Correctness of Broadcast via Multicast: Graphically and Formally

Wolfgang Jeltsch Javier Díaz

Working Formal Methods Symposium 2022

Iași, Romania
19–20 September 2022

Introduction

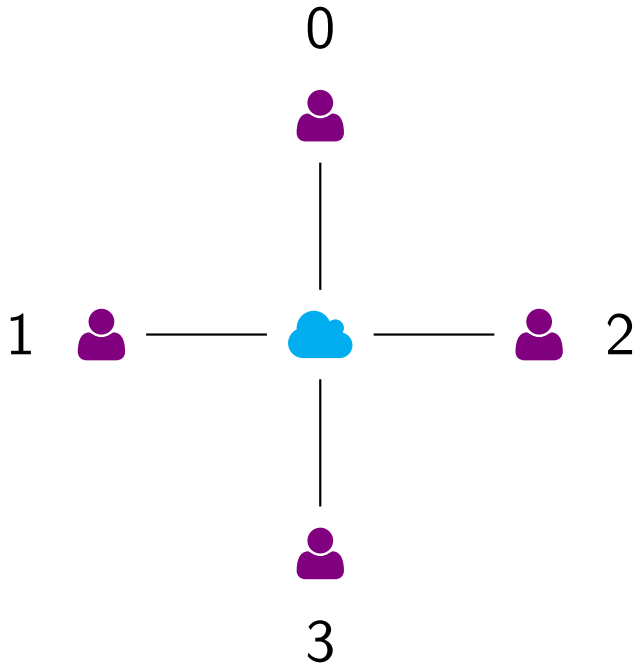
- Maintaining data consistency in distributed systems using broadcast
  - Distribution of blocks in the Cardano blockchain system
- Mismatch between theory and practice:
  - Proofs of correctness and security assume direct broadcast
  - Implementations perform broadcast via repeated multicast
- Bridge the gap with a formal proof
  - Show equivalence of both broadcast flavors using Isabelle/HOL
- Features:
  - Intelligible proof code through equivalence reasoning with processes
  - Vivid presentation through a graphical notation for processes

Introduction

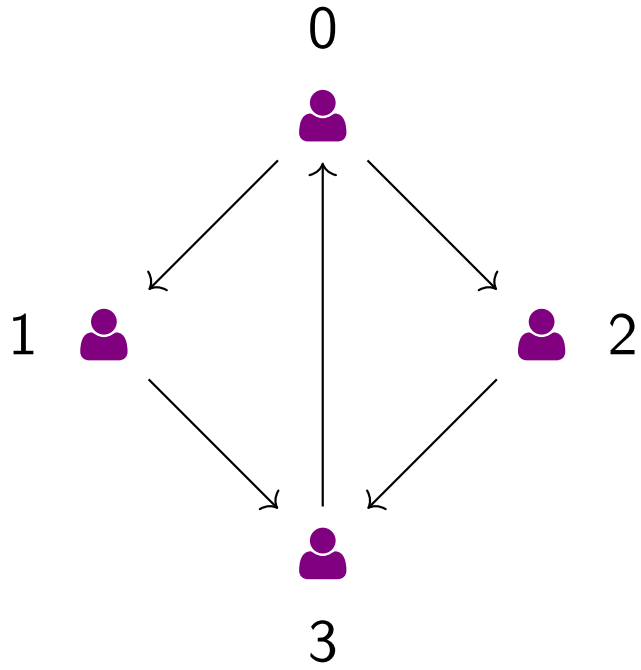
- Maintaining data consistency in distributed systems using broadcast
  - Distribution of blocks in the Cardano blockchain system
- Mismatch between theory and practice:
  - Proofs of correctness and security assume direct broadcast
  - Implementations perform broadcast via repeated multicast
- Bridge the gap with a formal proof
  - Show equivalence of both broadcast flavors using Isabelle/HOL
- Features:
  - Intelligible proof code through equivalence reasoning with processes
  - Vivid presentation through a graphical notation for processes

