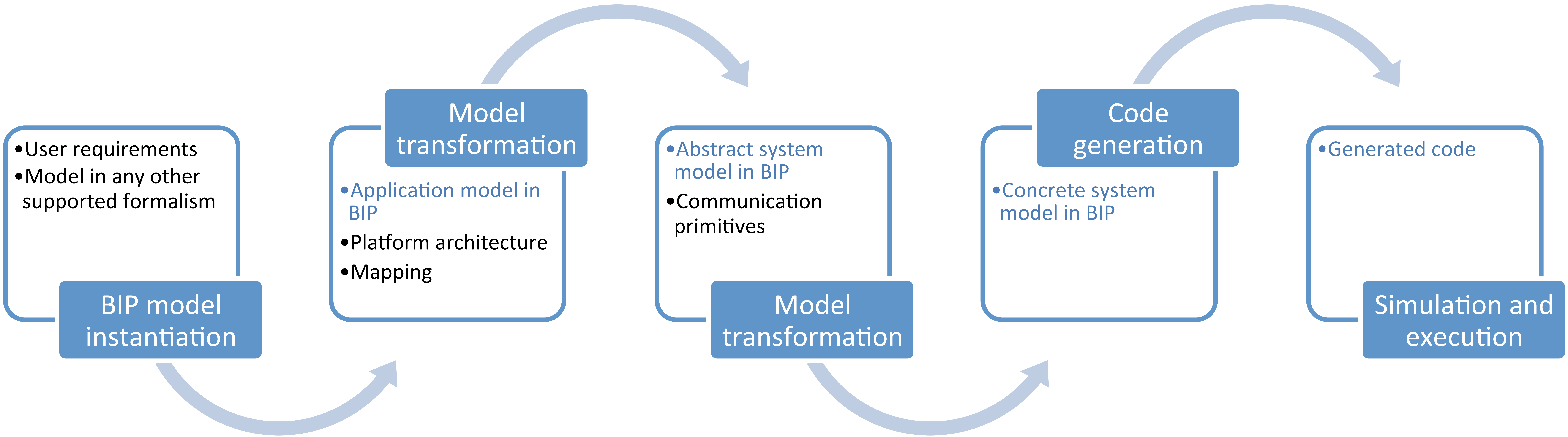
Rigorous System Design using BIP: Correctness by All Means

