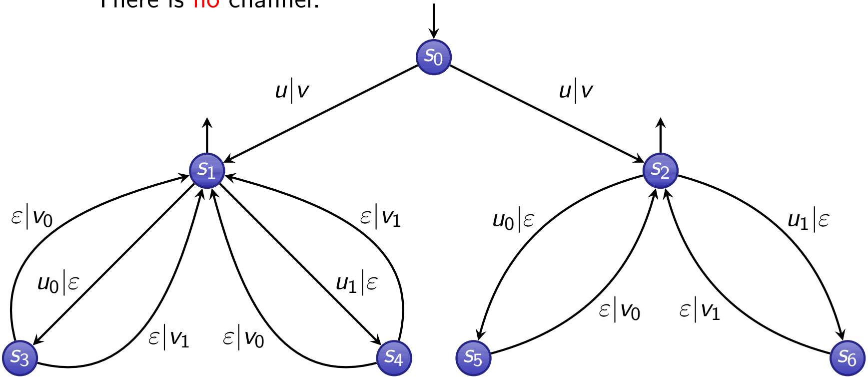
s_1 introduces errors.



An encoding state is not enough

s_1 introduces errors.

There is no channel.



Outline

Undecidability of the synthesis problem

Scheme of the proof: Encoding Post Correspondence Problem.

Given alphabet $\Sigma = \{1, \ldots n\}$ and instance $\mathcal{I} = (x, y)$ of PCP, with morphisms

$$x : \left| \begin{array}{ccc} \Sigma & \rightarrow & A^* \\ i & \mapsto & x_i \end{array} \right. \quad \text{and} \quad y : \left| \begin{array}{ccc} \Sigma & \rightarrow & A^* \\ i & \mapsto & y_i \end{array} \right.$$

a solution is a non empty word $\sigma \in \Sigma^+$ such that $x(\sigma) = y(\sigma)$.

From $\mathcal{I}$, build a transducer $\mathcal{M}_\mathcal{I}$ reading on $\{\top, \bot\} \uplus \Sigma$ and writing on $\{\top, \bot\} \uplus A$ such that:

$$\mathcal{M}_\mathcal{I} \text{ has a channel iff } \mathcal{I} \text{ has a solution}$$

Undecidability of the synthesis problem

Scheme of the proof: Encoding Post Correspondence Problem.

Given alphabet $\Sigma = \{1, \ldots n\}$ and instance $\mathcal{I} = (x, y)$ of PCP, with morphisms

$$x : \left| \begin{array}{ccc} \Sigma & \rightarrow & A^* \\ i & \mapsto & x_i \end{array} \right. \quad \text{and} \quad y : \left| \begin{array}{ccc} \Sigma & \rightarrow & A^* \\ i & \mapsto & y_i \end{array} \right.$$

a solution is a non empty word $\sigma \in \Sigma^+$ such that $x(\sigma) = y(\sigma)$.

From $\mathcal{I}$, build a transducer $\mathcal{M}_\mathcal{I}$ reading on $\{\top, \bot\} \uplus \Sigma$ and writing on $\{\top, \bot\} \uplus A$ such that:

$$\mathcal{M}_\mathcal{I} \text{ has a channel iff } \mathcal{I} \text{ has a solution}$$

Definition of $\mathcal{M}_\mathcal{I}$:

$$\mathcal{M}_\mathcal{I}(b\sigma) = \left(A^+ b\right) \cup \left((A^+ \setminus \{x(\sigma)\})\overline{b}\right) \cup \left((A^+ \setminus \{y(\sigma)\})\overline{b}\right)$$

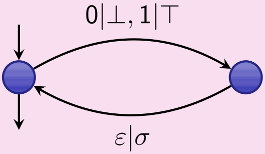
On input $b\sigma$, $\mathcal{M}_\mathcal{I}$ returns an arbitrary (non empty) word on A followed by the input bit b, or its opposite except for $x(\sigma) \cap y(\sigma)$.