formal, yet intuitive

Our example

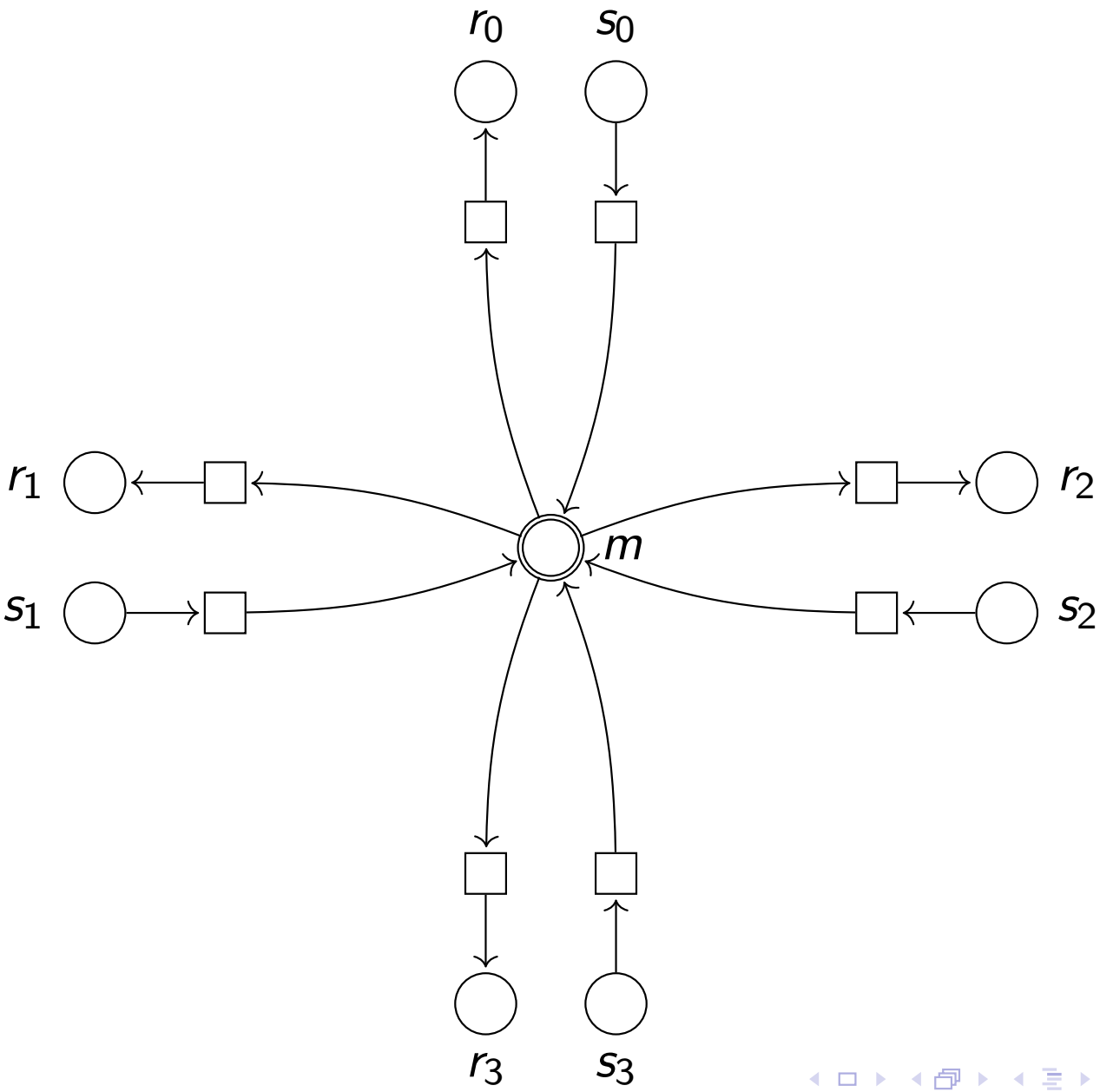


Broadcast network

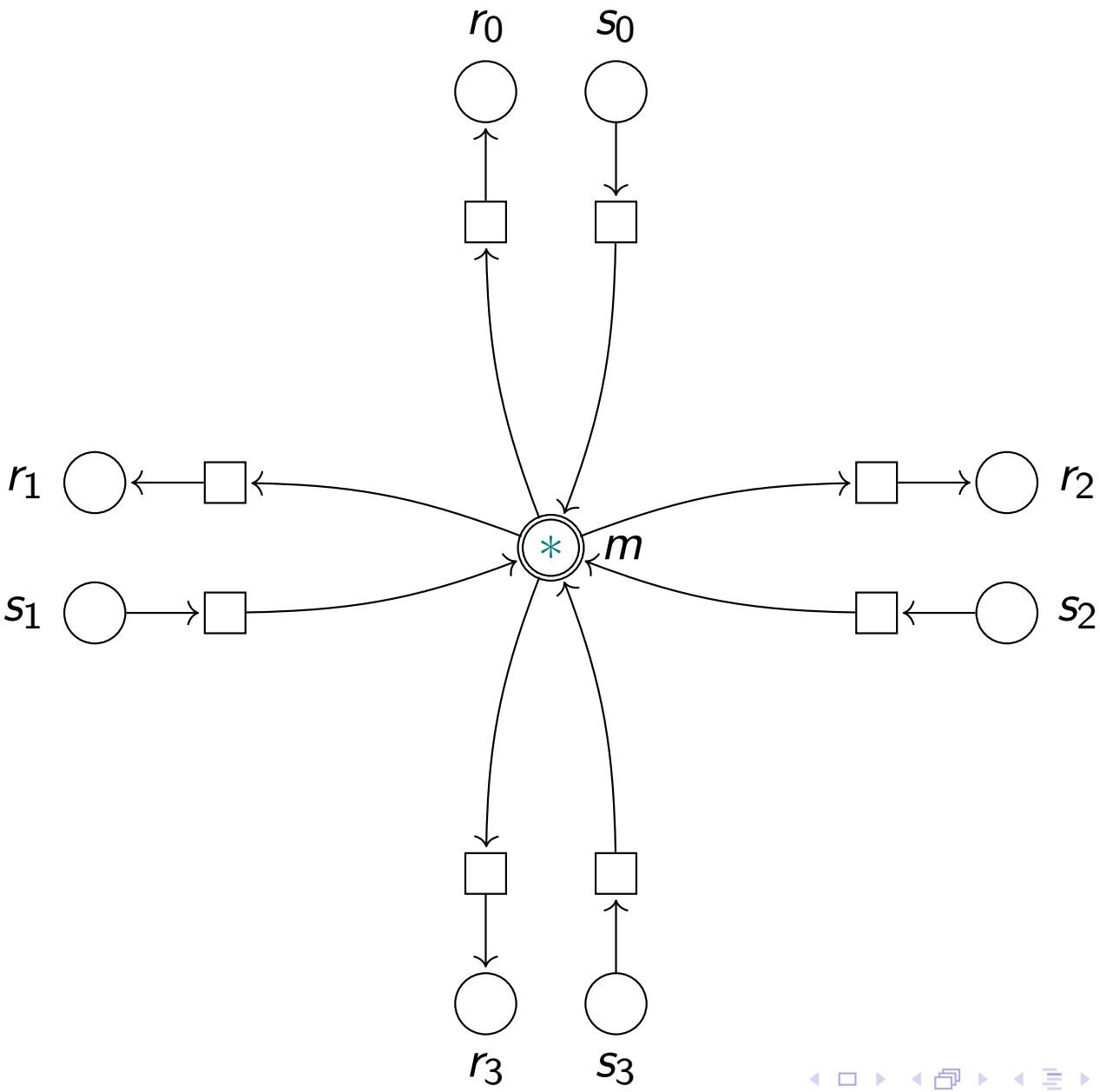


Multicast network

