# Deducible information flow

Cătălin Dima

LACL, Université Paris 12

Joint work with E. Asarin, C. Enea, R. Gramatovici

# A wide span of approaches to information flow

- Noninterference following Goguen & Meseguer:
  - One group of users [...] is noninterfering with another group of users if what the first group of users does [...] has no effect on what the second group of users can see.
- Various formalizations:
  - Trace based – Noninterference, Separability, Generalized Noninterference, Nondeducibility on Strategies, the “Perfect Security Property”, Forward Correctability, etc.
  - Bisimulation based – Bisimulation-based Nondeducibility on Compositions.
  - Compositionality based – the Selective Interleaving Functions (McLean).
  - Language based – Denning, Volpano & Smith.
  - Logic based – deontic logic (Fr. Cuppens, Halpern & O’Neill).

# A wide span of approaches to information flow

- Noninterference following Goguen & Meseguer:
  - One group of users [...] is noninterfering with another group of users if what the first group of users does [...] has no effect on what the second group of users can see.
- Various formalizations:
  - Trace based – Noninterference, Separability, Generalized Noninterference, Nondeducibility on Strategies, the “Perfect Security Property”, Forward Correctability, etc.
  - Bisimulation based – Bisimulation-based Nondeducibility on Compositions.
  - Compositionality based – the Selective Interleaving Functions (McLean).
  - Language based – Denning, Volpano & Smith.
  - Logic based – deontic logic (Fr. Cuppens, Halpern & O’Neill).

# A wide span of approaches to information flow

- Noninterference following Goguen & Meseguer:
  - One group of users [...] is noninterfering with another group of users if what the first group of users does [...] has no effect on what the second group of users can see.
- Various formalizations:
  - Trace based – Noninterference, Separability, Generalized Noninterference, Nondeducibility on Strategies, the “Perfect Security Property”, Forward Correctability, etc.
  - Bisimulation based – Bisimulation-based Nondeducibility on Compositions.
  - Compositionality based – the Selective Interleaving Functions (McLean).
  - Language based – Denning, Volpano & Smith.
  - Logic based – deontic logic (Fr. Cuppens, Halpern & O’Neill).

# A wide span of approaches to information flow

- Noninterference following Goguen & Meseguer:
  - One group of users [...] is noninterfering with another group of users if what the first group of users does [...] has no effect on what the second group of users can see.
- Various formalizations:
  - Trace based – Noninterference, Separability, Generalized Noninterference, Nondeducibility on Strategies, the "Perfect Security Property", Forward Correctability, etc.
  - Bisimulation based – Bisimulation-based Nondeducibility on Compositions.
  - Compositionality based – the Selective Interleaving Functions (McLean).
  - Language based – Denning, Volpano & Smith.
  - Logic based – deontic logic (Fr. Cuppens, Halpern & O'Neill).

# A wide span of approaches to information flow

- Noninterference following Goguen & Meseguer:
  - One group of users [...] is noninterfering with another group of users if what the first group of users does [...] has no effect on what the second group of users can see.
- Various formalizations:
  - Trace based – Noninterference, Separability, Generalized Noninterference, Nondeducibility on Strategies, the “Perfect Security Property”, Forward Correctability, etc.
  - Bisimulation based – Bisimulation-based Nondeducibility on Compositions.
  - Compositionality based – the Selective Interleaving Functions (McLean).
  - Language based – Denning, Volpano & Smith.
  - Logic based – deontic logic (Fr. Cuppens, Halpern & O’Neill).

# A wide span of approaches to information flow

- Noninterference following Goguen & Meseguer:
  - One group of users [...] is noninterfering with another group of users if what the first group of users does [...] has no effect on what the second group of users can see.
- Various formalizations:
  - Trace based – Noninterference, Separability, Generalized Noninterference, Nondeducibility on Strategies, the “Perfect Security Property”, Forward Correctability, etc.
  - Bisimulation based – Bisimulation-based Nondeducibility on Compositions.
  - Compositionality based – the Selective Interleaving Functions (McLean).
  - Language based – Denning, Volpano & Smith.
  - Logic based – deontic logic (Fr. Cuppens, Halpern & O’Neill).