Part 2 – 1st of September, 2023

VTSA summer school

Simon Bliudze, Inria Lille

Quick recap — Rigorous design workflow



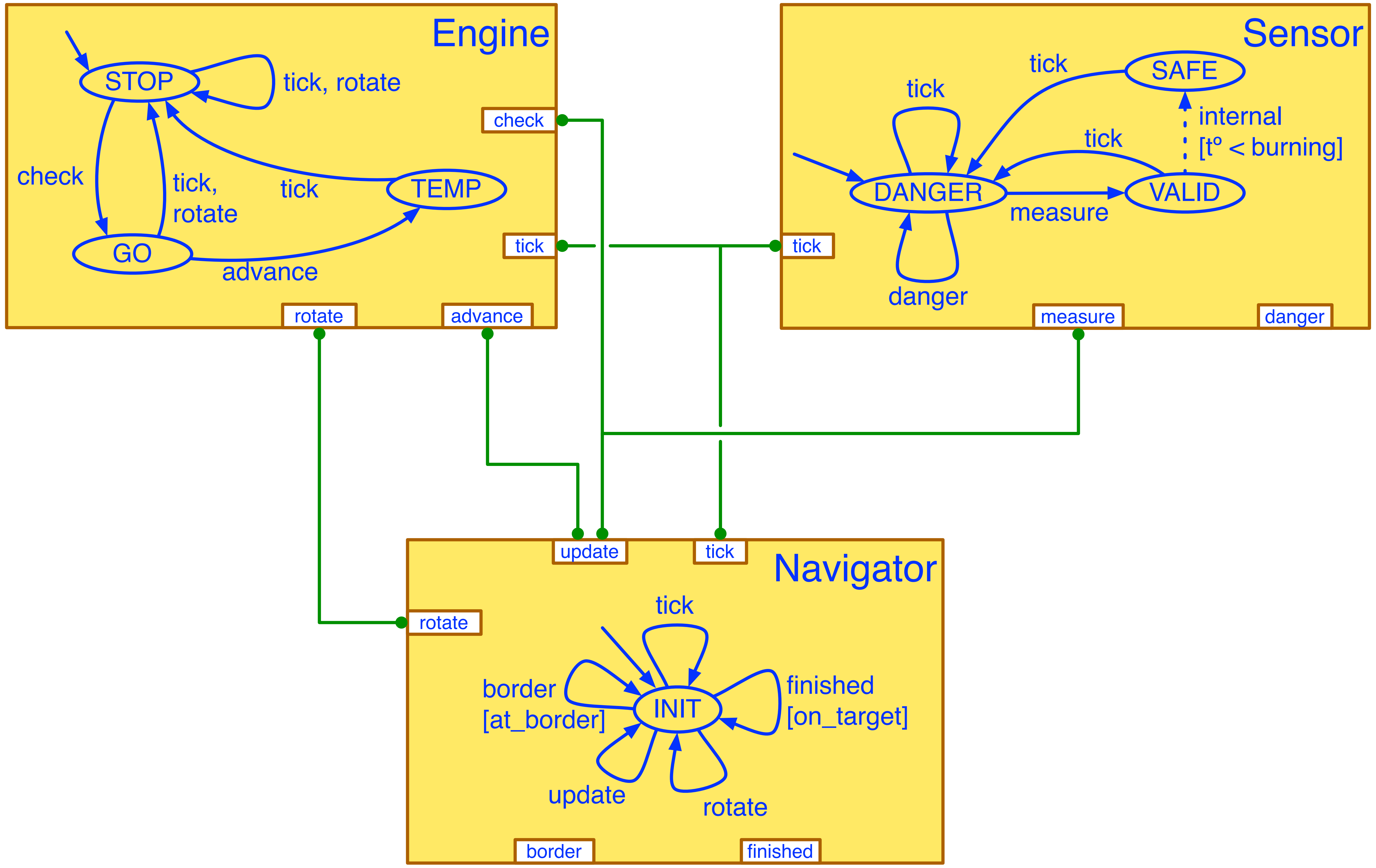
Validate first, then generate the code

A sequence of semantics-preserving transformations

Quick recap — The BIP language

Provide a higher-level abstraction for coordination of concurrent components

- Behaviour = Components
  - Finite State Machines with variables
- Interaction = Connectors
  - Define allowed synchronisations
- Priorities
  - Strict partial order on interactions