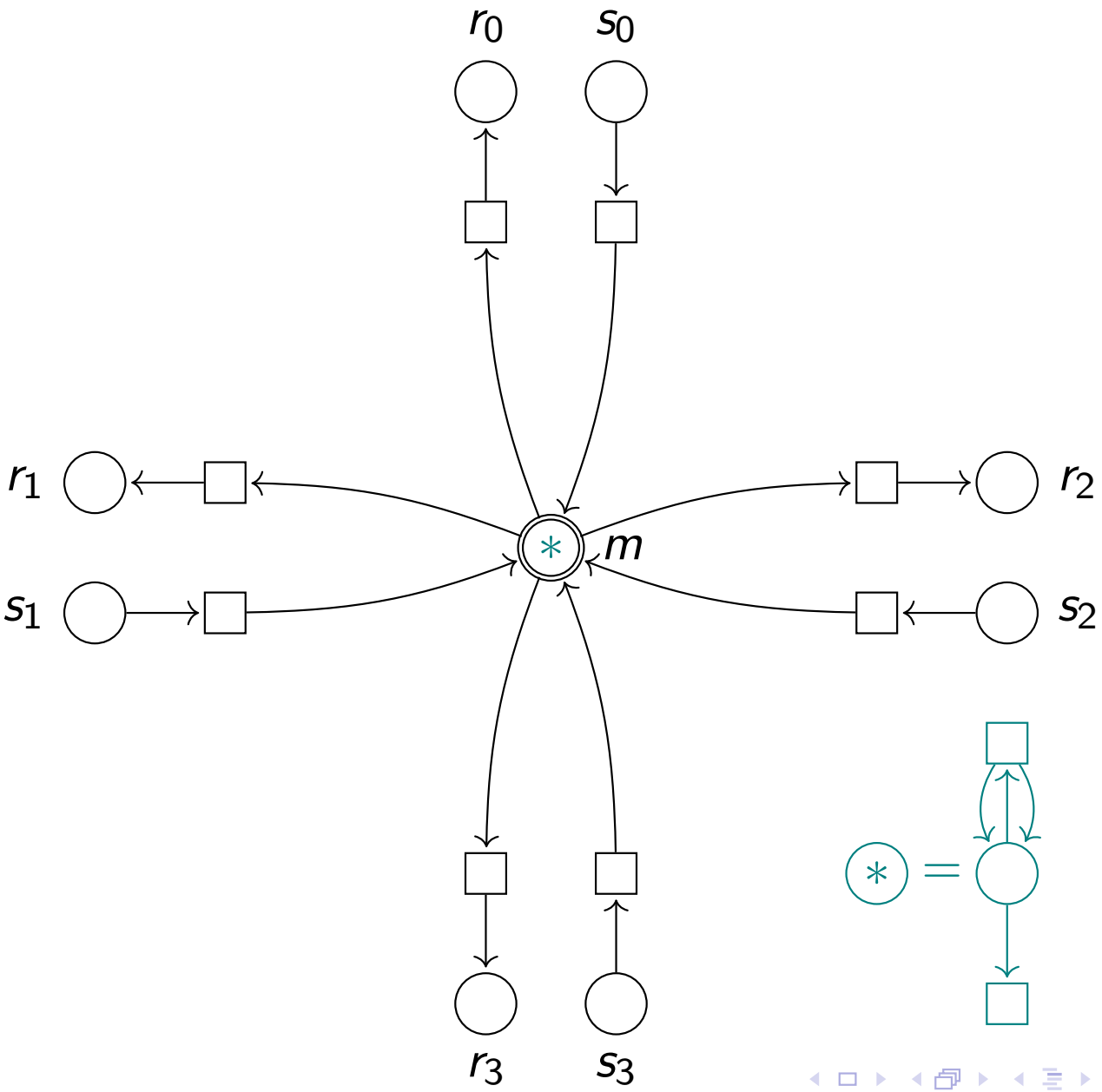
A communication net for direct broadcast



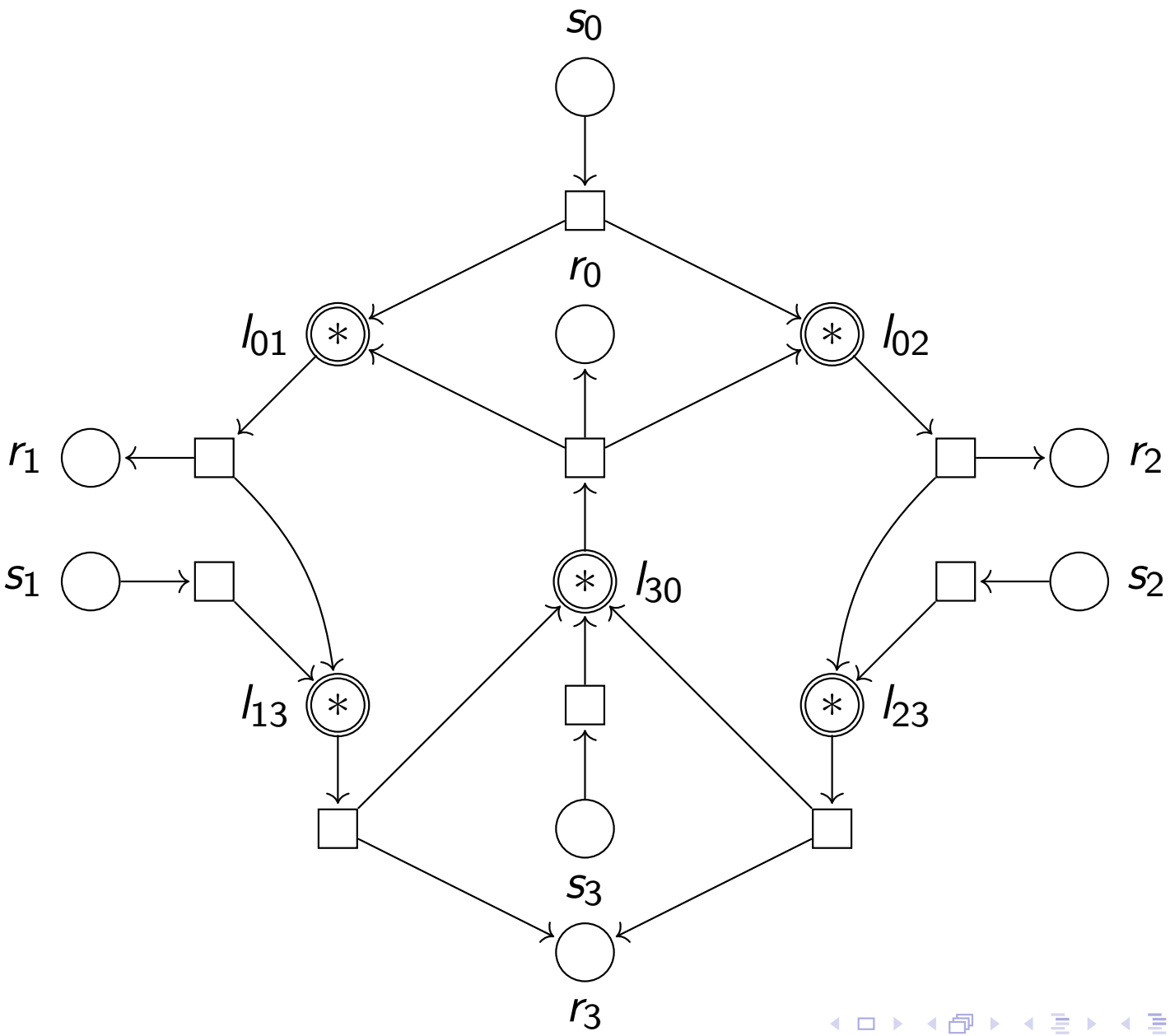
A communication net for direct broadcast