- Information flow is about creating covert channels.
  - Trace-based and bisimulation-based approaches.
- Information flow is about deduction of high-level activity.
  - Language-based approaches.
- Is the following program (system) safe?

```
x:  High integer;
read(x);
write_low(2);
```

- Yes (Denning, Volpano & Smith) : no information is revealed about the value of x.
- No (some of the trace-based or models) : Harry can input a noninteger real, or choose not to input any value, and this crashes the system.

- Information flow is about creating covert channels.
  - Trace-based and bisimulation-based approaches.
- Information flow is about deduction of high-level activity.
  - Language-based approaches.
- Is the following program (system) safe?

```
x:  High integer;
read(x);
write_low(2);
```

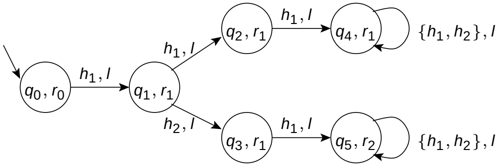
- Yes (Denning, Volpano & Smith) : no information is revealed about the value of x.
- No (some of the trace-based or models) : Harry can input a noninteger real, or choose not to input any value, and this crashes the system.

- Can we relate different views of information flow?
- Can we specify the (quantity of) information that can be leaked in a system?
- Can we specify some strategy for Larry to “maximize” his information about Harry’s choices?

- Can we relate different views of information flow?
- Can we specify the (quantity of) information that can be leaked in a system?
- Can we specify some strategy for Larry to “maximize” his information about Harry’s choices?

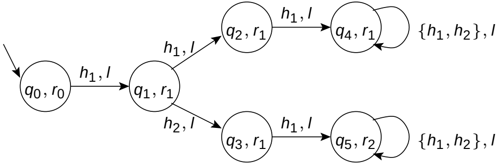
- Can we relate different views of information flow?
- Can we specify the (quantity of) information that can be leaked in a system?
- Can we specify some strategy for Larry to “maximize” his information about Harry’s choices?

- Events : inputs and outputs.
  - High-level inputs $H$.
  - Low-level inputs $L$.
  - States $Q$.
  - High-level outputs $\chi : Q \to Q_H$
  - Low-level outputs $\lambda : Q \to Q_L$
- Transitions $\delta \subseteq Q \times H \times L \times Q$.
  - Synchronous model.
  - Nondeterministic system decisions.
  - Nondeterministic variant of Johnson & Wittbold.



# Strategies

- (The set of) $\infty$-strategy for $H$: $\mathrm{Str}_H^\infty = \{s : Q_H^* \to H\}$.
- (The set of) $n$-strategy for $H$: $\mathrm{Str}_H^n = \{s : Q_H^{\leq n-1} \to H\}$.



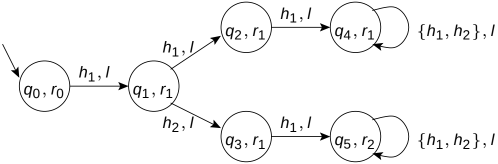

$$\begin{array}{llll} s_1(\epsilon) = h_1 & s_1(q_1) = h_1 & s_1(q_1 q_2) = h_1 & s_1(w) = h_1 \text{ otherwise} \\ s_2(\epsilon) = h_1 & s_2(q_1) = h_2 & s_2(q_1 q_3) = h_2 & s_2(w) = h_1 \text{ otherwise} \end{array}$$

- Run $\rho_1 = (q_0, r_0) \xrightarrow{h_1, l} (q_1, r_1)$
  - $\rho_1$ compatible with both strategies.
- Run $\rho_2 = (q_0, r_0) \xrightarrow{h_1, l} (q_1, r_1) \xrightarrow{h_2, l} (q_3, r_1)$
  - Compatible only with strategy $s_2$.

