

# Channel Synthesis Revisited

Béatrice Bérard<sup>1</sup>   Olivier Carton<sup>2</sup>

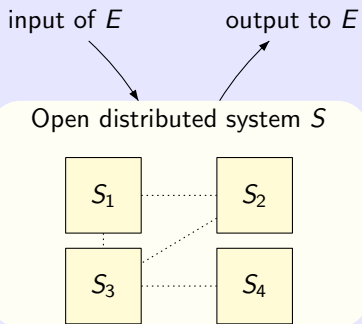
<sup>1</sup>Université Pierre & Marie Curie, LIP6/MoVe, CNRS UMR 7606

<sup>2</sup>Université Paris-Diderot, LIAFA, CNRS UMR 7089

Work partially supported by projects ANR FREC and Coopération France-Québec - 2012/26/SCAC

8th International Conference on Languages and Automata Theory and Applications  
March 10th, 2014

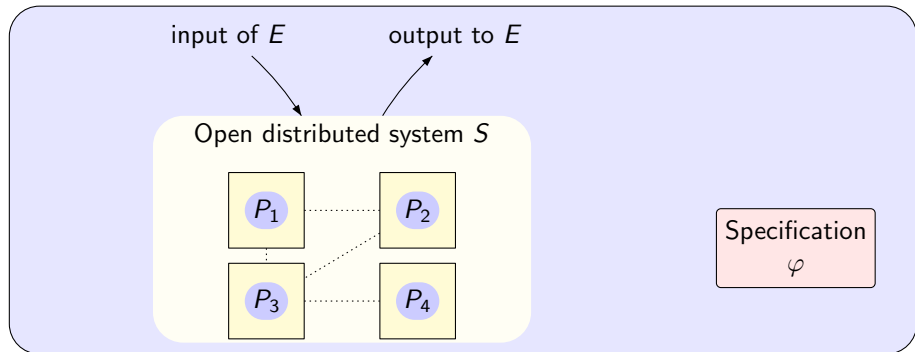
# Distributed synthesis



Specification

$\varphi$

# Distributed synthesis



## Problems

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

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

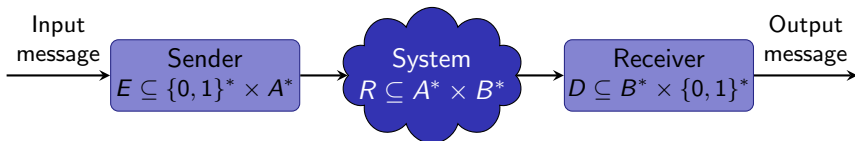
# Channel synthesis

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



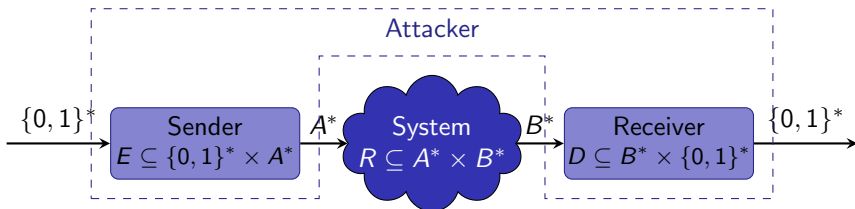
# Channel synthesis

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



# 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**

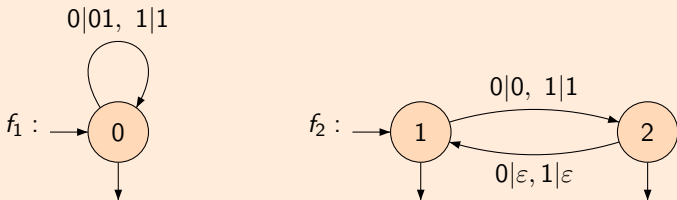


# Finite transducers

A transducer is a finite automaton with set of labels  $Lab \subseteq A^* \times B^*$ , it accepts a rational relation  $R$ ,

- ▶  $dom(R) = \{u \in A^* \mid (u, v) \in R \text{ for some } v \in B^*\}$ ,
- ▶  $range(R) = \{v \in B^* \mid (u, v) \in R \text{ for some } u \in A^*\}$ .