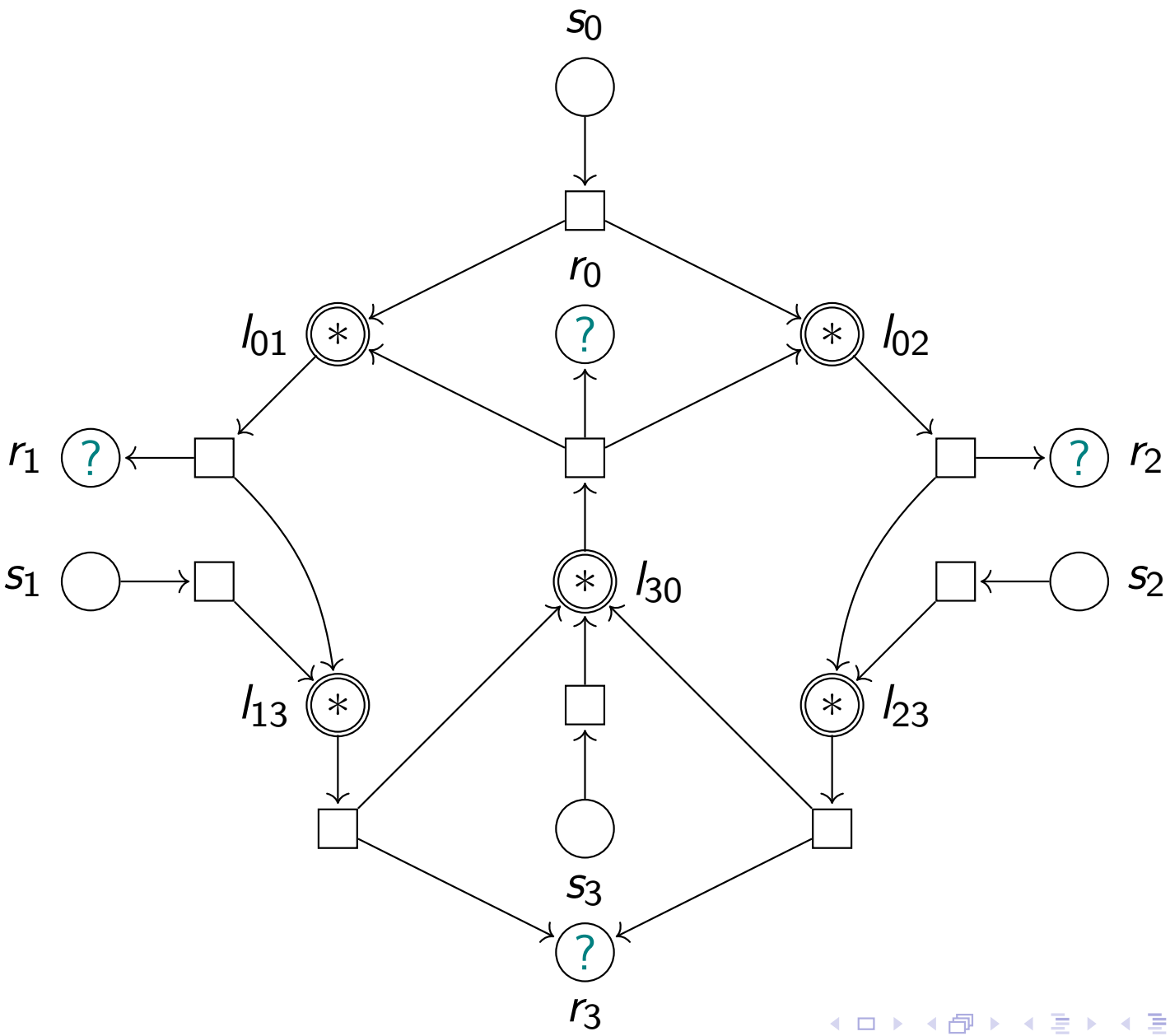
A communication net for direct broadcast



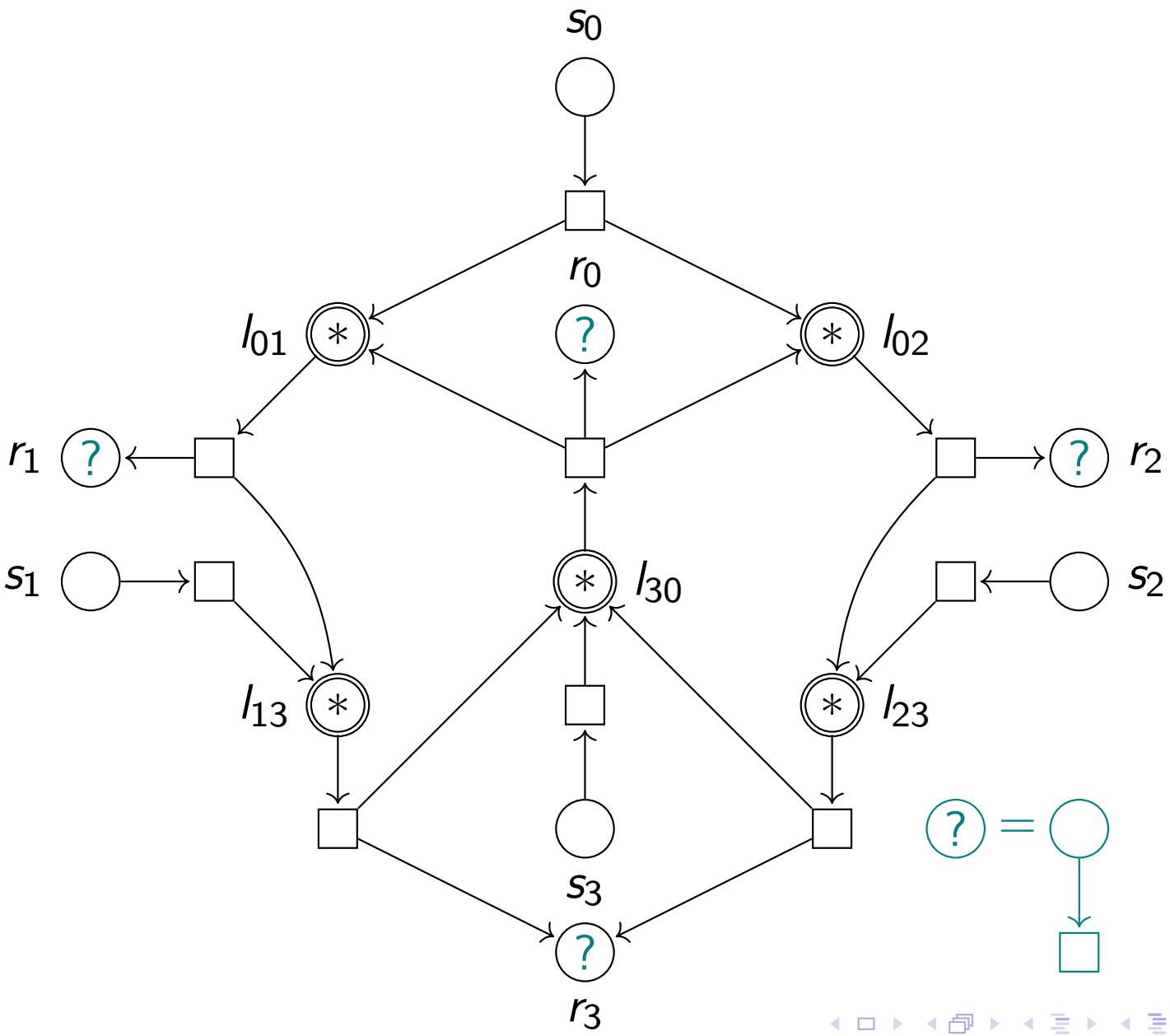
A communication net for broadcast via multicast