# Covert channel capacity

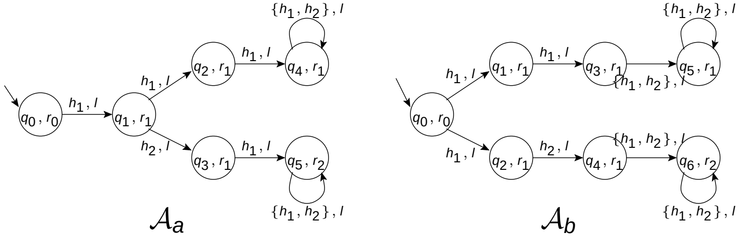
- Given $s \in \mathrm{Str}_H^\infty$, $\mathrm{Obs}_L(s)$ is the set of low-level observable behaviors compatible with $s$.
  - I.e. projections onto $L \times Q_L$ of runs compatible with $s$.
- Covert channel capacity:

$$K_\mathcal{A} = card(B_\mathcal{A}) - 1 \quad \text{where} \quad B_\mathcal{A} = \{\mathrm{Obs}_L(s) \mid s \in \mathrm{Str}_H^\infty\}$$



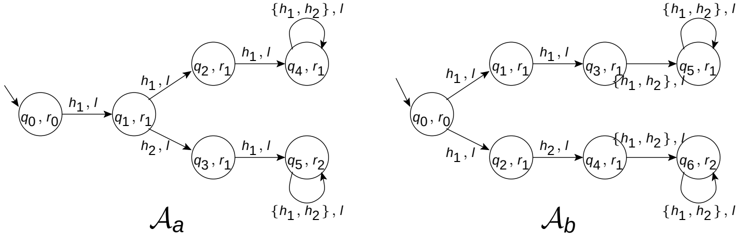

  - $K_\mathcal{A} = 4$, since 5 classes of the type $\mathrm{Obs}_L(s)$.

- Compare the two systems below:




- Both have $K_{\mathcal{A}} = 4$...
- ... but are they really similar?
  - In $\mathcal{A}_a$, Harry has a choice in state $(q_1, r_1)$ between two admissible actions.
  - In $\mathcal{A}_b$, the system has a choice in state $(q_0, r_0)$.
- So, if we consider only admissible actions, $\mathcal{A}_b$ is better than $\mathcal{A}_a$.

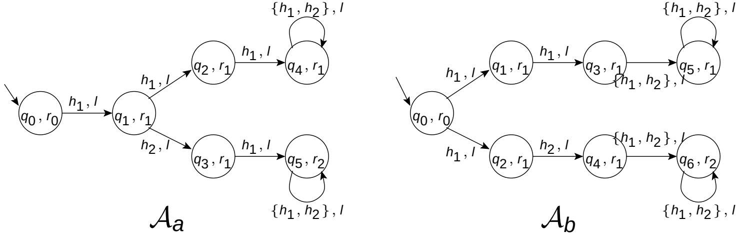
- Compare the two systems below:




- Both have $K_{\mathcal{A}} = 4$...
- ... but are they really similar?
  - In $\mathcal{A}_a$, Harry has a choice in state $(q_1, r_1)$ between two admissible actions.
  - In $\mathcal{A}_b$, the system has a choice in state $(q_0, r_0)$.
- So, if we consider only admissible actions, $\mathcal{A}_b$ is better than $\mathcal{A}_a$.

# Admissible strategies

- $s \in \mathrm{Str}_H^n$ is admissible if every run $\rho$ of length $m \leq n$ which is compatible with $s$ is a prefix of a run $\rho'$ of length $n$ which is compatible with $s$ too.
- The set of admissible $\infty$-strategies for $H$ : $\mathrm{Adm}_H^\infty$.

