Optimal Assumptions for Synthesis

Romain Brenguier

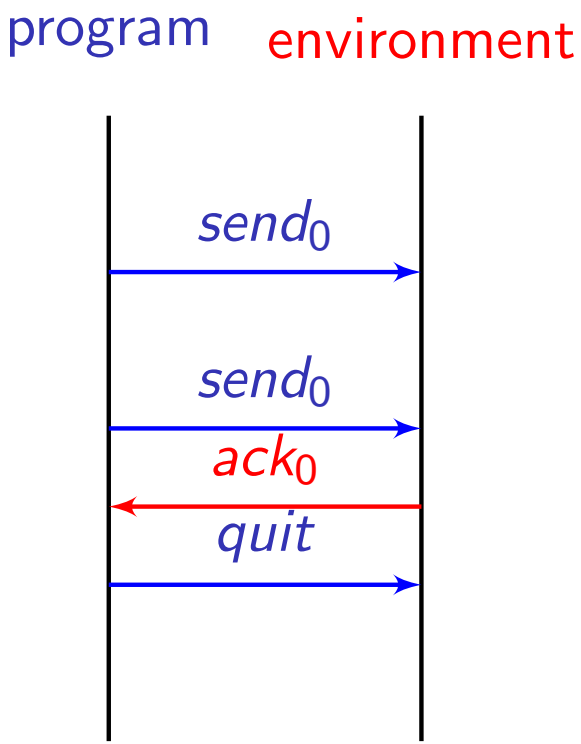
HIGHLIGHTS

diffblue

Church's synthesis problem (1957)

$$Spec \subseteq (\Sigma_{Input} \cdot \Sigma_{Output})^{\omega}$$

A simple protocol



$$Spec = (send_0 \cdot \neg ack_0)^* \cdot send_0 \cdot ack_0 \cdot quit \cdot \Sigma^\omega$$

Assumption

$$A \subseteq (\Sigma_I \cdot \Sigma_O)^\omega$$

Assumption

$$A \subseteq (\Sigma_I \cdot \Sigma_O)^\omega$$

Sufficient assumption

$$\sigma \models A \Rightarrow Spec$$

Assumption

$$A \subseteq (\Sigma_I \cdot \Sigma_O)^\omega$$

Sufficient assumption

$$\sigma \models A \Rightarrow Spec$$

Example

$\mathtt{F}\ ack_0$ is sufficient for the protocol but not optimal

Necessary and sufficient assumption for a strategy

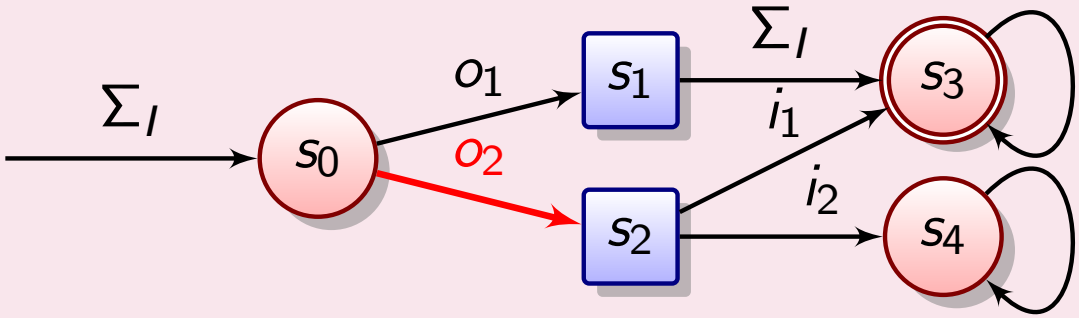
$$\mathsf{A}(\sigma) = \quad \mathit{outcome}(\sigma) \Rightarrow \mathit{Spec}$$

Necessary and sufficient assumption for a strategy

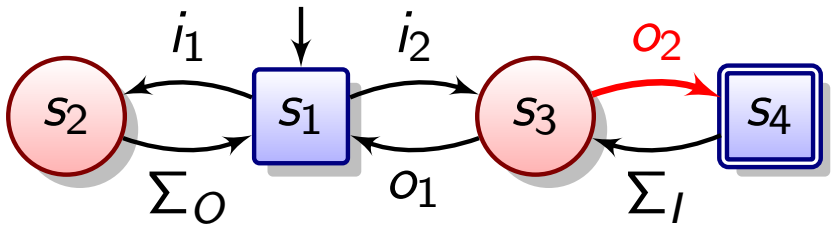
$$\mathsf{A}(\sigma) = \quad \mathit{outcome}(\sigma) \Rightarrow \mathit{Spec}$$

Exercise

Is the assumption corresponding to $\sigma : s_0 \rightarrow o_2$ optimal for *Spec* given by this Büchi automaton?