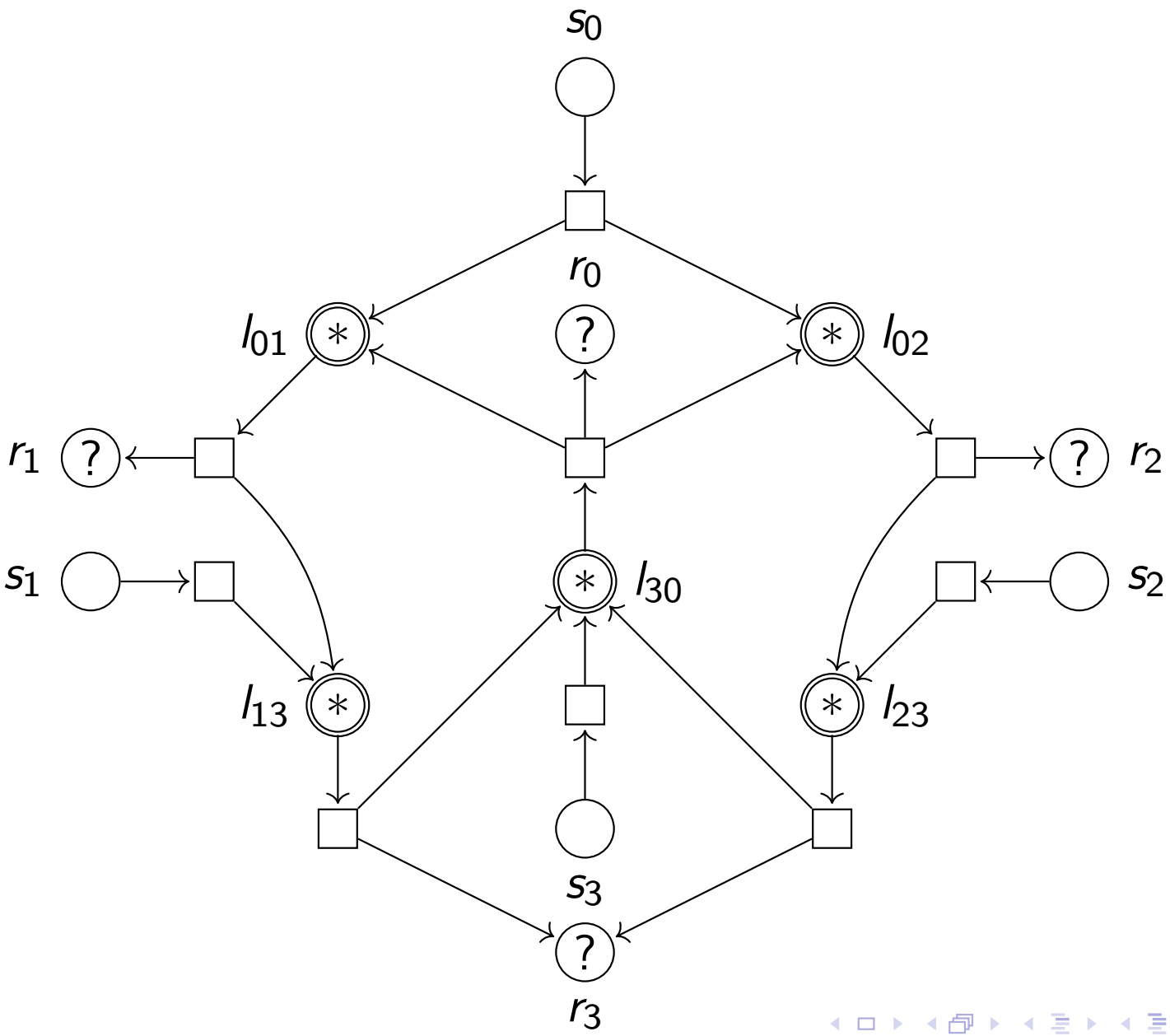
Permitting arbitrary arrival patterns



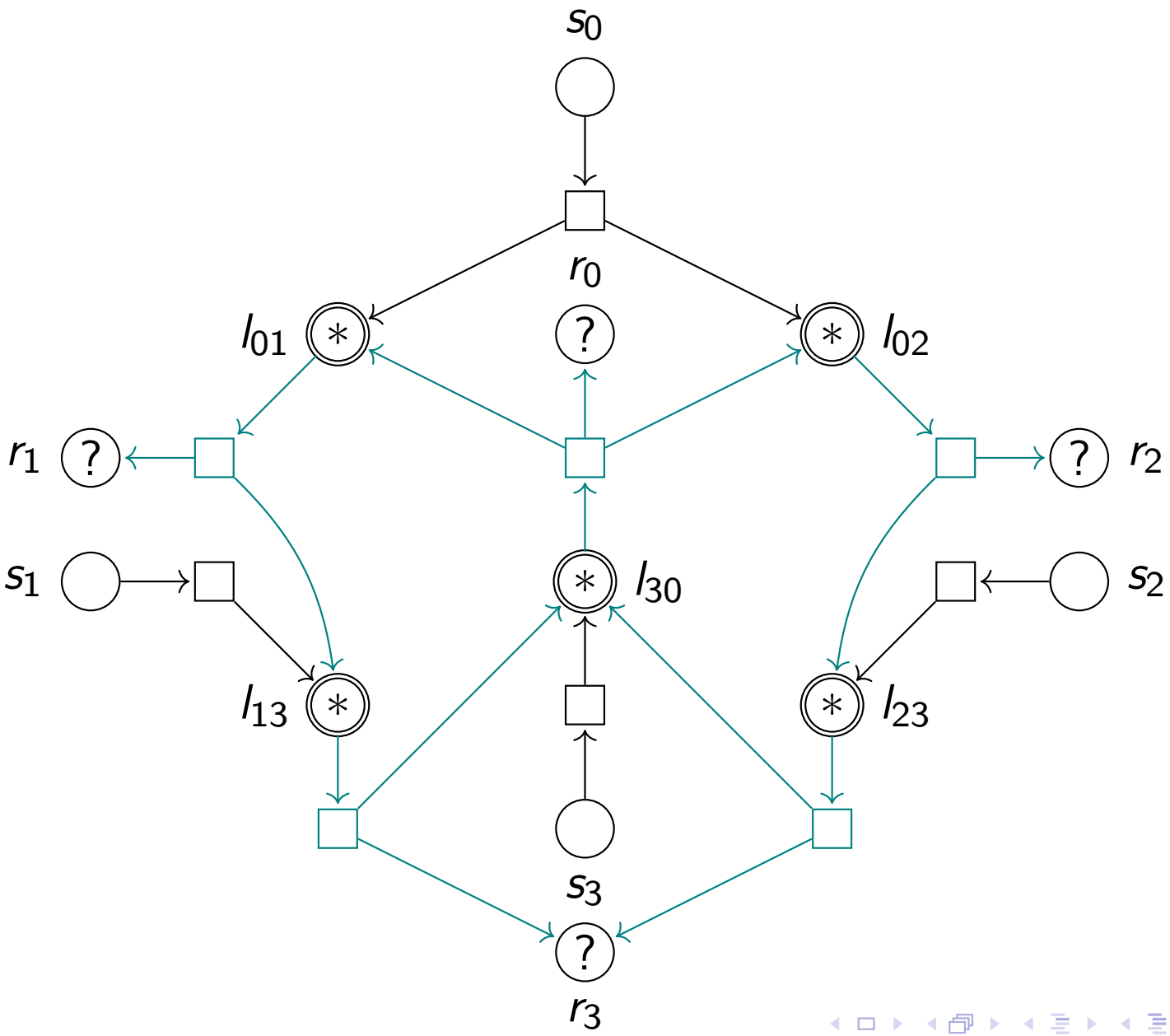