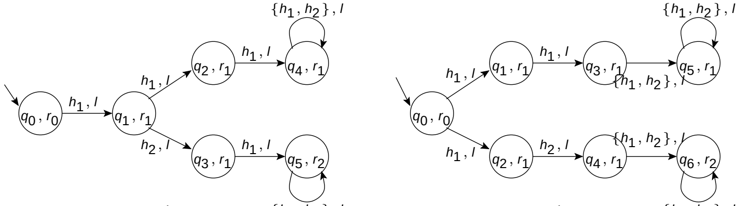



- $\mathcal{A}_a$ has two admissible $\infty$-strategies, $\mathcal{A}_b$ has only one.

# Admissible covert channel capacity

- The admissible covert channel capacity allowed by the system $\mathcal{A}$ is

$$Ka_{\mathcal{A}} = card(Ba_{\mathcal{A}}) - 1 \quad \text{where} \quad Ba_{\mathcal{A}} = \{\mathrm{Obs}_L(s) \mid s \in \mathrm{Adm}_H^{\infty}\}$$



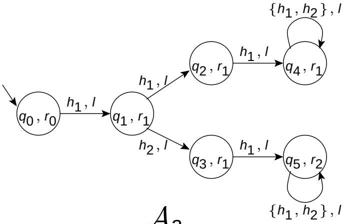

$\mathcal{A}_a$ $\mathcal{A}_b$

- $Ka_{\mathcal{A}_a} = 1, Ka_{\mathcal{A}_b} = 0.$
- If we transform a system $\mathcal{A}$ into another system $\mathcal{B}$ by appending a trash state, then $K_{\mathcal{A}} = Ka_{\mathcal{B}}$.

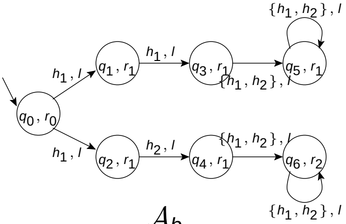
# Admissible covert channel capacity

- The admissible covert channel capacity allowed by the system $\mathcal{A}$ is

$$Ka_{\mathcal{A}} = card(Ba_{\mathcal{A}}) - 1 \quad \text{where} \quad Ba_{\mathcal{A}} = \left\{ \mathrm{Obs}_L(s) \mid s \in \mathrm{Adm}_H^{\infty} \right\}$$




$\mathcal{A}_a$




$\mathcal{A}_b$

- $Ka_{\mathcal{A}_a} = 1, Ka_{\mathcal{A}_b} = 0.$
- If we transform a system $\mathcal{A}$ into another system $\mathcal{B}$ by appending a trash state, then $K_{\mathcal{A}} = Ka_{\mathcal{B}}$.

# The example program

```
x:  High integer;
read(x);
write_low(2);
```

- Has zero admissible covert channel capacity.
- Has non-zero covert channel capacity.

# Deducible information flow

- Given $\theta \in \mathsf{Runs}^{\leq n}(\mathcal{A}_L)$ (low-level observation of a run in $\mathcal{A}$), Larry's knowledge after observing $\theta$ is the set of $n$-strategies compatible with $\theta$.

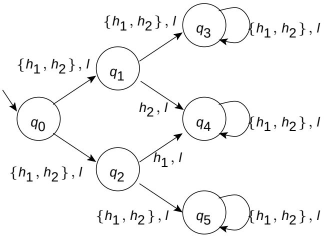
$$\mathsf{knl}(\theta, \mathsf{Tr}) = \{s \in \mathsf{Adm}_H^n \mid \exists \rho \in \mathsf{Runs}(\mathcal{A}) \text{ s.t. } \theta = \rho\big|_L \text{ and } s \text{ is compatible with } \rho\}$$

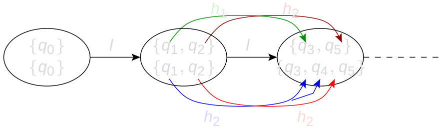
- $\mathcal{A}$ **has no deducible information flow** if $\forall \theta_1, \theta_2 \in \mathsf{Runs}(\mathcal{A}_L)$ with $\theta_1 \preceq \theta_2$,

$$\mathsf{knl}(\theta_1, \mathsf{Tr}) \preceq \mathsf{knl}(\theta_2, \mathsf{Tr})$$

  - Getting more information means excluding some strategies.
  - Kripke-style model of information flow.