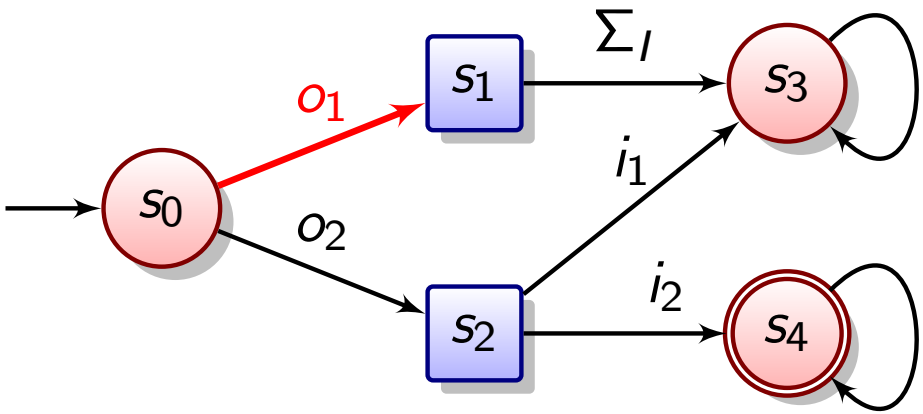
Strongly winning strategies



Theorem

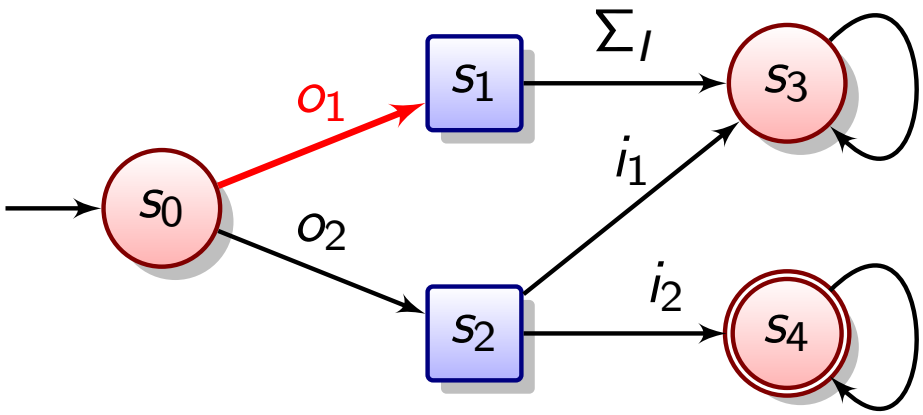
σ strongly winning $\Rightarrow$ $\mathsf{A}(\sigma)$ optimal
A optimal $\Rightarrow$ $\exists\sigma$ strongly winning such that $A = \mathsf{A}(\sigma)$.

Not all assumptions are good



$\sigma : s_0 \rightarrow o_1$

Not all assumptions are good



$\sigma : s_0 \rightarrow o_1$

- strongly winning
- $\mathrm{A}(\sigma) = \neg o_1$
- ensures $A \Rightarrow \mathit{Spec}$ by making sure $\neg A$ holds

Ensurable assumptions

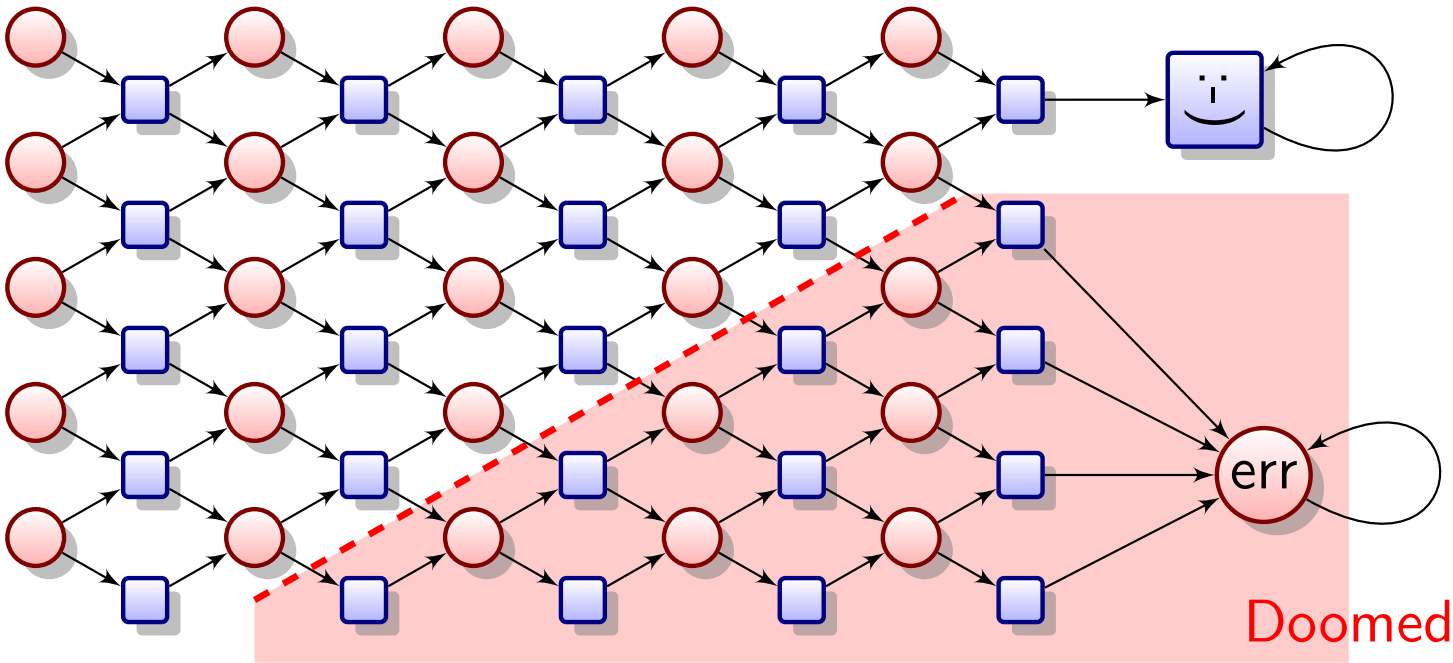
assumption for which the environment has a winning strategy