Permitting arbitrary arrival patterns



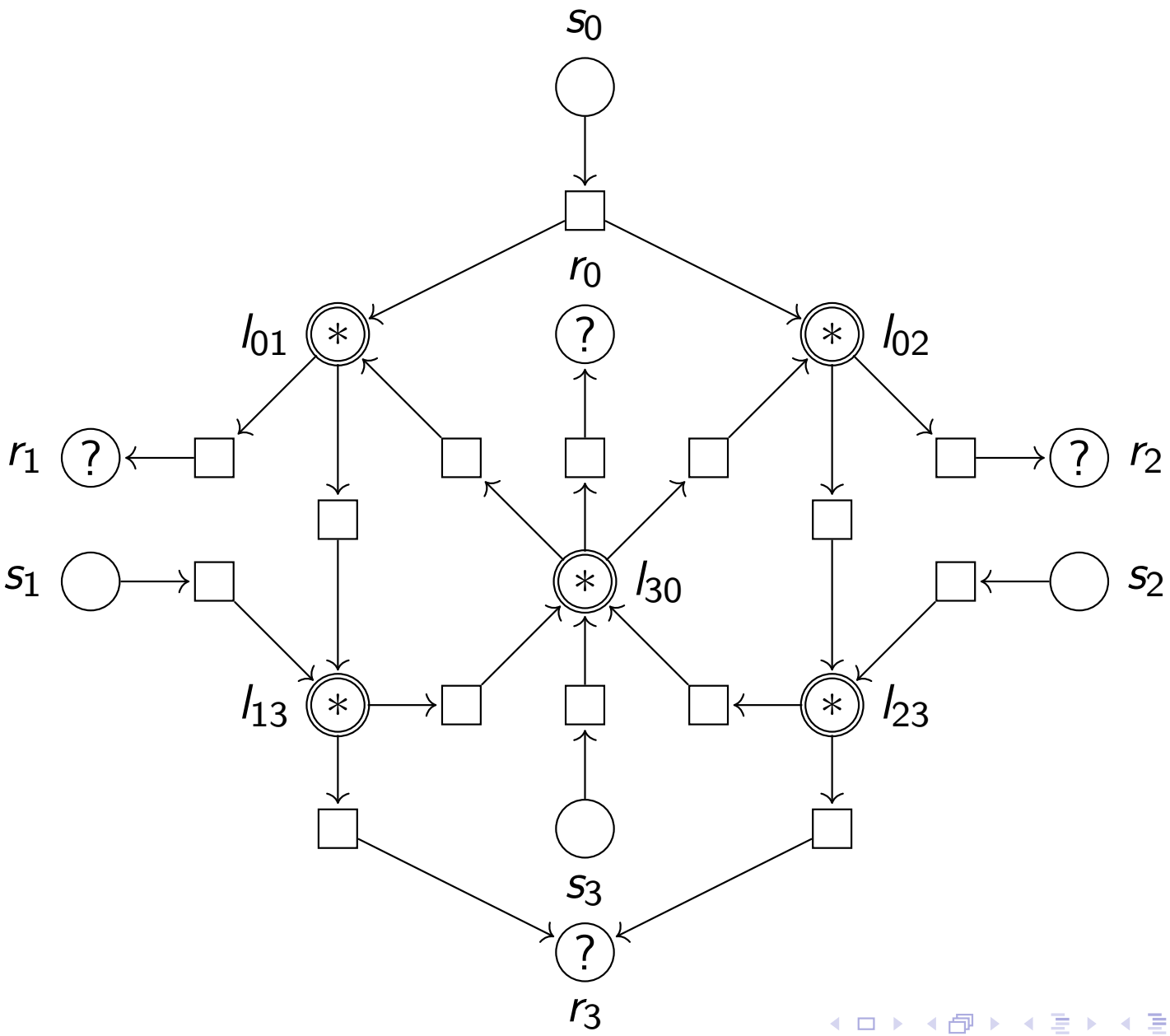
The first transformation step: graphically