# Decidability

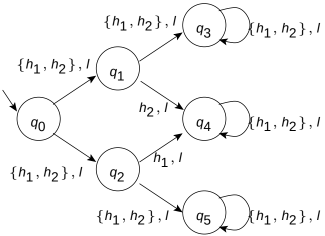


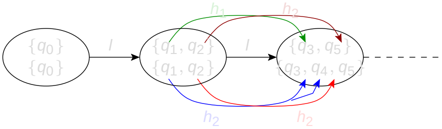




- $\lambda(q_0) = r_0, \lambda(q_1) = \lambda(q_2) = r_1, \lambda(q_3) = r_3, \lambda(q_4) = r_4, \lambda(q_5) = r_5.$
- Construct pairs of finite-state strategies.
- Check whether only pairs of sets of states having the same low-level projection are constructed:

$$\lambda(\{q_3, q_5\}) = \{r_3, r_5\} \neq \lambda(\{q_3, q_4, q_5\}) = \{r_3, r_4, r_5\}$$

# Decidability

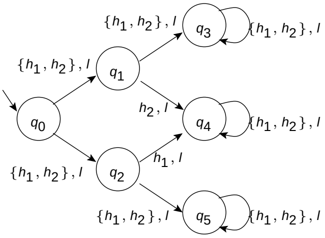


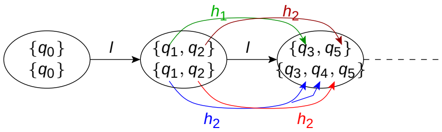




- $\lambda(q_0) = r_0, \lambda(q_1) = \lambda(q_2) = r_1, \lambda(q_3) = r_3, \lambda(q_4) = r_4, \lambda(q_5) = r_5.$
- Construct pairs of finite-state strategies.
- Check whether only pairs of sets of states having the same low-level projection are constructed:

$$\lambda(\{q_3, q_5\}) = \{r_3, r_5\} \neq \lambda(\{q_3, q_4, q_5\}) = \{r_3, r_4, r_5\}$$

# Decidability




- $\lambda(q_0) = r_0, \lambda(q_1) = \lambda(q_2) = r_1, \lambda(q_3) = r_3, \lambda(q_4) = r_4, \lambda(q_5) = r_5$.
- Construct pairs of finite-state strategies.
- Check whether only pairs of sets of states having the same low-level projection are constructed:

$$\lambda\big(\{q_3, q_5\}\big) = \{r_3, r_5\} \neq \lambda\big(\{q_3, q_4, q_5\}\big) = \{r_3, r_4, r_5\}$$

# Bisimulation (synchronous variant)

- For $s \in \mathrm{Str}_H^\infty$, the *s*-governed system $\mathcal{A}(s)$ is $\mathcal{A}(s) = \big(\mathcal{R}, Q_H, Q_L, H, L, \tilde{\delta}, q_0, \tilde{\chi}, \tilde{\lambda}\big)$ where

$$\mathcal{R} = \big\{(q,z) \mid z \in (Q_H)^*, z = z'r, r \in Q_H, \chi(q) = r\big\}$$

$$\tilde{\delta} = \big\{((q,z),h,l,(q',z\chi(r))) \mid z \in (Q^H)^*, (q,h,l,r) \in \delta, s(z) = h\big\} \cup \big\{((q_0,\epsilon),h,l,(q,\chi(q))) \mid (q_0,h,l,q) \in \delta\big\}$$

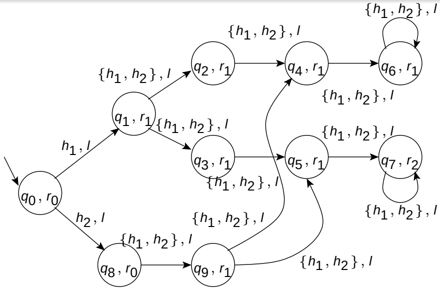
$$\tilde{\chi}((q,z)) = \chi(r) \text{ if } z = z'r \text{ for some } r \in Q_H$$

$$\tilde{\lambda}((q,z)) = \lambda(q)$$

  $\mathcal{A}(s)$ is an automaton model for the composition between a system and a high-level strategy.