A relation  $R$  realized by a transducer, as a union of two functions:  
 $R = f_1 + f_2$



$R(00) = \{0101, 0\}$  and  $R(01) = \{011, 0\}$ .

$range(f_1) = (01 + 1)^*$  and  $range(f_2) = (0 + 1)^*$ .

# Channels with transducers

- ▶ The identity relation on  $A^*$  is  $Id_{A^*} = \{(w, w) \mid w \in A^*\}$ .
- ▶ Rational relations can be composed:  $RR'$ .

## Definition

A channel for a rational relation  $R$  is a pair  $(E, D)$  of rational relations such that

$$ERD = Id_{\{0,1\}^*}$$

## Problems:

Given  $R$ , does there exist a channel  $(E, D)$  for  $R$ ? If it exists, can it be computed?



# Channels with transducers

- ▶ The identity relation on  $A^*$  is  $Id_{A^*} = \{(w, w) \mid w \in A^*\}$ .
- ▶ Rational relations can be composed:  $RR'$ .

## Definition

A channel for a rational relation  $R$  is a pair  $(E, D)$  of rational relations such that

$$ERD = Id_{\{0,1\}^*}$$

## Problems:

Given  $R$ , does there exist a channel  $(E, D)$  for  $R$ ? If it exists, can it be computed?

## Previous results [BBLMRS 2011]

- ▶ The channel synthesis problem is undecidable.
- ▶ When  $R$  is a function, the problem is decidable and if it exists, the channel can be computed in polynomial time.

# Outline

Growth of languages

Patterns

Conclusion

# Growth of languages

## Definition

For a language  $L$  over alphabet  $A$ , the growth of  $L$  is  $\delta_L$ :

$$\delta_L(n) = \text{card}(L \cap A^{\leq n})$$

$L$  has polynomial growth if  $\delta_L(n)$  is bounded by some polynomial  
finite unions of languages of the form  $u_1 v_1^* \dots u_k v_k^* u_{k+1}$

$L$  has exponential growth if  $\delta_L(n)$  is greater than some exponential  
languages containing some  $u(v + \bar{v})^* w$  (where  $\{v, \bar{v}\}$  is a code)

# Growth of languages

## Definition

For a language  $L$  over alphabet  $A$ , the growth of  $L$  is  $\delta_L$ :

$$\delta_L(n) = \text{card}(L \cap A^{\leq n})$$

$L$  has polynomial growth if  $\delta_L(n)$  is bounded by some polynomial  
finite unions of languages of the form  $u_1 v_1^* \dots u_k v_k^* u_{k+1}$

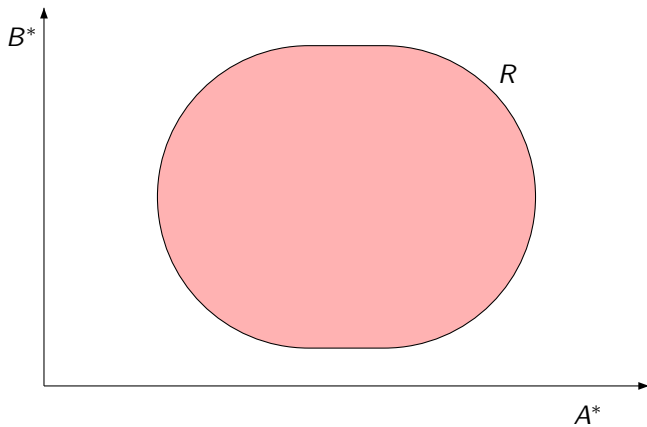
$L$  has exponential growth if  $\delta_L(n)$  is greater than some exponential  
languages containing some  $u(v + \bar{v})^* w$  (where  $\{v, \bar{v}\}$  is a code)

## Rational bijections [Maurer, Nivat; 1980]

- ▶ The growth of a rational language is either polynomial or exponential.
- ▶ There is a rational bijection between two rational languages if and only if they have the same growth:
  - ▶ both finite with same cardinality,
  - ▶ or both polynomial with same degree for the minimal polynomial,
  - ▶ or both exponential.