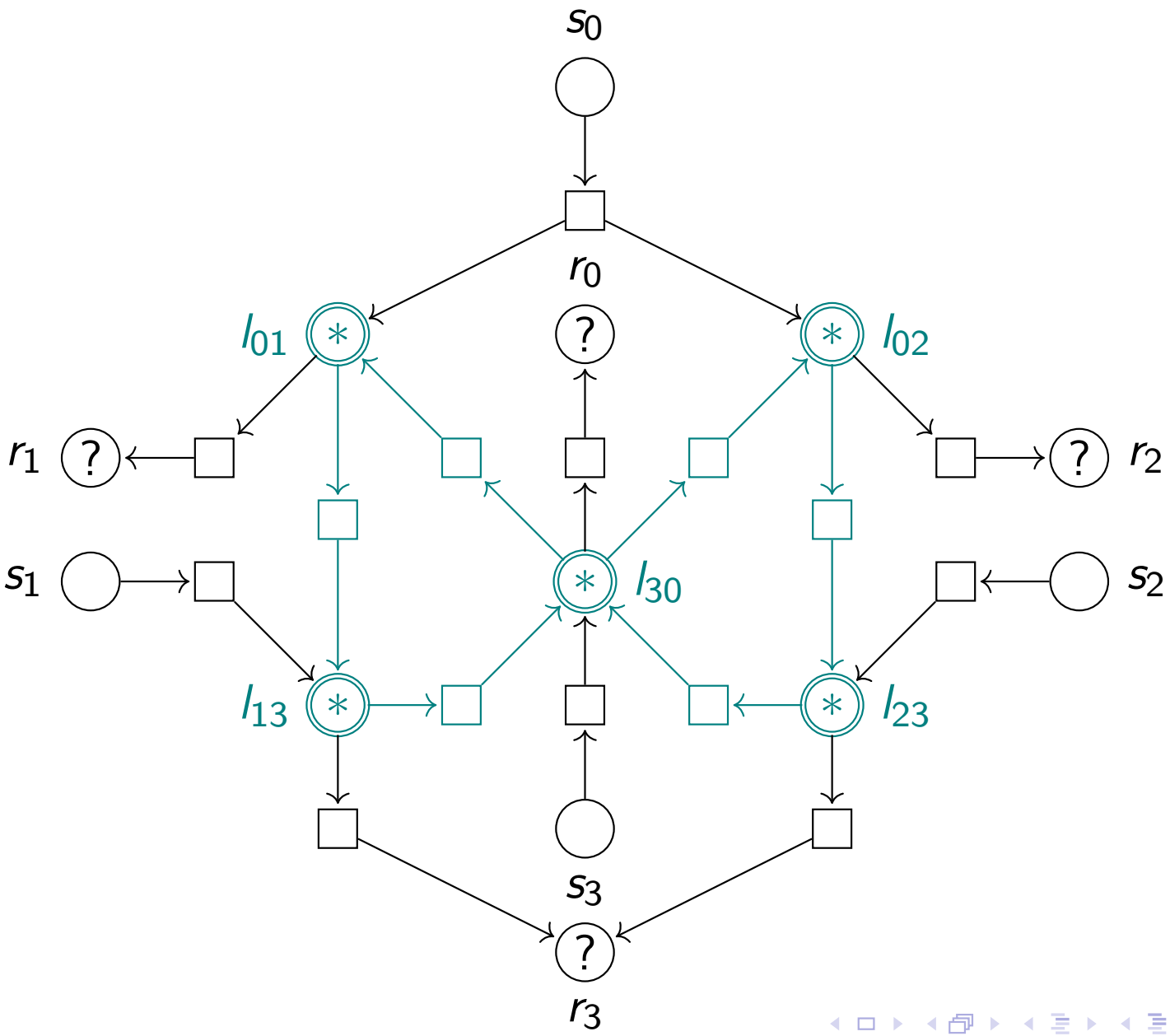
The first transformation step: graphically



The first transformation step: graphically



The first transformation step: graphically



The first transformation step: formally

$$
\begin{aligned}
&\text{¤}^{?} r_0 \parallel \text{¤}^{?} r_1 \parallel \text{¤}^{?} r_2 \parallel \text{¤}^{?} r_3 \parallel \\
&\text{¤}^{*} l_{01} \parallel \text{¤}^{*} l_{02} \parallel \text{¤}^{*} l_{13} \parallel \text{¤}^{*} l_{23} \parallel \text{¤}^{*} l_{30} \parallel \\
&l_{01} \Rightarrow [r_1, l_{13}] \parallel \\
&l_{02} \Rightarrow [r_2, l_{23}] \parallel \\
&l_{13} \Rightarrow [r_3, l_{30}] \parallel \\
&l_{23} \Rightarrow [r_3, l_{30}] \parallel \\
&l_{30} \Rightarrow [r_0, l_{01}, l_{02}]
\end{aligned}
$$

The first transformation step: formally

$$
\begin{aligned}
&\text{¤}^{?} r_0 \parallel \text{¤}^{?} r_1 \parallel \text{¤}^{?} r_2 \parallel \text{¤}^{?} r_3 \parallel \\
&\text{¤}^{*} l_{01} \parallel \text{¤}^{*} l_{02} \parallel \text{¤}^{*} l_{13} \parallel \text{¤}^{*} l_{23} \parallel \text{¤}^{*} l_{30} \parallel \\
&l_{01} \Rightarrow [r_1, l_{13}] \parallel \\
&l_{02} \Rightarrow [r_2, l_{23}] \parallel \\
&l_{13} \Rightarrow [r_3, l_{30}] \parallel \\
&l_{23} \Rightarrow [r_3, l_{30}] \parallel \\
&l_{30} \Rightarrow [r_0, l_{01}, l_{02}] \\
&\approx \\
&(\text{¤}^{+} l_{01} \parallel \prod a \leftarrow [r_1, l_{13}].\ \text{¤}^{?} a \parallel l_{01} \Rightarrow [r_1, l_{13}]) \parallel \\
&(\text{¤}^{+} l_{02} \parallel \prod a \leftarrow [r_2, l_{23}].\ \text{¤}^{?} a \parallel l_{02} \Rightarrow [r_2, l_{23}]) \parallel \\
&(\text{¤}^{+} l_{13} \parallel \prod a \leftarrow [r_3, l_{30}].\ \text{¤}^{?} a \parallel l_{13} \Rightarrow [r_3, l_{30}]) \parallel \\
&(\text{¤}^{+} l_{23} \parallel \prod a \leftarrow [r_3, l_{30}].\ \text{¤}^{?} a \parallel l_{23} \Rightarrow [r_3, l_{30}]) \parallel \\
&(\text{¤}^{+} l_{30} \parallel \prod a \leftarrow [r_0, l_{01}, l_{02}].\ \text{¤}^{?} a \parallel l_{30} \Rightarrow [r_0, l_{01}, l_{02}])
\end{aligned}
$$

The first transformation step: formally

$$
\begin{aligned}
&(\,¤^{+} l_{01} \parallel \prod a \leftarrow [r_1, l_{13}].\ ¤^{?} a \parallel l_{01} \Rightarrow [r_1, l_{13}]) \parallel \\
&(\,¤^{+} l_{02} \parallel \prod a \leftarrow [r_2, l_{23}].\ ¤^{?} a \parallel l_{02} \Rightarrow [r_2, l_{23}]) \parallel \\
&(\,¤^{+} l_{13} \parallel \prod a \leftarrow [r_3, l_{30}].\ ¤^{?} a \parallel l_{13} \Rightarrow [r_3, l_{30}]) \parallel \\
&(\,¤^{+} l_{23} \parallel \prod a \leftarrow [r_3, l_{30}].\ ¤^{?} a \parallel l_{23} \Rightarrow [r_3, l_{30}]) \parallel \\
&(\,¤^{+} l_{30} \parallel \prod a \leftarrow [r_0, l_{01}, l_{02}].\ ¤^{?} a \parallel l_{30} \Rightarrow [r_0, l_{01}, l_{02}])
\end{aligned}
$$