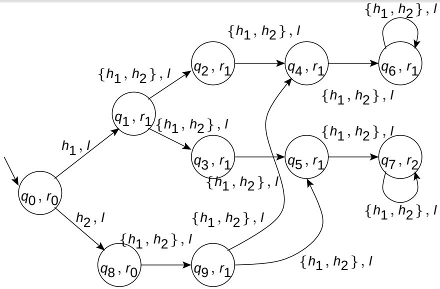
- $\mathcal{A}$ has the bisimulation-based nondeducibility on composition (**BNDC**), property if $\forall s_1, s_2 \in \mathrm{Str}_H^\infty$, $\mathcal{A}(s_1)$ and $\mathcal{A}(s_2)$ are *bisimilar*.
  - Bisimulation on the set of states of $\mathcal{A}(s_1)$ times the set of states of $\mathcal{A}(s_2)$.

# Bisimulation vs. strategies



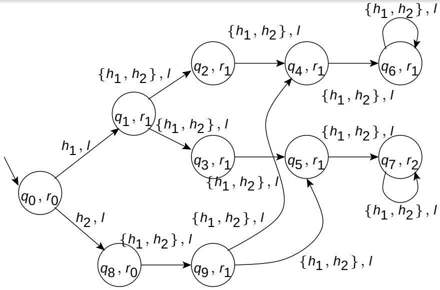

- States $(q_2, r_1)$ and $(q_9, r_1)$ cannot be bisimilar.
- Hence, for any $s_1$ with $s_1(\epsilon) = h_1$ and any $s_2$ with $s_2(\epsilon) = h_2$, $\mathcal{A}(s_1)$ is not bisimilar with $\mathcal{A}(s_2)$.
- But $\mathrm{Obs}(s)$ is the same for any strategy $s$.
- System choices should not be considered as sources of information leak!

# Bisimulation vs. strategies



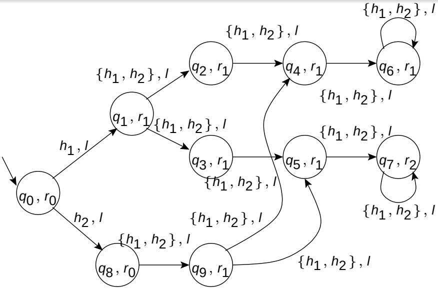

- States $(q_2, r_1)$ and $(q_9, r_1)$ cannot be bisimilar.
- Hence, for any $s_1$ with $s_1(\epsilon) = h_1$ and any $s_2$ with $s_2(\epsilon) = h_2$, $\mathcal{A}(s_1)$ is not bisimilar with $\mathcal{A}(s_2)$.
- But Obs$(s)$ is the same for any strategy $s$.
- System choices should not be considered as sources of information leak!

# Bisimulation vs. strategies




- States $(q_2, r_1)$ and $(q_9, r_1)$ cannot be bisimilar.
- Hence, for any $s_1$ with $s_1(\epsilon) = h_1$ and any $s_2$ with $s_2(\epsilon) = h_2$, $\mathcal{A}(s_1)$ is not bisimilar with $\mathcal{A}(s_2)$.
- But Obs$(s)$ is the same for any strategy $s$.
- System choices should not be considered as sources of information leak!

# Bisimulation vs. strategies




- States $(q_2, r_1)$ and $(q_9, r_1)$ cannot be bisimilar.
- Hence, for any $s_1$ with $s_1(\epsilon) = h_1$ and any $s_2$ with $s_2(\epsilon) = h_2$, $\mathcal{A}(s_1)$ is not bisimilar with $\mathcal{A}(s_2)$.
- But Obs$(s)$ is the same for any strategy $s$.
- System choices should not be considered as sources of information leak!