On input $b_1\sigma_1 \ldots b_p\sigma_p$, $\mathcal{M}_\mathcal{I}$ returns $\mathcal{M}_\mathcal{I}(b_1\sigma_1) \ldots \mathcal{M}_\mathcal{I}(b_p\sigma_p)$,
with $\mathcal{M}_\mathcal{I}(\varepsilon) = \varepsilon$, and $\mathcal{M}_\mathcal{I}(w) = \emptyset$ otherwise.

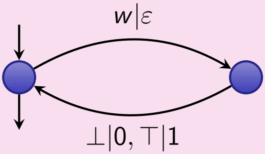
Undecidability (continued)

- The relation $\mathcal{M}_{\mathcal{I}}$ can be realized by a transducer;
- If $x(\sigma) \neq y(\sigma)$ for all $\sigma \neq \varepsilon$, then $\mathcal{M}_{\mathcal{I}}$ outputs $A^+ \cdot \{\top, \bot\}$ for any $b\sigma$ and there can be no channel;
- If $x(\sigma) = y(\sigma) = w$ for some σ, the bit b can be transmitted by detecting w. For example, to transmit 0:
  1. the encoder sends $\bot \cdot \sigma$,
  2. it will be transformed by $\mathcal{M}_{\mathcal{I}}$ into $\left(A^+ \cdot \bot\right) \cup \left((A^+ \setminus \{w\}) \cdot \top\right)$;
  3. the decoder rejects what does not start by w, then reads the bit; in this case, it is $\bot$, which is transformed into 0.

$\mathcal{E}$:



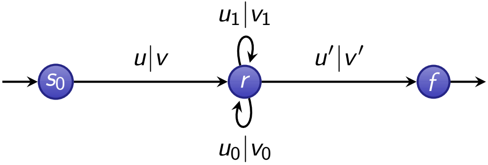
$\mathcal{D}$:



The case of functional transducers

Proposition

If a functional transducer has an encoding state, then it has a channel.



The encoder is $\mathcal{E} = (\varepsilon, u) \cdot \{(0, u_0), (1, u_1)\}^* \cdot (\varepsilon, u')$,
the decoder is $\mathcal{D} = (v, \varepsilon) \cdot \{(v_0, 0), (v_1, 1)\}^* \cdot (v', \varepsilon)$.

$\rightsquigarrow$ The decision procedure consists in finding an encoding state.

Detecting encoding states

Let $\mathcal{M}$ be a functional transducer and s a (useful) state of $\mathcal{M}$

1. Consider $\mathcal{M}_s$, similar to $\mathcal{M}$, with s as initial and final state.
2. Find $u_0 \in A^+$ such that $\mathcal{M}_s(u_0) \neq \varepsilon$, *i.e.* a cycle on s labeled by $u_0|v_0$ with $v_0 \neq \varepsilon$. If all cycles have output ε, s is not an encoding state.
3. Otherwise compute the (rational) set of words $N(v_0) \subseteq Im(\mathcal{M}_s)$ that do not commute with v_0. If $N(v_0)$ is empty, s is not an encoding state.
4. Otherwise compute P the preimage of $N(v_0)$ by $\mathcal{M}_s$, pick $u_1 \in P$ and let $v_1 = \mathcal{M}_s(u_1)$: State s is encoding with cycles $u_0|v_0$ and $u_1|v_1$.

Outline

Conclusion

- The case of synthesis under study is very simple:
  - a simple model: transducers;
  - a simple specification: input = output.

  But the problem is already undecidable !
- An even simpler case, namely functional transducers, is decidable, with polynomial complexity.
- It can nonetheless be used to detect covert communication in systems with limited nondeterminism.
- The complexity gap gives hope for finding intermediate decidable classes:
  - of transducers;
  - of specification.

Thank you

$\top$-half of $\mathcal{M}_{\mathcal{I}}$