Channel Synthesis for Finite Transducers

Gilles Benattar\textsuperscript{1}  Béatrice Bérard\textsuperscript{2}  Didier Lime\textsuperscript{1}  John Mullins\textsuperscript{3}  Olivier H. Roux\textsuperscript{1}  Mathieu Sassolas\textsuperscript{2}

\textsuperscript{1}École Centrale de Nantes, IRCCyN, CNRS UMR 6597  
\textsuperscript{2}Université Pierre & Marie Curie, LIP6/MoVe, CNRS UMR 7606  
\textsuperscript{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

input of $E$  

output to $E$

Open distributed system $S$

$S_1$  

$S_2$

$S_3$  

$S_4$

Specification $\phi$
Two 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)
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
A transducer is a finite automaton with set of labels $\text{Lab} \subseteq A^* \times B^*$, it implements a rational relation.

The identity relation on $A^*$ is $\text{Id}(A^*) = \{(w, w) | w \in A^*\}$.

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

$$\mathcal{E} \cdot \mathcal{M} \cdot \mathcal{D} = \text{Id}(\{0, 1\}^*)$$

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 $ld(\{0,1\}^*)$ which is a functional relation.
3. Otherwise decide whether $\mathcal{E} \cdot \mathcal{M} \cdot \mathcal{D} = ld(\{0,1\}^*)$, 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 paths: $r \xrightarrow{u_0|v_0} r$ and $r \xrightarrow{u_1|v_1} r$,
- the labels form codes: $u_0u_1 \neq u_1u_0$ and $v_0v_1 \neq v_1v_0$.

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 $u_1u_0$ and 1 with $u_0u_1$. The decoder decodes $v_1v_0$ into 0, $v_0v_1$ 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

Results and tools
- Verification problem
- A necessary condition for synthesis

The synthesis problem
- The general case
- The case of functional transducers

Conclusion
Undecidability of the synthesis problem

Scheme of the proof: Encoding Post Correspondence Problem.

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

$$
\begin{align*}
  x : & \quad \Sigma \to A^* \\
  & i \mapsto x_i \\
  & \quad \text{and} \\
  y : & \quad \Sigma \to A^* \\
  & i \mapsto y_i
\end{align*}
$$

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

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

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

$$
x : \begin{array}{c|c}
\Sigma & A^* \\
\hline
d_i & x_i
\end{array} \quad \text{and} \quad
y : \begin{array}{c|c}
\Sigma & A^* \\
\hline
d_i & y_i
\end{array}
$$

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 $\{\top, \bot\} \cup \Sigma$ and writing on $\{\top, \bot\} \cup A$ such that:

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

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

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

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 $M_I$ can be realized by a transducer;
- If $x(\sigma) \neq y(\sigma)$ for all $\sigma \neq \varepsilon$, then $M_I$ outputs $A^+ \cdot \{\top, \bot\}$ for any $b\sigma$ and there can be no channel;
- If $x(\sigma) = y(\sigma) = w$ for some $\sigma$, 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 $M_I$ into $(A^+ \cdot \bot) \cup ((A^+ \setminus \{w\}) \cdot \top)$;
  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.

\[\mathcal{E} : \begin{array}{c|c|c}
0 | \bot & , & 1 | \top \\
\varepsilon | \sigma
\end{array} \quad \quad \mathcal{D} : \begin{array}{c|c|c|c}
w | \varepsilon & \quad & \bot | 0, \top | 1
\end{array}\]
The case of functional transducers

Proposition

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

\[
\begin{align*}
E &= (\varepsilon, u) \cdot \{(0, u_0), (1, u_1)\}^* \cdot (\varepsilon, u'), \\
D &= (v, \varepsilon) \cdot \{(v_0, 0), (v_1, 1)\}^* \cdot (v', \varepsilon).
\end{align*}
\]

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

\( \rightarrow \) 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 $\varepsilon$, $s$ is not an encoding state.
3. Otherwise compute the (rational) set of words $N(v_0) \subseteq \text{Im}(\mathcal{M}_s)$ 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

Results and tools
Verification problem
A necessary condition for synthesis

The synthesis problem
The general case
The case of functional transducers

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 $M_I$

$(\top, q_*)$  \(\xrightarrow{\varepsilon|a,T, \ a \in A} q_0\)

$q_0$  \(\xrightarrow{i|\varepsilon, \ i \in \Sigma} T|\varepsilon\)

$(\top, q<)$  \(\xrightarrow{T|\varepsilon} T, y\)

$(\top, q\neq)$  \(\xrightarrow{\varepsilon|\bot} T, x\)

$(\top, q>)$  \(\xrightarrow{T|\varepsilon} T, y\)

$\varepsilon|a, \ a \in A$

$\varepsilon|aT, \ a \in A$

$i|\varepsilon, \ i \in \Sigma$

$\varepsilon|\bot$