# A synchronous variant of Generalized Noninterference

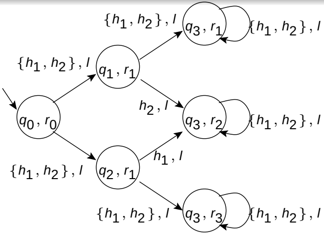
- A system is $H$-input total if

$$\forall q \in Q, \forall h \in H\ \exists l \in L \text{such that } \delta(q, h, l) \neq \emptyset$$

- $\mathcal{A}$ satisfies Synchronous Generalized Noninterference (**SGNI**) if it is $H$-input total and for any two runs $\rho, \rho'$, we may "recombine" the low-level events in $\rho$ and the high-level events in $\rho'$ to obtain a new run of $\mathcal{A}$.
  - Formally, $\mathcal{A}$ has to satisfy the following property:

    *For any two runs $\rho, \rho'$ with $\rho = (q_{i-1} \xrightarrow{h_i, l_i} q_i)_{1 \leq i \leq n}$, there exists a run $\rho'' = (r_{i-1} \xrightarrow{h_i, l_i'} r_i)$ with $\rho''\big|_L = \rho'\big|_L$.*
  - Note that the sequences of $H$-inputs in $\rho$ and $\rho''$ are the same.

# SGNI and admissible covert channel capacity

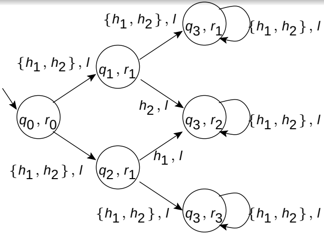



- System $\mathcal{A}_{sgni}$ satisfies SGNI...
- ... but does not have zero admissible covert channel capacity:

$$\begin{array}{llll} s_1(\epsilon) = h_1 & s_1(q_1) = h_1 & s_1(q_2) = h_1 & s_1(z) = \text{ arbitrary, otherwise} \\ s_2(\epsilon) = h_1 & s_2(q_1) = h_1 & s_2(q_2) = h_2 & s_2(z) = \text{ arbitrary, otherwise} \end{array}$$

- $\mathrm{Obs}(s_1) \neq \mathrm{Obs}(s_2)$, since $r_0 \xrightarrow{l} r_1 \xrightarrow{l} r_2 \in \mathrm{Obs}(s_2) \setminus \mathrm{Obs}(s_1)$.
- Note that $\mathrm{Obs}(s_1) \subsetneq \mathrm{Obs}(s_2)$!

# SGNI and admissible covert channel capacity



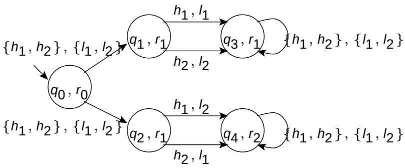

- System $\mathcal{A}_{sgni}$ satisfies SGNI...
- ... but does not have zero admissible covert channel capacity:

$$\begin{array}{llll} s_1(\epsilon) = h_1 & s_1(q_1) = h_1 & s_1(q_2) = h_1 & s_1(z) = \text{arbitrary, otherwise} \\ s_2(\epsilon) = h_1 & s_2(q_1) = h_1 & s_2(q_2) = h_2 & s_2(z) = \text{arbitrary, otherwise} \end{array}$$

- $\mathrm{Obs}(s_1) \neq \mathrm{Obs}(s_2)$, since $r_0 \xrightarrow{l} r_1 \xrightarrow{l} r_2 \in \mathrm{Obs}(s_2) \setminus \mathrm{Obs}(s_1)$.
- Note that $\mathrm{Obs}(s_1) \subsetneq \mathrm{Obs}(s_2)$!