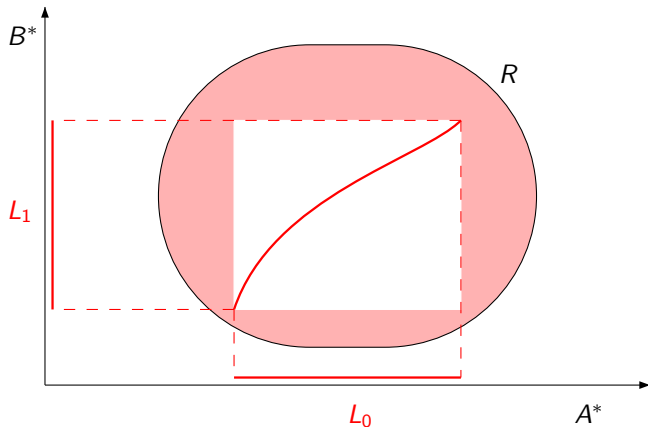
# A characterization of channels

A relation  $R$  has a channel iff there are two rational languages  $L_0$  and  $L_1$  with exponential growth such that  $R \cap (L_0 \times L_1)$  is a bijection between  $L_0$  and  $L_1$ .



# A characterization of channels

A relation  $R$  has a channel iff there are two rational languages  $L_0$  and  $L_1$  with exponential growth such that  $R \cap (L_0 \times L_1)$  is a bijection between  $L_0$  and  $L_1$ .



Uses the Uniformization Theorem [Schützenberger]: Any rational relation  $R$  contains a rational function with same domain.

# Channels for bounded relations

A rational relation  $R$  is bounded by  $k$  iff there exist  $k$  rational functions  $f_1, \dots, f_k$  such that  $R = f_1 + \dots + f_k$ . [Weber; 1996], [Sakarovitch, de Souza; 2008].

For a bounded relation  $R$

$R = f_1 + \dots + f_k$ , where each  $f_i$  is a rational function:

- ▶  $R$  has a channel
- ▶ iff at least one  $f_i$  has a channel
- ▶ iff  $range(R)$  has an exponential growth

# Channels for bounded relations

A rational relation  $R$  is bounded by  $k$  iff there exist  $k$  rational functions  $f_1, \dots, f_k$  such that  $R = f_1 + \dots + f_k$ . [Weber; 1996], [Sakarovitch, de Souza; 2008].

For a bounded relation  $R$

$R = f_1 + \dots + f_k$ , where each  $f_i$  is a rational function:

- ▶  $R$  has a channel
- ▶ iff at least one  $f_i$  has a channel
- ▶ iff  $\text{range}(R)$  has an exponential growth

## Channel synthesis

For  $R$  given as  $f_1 + \dots + f_k$ , where each  $f_i$  is a rational function, the existence of a channel is decidable in linear time. When it exists, the channel can be effectively computed.

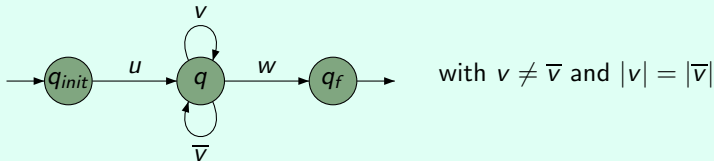


# Patterns

## From exponential growth to patterns

Let  $L$  be accepted by a finite automaton  $\mathcal{A}$ .

Then  $L$  has exponential growth if and only if  $\mathcal{A}$  contains paths:



This can be checked in linear time.

## Definition

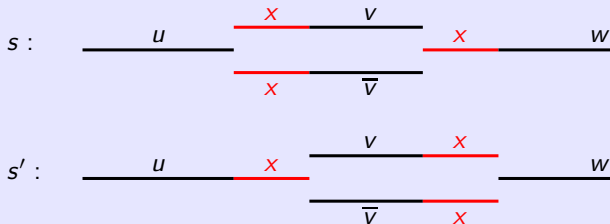
A pattern is a 4-tuple  $s = (u, v, \bar{v}, w)$  such that  $v \neq \bar{v}$  and  $|v| = |\bar{v}|$ .