The first transformation step: formally

$$
\begin{aligned}
&(\text{¤}^{+} l_{01} \parallel \prod a \leftarrow [r_1, l_{13}].\ \text{¤}^{?} a \parallel l_{01} \Rightarrow [r_1, l_{13}]) \parallel \\
&(\text{¤}^{+} l_{02} \parallel \prod a \leftarrow [r_2, l_{23}].\ \text{¤}^{?} a \parallel l_{02} \Rightarrow [r_2, l_{23}]) \parallel \\
&(\text{¤}^{+} l_{13} \parallel \prod a \leftarrow [r_3, l_{30}].\ \text{¤}^{?} a \parallel l_{13} \Rightarrow [r_3, l_{30}]) \parallel \\
&(\text{¤}^{+} l_{23} \parallel \prod a \leftarrow [r_3, l_{30}].\ \text{¤}^{?} a \parallel l_{23} \Rightarrow [r_3, l_{30}]) \parallel \\
&(\text{¤}^{+} l_{30} \parallel \prod a \leftarrow [r_0, l_{01}, l_{02}].\ \text{¤}^{?} a \parallel l_{30} \Rightarrow [r_0, l_{01}, l_{02}]) \\
\approx\ &(\text{¤}^{+} l_{01} \parallel \prod a \leftarrow [r_1, l_{13}].\ \text{¤}^{?} a \parallel \prod a \leftarrow [r_1, l_{13}].\ l_{01} \rightarrow a) \parallel \\
&(\text{¤}^{+} l_{02} \parallel \prod a \leftarrow [r_2, l_{23}].\ \text{¤}^{?} a \parallel \prod a \leftarrow [r_2, l_{23}].\ l_{02} \rightarrow a) \parallel \\
&(\text{¤}^{+} l_{13} \parallel \prod a \leftarrow [r_3, l_{30}].\ \text{¤}^{?} a \parallel \prod a \leftarrow [r_3, l_{30}].\ l_{13} \rightarrow a) \parallel \\
&(\text{¤}^{+} l_{23} \parallel \prod a \leftarrow [r_3, l_{30}].\ \text{¤}^{?} a \parallel \prod a \leftarrow [r_3, l_{30}].\ l_{23} \rightarrow a) \parallel \\
&(\text{¤}^{+} l_{30} \parallel \prod a \leftarrow [r_0, l_{01}, l_{02}].\ \text{¤}^{?} a \parallel \prod a \leftarrow [r_0, l_{01}, l_{02}].\ l_{30} \rightarrow a)
\end{aligned}
$$

The first transformation step: formally

$$
\begin{aligned}
&(\,¤^{+} l_{01} \parallel \prod a \leftarrow [r_1, l_{13}].\ ¤^{?} a \parallel \prod a \leftarrow [r_1, l_{13}].\ l_{01} \rightarrow a) \parallel \\
&(\,¤^{+} l_{02} \parallel \prod a \leftarrow [r_2, l_{23}].\ ¤^{?} a \parallel \prod a \leftarrow [r_2, l_{23}].\ l_{02} \rightarrow a) \parallel \\
&(\,¤^{+} l_{13} \parallel \prod a \leftarrow [r_3, l_{30}].\ ¤^{?} a \parallel \prod a \leftarrow [r_3, l_{30}].\ l_{13} \rightarrow a) \parallel \\
&(\,¤^{+} l_{23} \parallel \prod a \leftarrow [r_3, l_{30}].\ ¤^{?} a \parallel \prod a \leftarrow [r_3, l_{30}].\ l_{23} \rightarrow a) \parallel \\
&(\,¤^{+} l_{30} \parallel \prod a \leftarrow [r_0, l_{01}, l_{02}].\ ¤^{?} a \parallel \prod a \leftarrow [r_0, l_{01}, l_{02}].\ l_{30} \rightarrow a)
\end{aligned}
$$

The first transformation step: formally

$$
\begin{aligned}
&(\,¤^{+} l_{01} \parallel \prod a \leftarrow [r_1, l_{13}].\ ¤^{?} a \parallel \prod a \leftarrow [r_1, l_{13}].\ l_{01} \rightarrow a) \parallel \\
&(\,¤^{+} l_{02} \parallel \prod a \leftarrow [r_2, l_{23}].\ ¤^{?} a \parallel \prod a \leftarrow [r_2, l_{23}].\ l_{02} \rightarrow a) \parallel \\
&(\,¤^{+} l_{13} \parallel \prod a \leftarrow [r_3, l_{30}].\ ¤^{?} a \parallel \prod a \leftarrow [r_3, l_{30}].\ l_{13} \rightarrow a) \parallel \\
&(\,¤^{+} l_{23} \parallel \prod a \leftarrow [r_3, l_{30}].\ ¤^{?} a \parallel \prod a \leftarrow [r_3, l_{30}].\ l_{23} \rightarrow a) \parallel \\
&(\,¤^{+} l_{30} \parallel \prod a \leftarrow [r_0, l_{01}, l_{02}].\ ¤^{?} a \parallel \prod a \leftarrow [r_0, l_{01}, l_{02}].\ l_{30} \rightarrow a) \\
\approx\ & \\
& ¤^{?} r_0 \parallel ¤^{?} r_1 \parallel ¤^{?} r_2 \parallel ¤^{?} r_3 \parallel \\
& ¤^{*} l_{01} \parallel ¤^{*} l_{02} \parallel ¤^{*} l_{13} \parallel ¤^{*} l_{23} \parallel ¤^{*} l_{30} \parallel \\
& l_{01} \rightarrow r_1 \parallel l_{02} \rightarrow r_2 \parallel l_{13} \rightarrow r_3 \parallel l_{23} \rightarrow r_3 \parallel l_{30} \rightarrow r_0 \parallel \\
& l_{01} \rightarrow l_{13} \parallel l_{02} \rightarrow l_{23} \parallel l_{13} \rightarrow l_{30} \parallel l_{23} \rightarrow l_{30} \parallel l_{30} \rightarrow l_{01} \parallel l_{30} \rightarrow l_{02}
\end{aligned}
$$

Follow the development

https://github.com/input-output-hk/network-equivalences