# SGNI and covert channel capacity

- ZCCC does not imply SGNI either:




- Any strategy is compatible with any run...
- ... but if we put

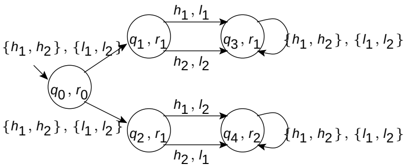
$$\rho = (q_0, r_0) \xrightarrow{h_1, l_1} (q_1, r_1) \xrightarrow{h_1, l_1} (q_3, r_1)$$

$$\rho' = (q_0, r_0) \xrightarrow{h_1, l_1} (q_2, r_1) \xrightarrow{h_2, l_1} (q_4, r_2)$$

then for no $\rho''$ which has the sequence of inputs $h_1, h_1$ (like $\rho$ has!) do we have $\rho''\big|_L = \rho'\big|_L$.

# SGNI and covert channel capacity

- ZCCC does not imply SGNI either:




- Any strategy is compatible with any run...
- ... but if we put

$$\rho = (q_0, r_0) \xrightarrow{h_1, l_1} (q_1, r_1) \xrightarrow{h_1, l_1} (q_3, r_1)$$
$$\rho' = (q_0, r_0) \xrightarrow{h_1, l_1} (q_2, r_1) \xrightarrow{h_2, l_1} (q_4, r_2)$$

then for no $\rho''$ which has the sequence of inputs $h_1, h_1$ (like $\rho$ has!) do we have $\rho''\big|_L = \rho'\big|_L$.

# Probabilistic systems as Markov decision processes

- Markov Decision Process with state space $Q$.
- For each $h \in H, l \in L$, $\delta_{h,l} : Q \times Q \to [0,1]$ is a probability measure,

$$\sum_{r \in Q} \delta_{h,l}(q,r) = 1$$

- Given $\sigma \in \mathrm{Str}_H^\infty$, $\tau \in \mathrm{Str}_L^\infty$, we have a probability space $\mathcal{P}(Q,\sigma,\tau) = (\mathrm{Runs}^{<\infty}, Pr_{\sigma,\tau})$

$$Pr_{\sigma,\tau}(\epsilon) = 1$$

$$Pr_{\sigma,\tau}(\rho \xrightarrow{h,l} q') = Pr_{\sigma,\tau}(\rho) \cdot \delta_{h,l}(q,q')$$

where $q$ is the final state in $\rho$.

# (Admissible) probabilistic covert channel capacity

- Have to consider runs that give the same low-level observation.

$$Pr_{\sigma_1,\tau}(\rho\big|_L) = \sum_{\rho'\big|_L = \rho\big|_L} Pr_{\sigma,\tau}(\rho')$$

- Idea: no information flow if

$$\forall \tau \in \mathrm{Str}_L^\infty, \forall \sigma_1, \sigma_2 \in \mathrm{Str}_H^\infty, \forall \rho \in \mathrm{Runs}^{<\infty}, Pr_{\sigma_1,\tau}(\rho\big|_L) = Pr_{\sigma_2,\tau}(\rho\big|_L)$$

- Zero probabilistic covert channel capacity: for each $\tau$, there exists only one probability distribution $Pr_{\cdot,\tau}$ on $\mathrm{Runs}^{<\infty}\big|_L$.
- Admissible ZPCCC : consider only the probability distribution on admissible runs.
- Conjecture: It is decidable whether a system has no probabilistic information flow.

# Conclusions

- A game-based model of information flow.
    - Synchronous model – time is a shared resource.
- Some differences with trace-based models and with bisimulation-based models.
- Decidability (for any type of high-level “Trojan Horse”).
- Elements of a logical framework for defining information flow.
- Elements of a probabilistic extension.

To dos:

- A logical form of the zero (admissible) covert channel capacity.
- In case of nonzero (admissible) PCCC, find the best strategy for Larry – the one that maximizes his “information” about Harry’s strategy.
- “Controller synthesis” (possibilistic case) : solve system nondeterminism in order to avoid information leak (if possible).