Exercise: Are these ensurable assumptions?

1) $\mathtt{F} i_1 \Leftrightarrow \mathtt{F} o_1$ 2) $i_1 \Rightarrow \mathtt{F} o_1$

Sufficient and neccessary ensurable assumptions

$$\mathrm{EA}(\sigma) = \mathrm{A}(\sigma) \setminus \mathrm{Doomed}(\sigma)$$

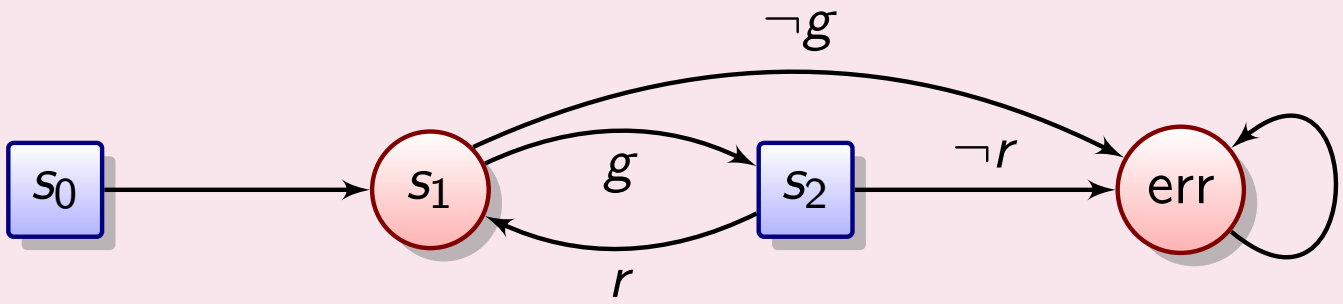


Strategic dominance

σ better than σ' no matter the environement

Exercise

Which strategy dominates the others for this safety specification?



Definition Non-dominated strategy

If there is no σ' which dominates σ, σ is said non-dominated.

Theorem

If σ is non-dominated, then $\mathrm{EA}(\sigma)$ is ensurable optimal.
If A is ensurable optimal, there is σ non-dominated, $A = \mathrm{EA}(\sigma)$.

Automation of the process

$Spec = (send_0 \cdot \neg ack_0)^* \cdot send_0 \cdot ack_0 \cdot quit$

Algorithm

Program σ

```
send_0();
while(!ack_0)
  send_0();
quit();
```

Assumption A

$\neg(\Sigma^* \cdot (send_0 \cdot \neg ack_0))^\omega$

Theorem

Given a parity automaton for *Spec*, we can compute in EXPTIME an ensurable optimal assumption as a parity automaton of poly. size.

Other questions (solved in [CONCUR'16])

- Scenarios: given $Scen$, find assumption A optimal, and program σ such that $Scen \subseteq A \cap outcome(\sigma)$
- Generalisation: given A sufficient, find assumption A', A' optimal s.t. $A \subseteq A'$
- Input-assumption: restriction only on inputs
  $\forall w, w' \in (\Sigma_I \cdot \Sigma_O)^\omega.\ \pi_I(w) = \pi_I(w') \wedge w \in A \Rightarrow w' \in A$

  Example: if inputs are read from a file, it does not make sense to have assumptions like $\mathtt{F}(o_1) \Leftrightarrow \mathtt{F}(i_1)$.

Conclusion

- Notion of optimal assumption based on language inclusion
- Ensurable assumptions are more relevant
- Characterised by admissible strategies
- Computable as parity automata

Future work

- Complexity of remorse-free strategies
- Implementation
- Quantitative setting