- ▶ Language of  $s$  :  $L_s = u(v + \bar{v})^* w$
- ▶ Subpattern of  $s$  :  $s' = (ux, y, \bar{y}, zw)$ , with  $x, y, \bar{y}, z \in (v + \bar{v})^*$ .  
Then  $L_{s'} \subseteq L_s$ .

# Conjugated patterns

## Definition

Patterns  $s$  and  $s'$  are **conjugated** if  $s = (u, xv, x\bar{v}, xw)$  and  $s' = (ux, vx, \bar{v}x, w)$  (or  $s' = (ux, \bar{v}x, vx, w)$ ). Then  $L_s = L_{s'}$ .



## Proposition

If  $s$  and  $s'$  are not conjugated, then one of them can be replaced by one of its subpatterns to make the associated languages disjoint. In particular,  $s$  and  $s'$  are conjugated iff  $L_s = L_{s'}$ .

# From patterns to channels

For patterns  $s = (u, v, \overline{v}, w)$  and  $s' = (u', v', \overline{v'}, w')$ , the function  $h_{s,s'}$  with graph  $(u, u')[(v, v') + (\overline{v}, \overline{v'})]^*(w, w')$  is a rational bijection from  $L_s$  onto  $L_{s'}$ .

## Proof of main result and channel synthesis

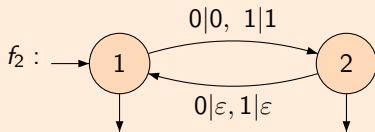
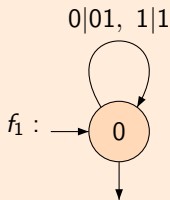
1. If  $f$  is a rational function such that  $\text{range}(f)$  has exponential growth, then there exist patterns  $s$  and  $s'$  such that  $h_{s,s'} \subseteq f$ .
2. If  $R$  has a channel and if  $f$  is a rational function, then  $R + f$  has a channel.

Procedure for  $R = f_1 + \dots + f_k$ :

- ▶ Find a channel for the first  $f_i$  with exponential growth, using 1.
- ▶ Use 2. to iteratively build a channel for  $f_i + f_{i+1}, \dots, f_i + \dots + f_k$ .

# Example: extraction of channel

$$R = f_1 + f_2$$



- For output pattern  $s_1 = (\varepsilon, 011, 101, \varepsilon)$ ,  $L_{s_1} \subseteq (01 + 1)^*$ .  
Corresponding input pattern:  $s = (\varepsilon, 01, 10, \varepsilon)$ , hence  $h_{s,s_1}$  gives a channel for  $f_1$ .
- In  $f_2$ ,  $s$  induces output pattern  $s_2 = (\varepsilon, 0, 1, \varepsilon)$ , but  $L_{s_1} \not\subseteq L_{s_2}$ ,  
so  $h_{s,s_1}$  does not produce a channel for  $R$ .
- Extract sub-pattern  $s' = (\varepsilon, 0101, 1010, \varepsilon)$  from  $s$ , as input pattern for  $f_2$ .  
Corresponding output pattern:  $s_3 = (\varepsilon, 00, 11, \varepsilon)$  not conjugated with  $s_1$ ,  
and  $L_{s_1} \cap L_{s_3} = \emptyset$ .
- Channel  $(E, D)$  for  $R = f_1 + f_2$  is built from  $h_{s',s_3}$ :  
 $E(0) = 0101$ ,  $E(1) = 1010$ , and  $D(00) = 0$ ,  $D(11) = 1$ .

# Conclusion

## Contribution

- ▶ We link the existence of a rational channel with the growth of rational languages, leading to new characterizations.
- ▶ As a consequence, we obtain a linear procedure to decide channel existence for a bounded transducer given as a sum of functions, and synthesis when the answer is positive.

## Future work

- ▶ Investigate more powerful channels, with two-ways or pushdown transducers.
- ▶ Extend the characterization to relations  $R$  such that the size of  $R(u)$  is bounded by a polynomial in  $|u|$ .

Thank you

# A small example of channel