Outline

Practical aspects

Overview of the RSD approach

CubETH case study

Operational semantics

BIP language introduction

Theoretical aspects

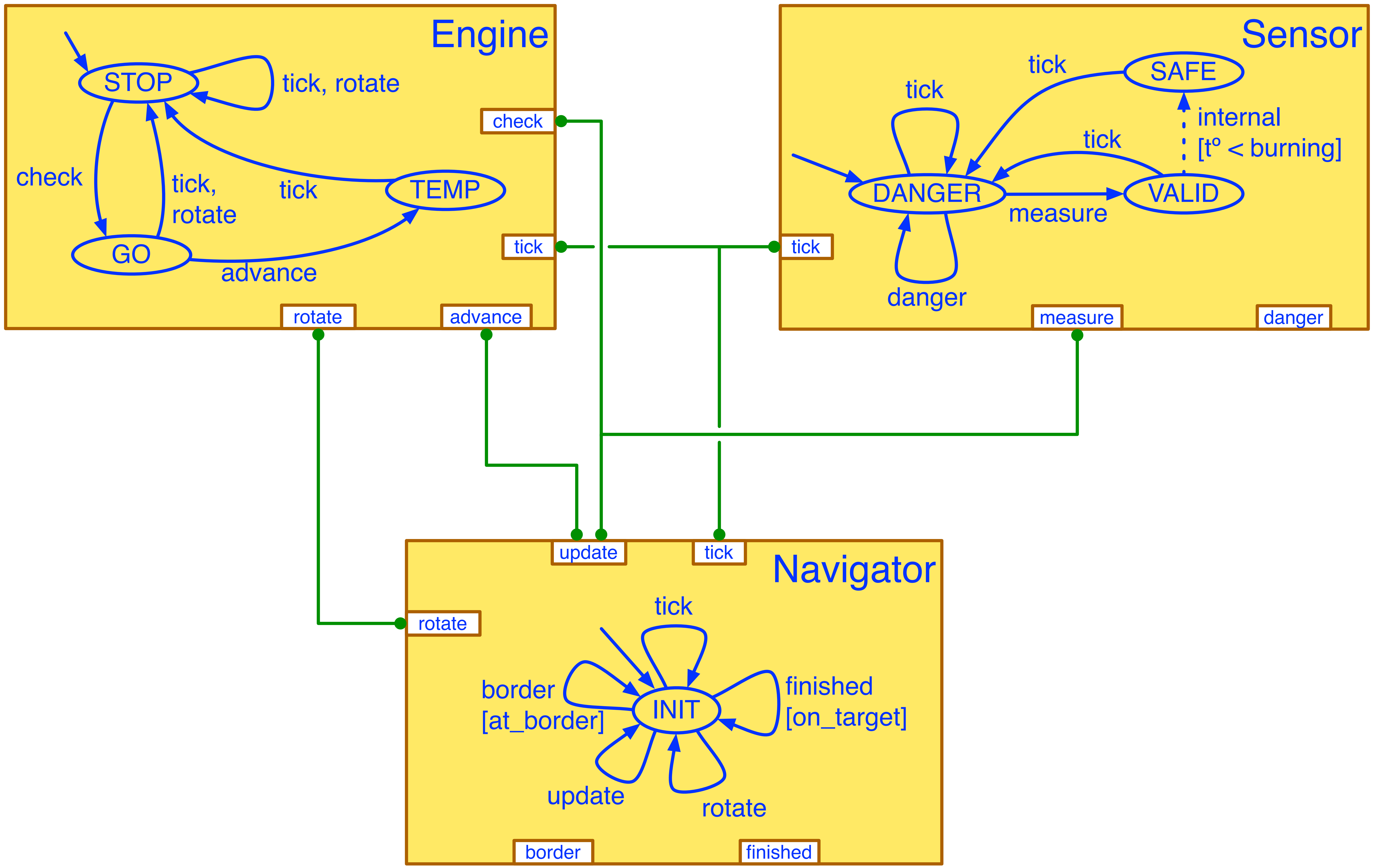
Connector modelling

Architectures: design patterns for BIP

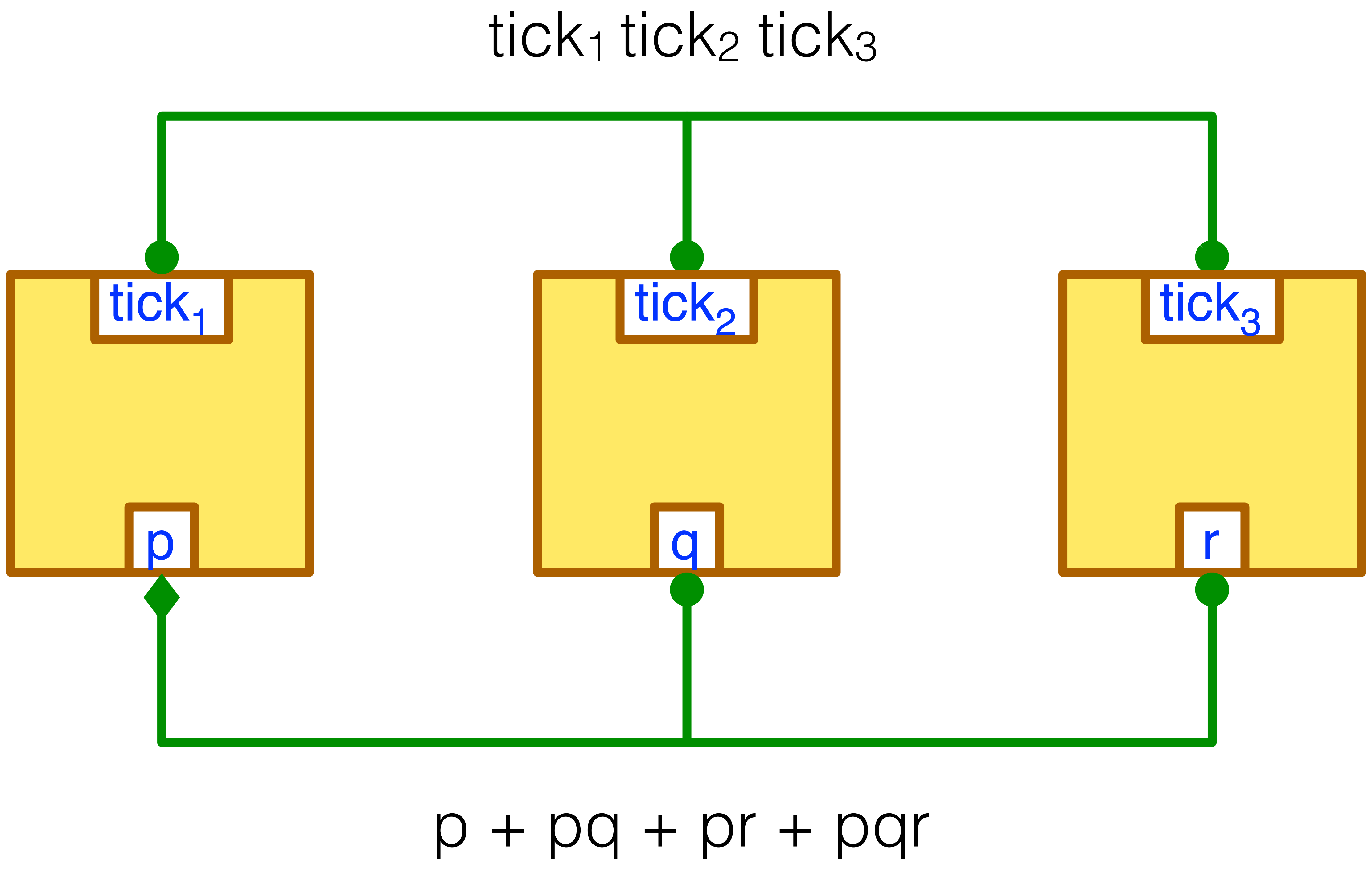
Connector synthesis

Expressiveness study

Interaction modelling



Connectors



Connectors are tree-like structures

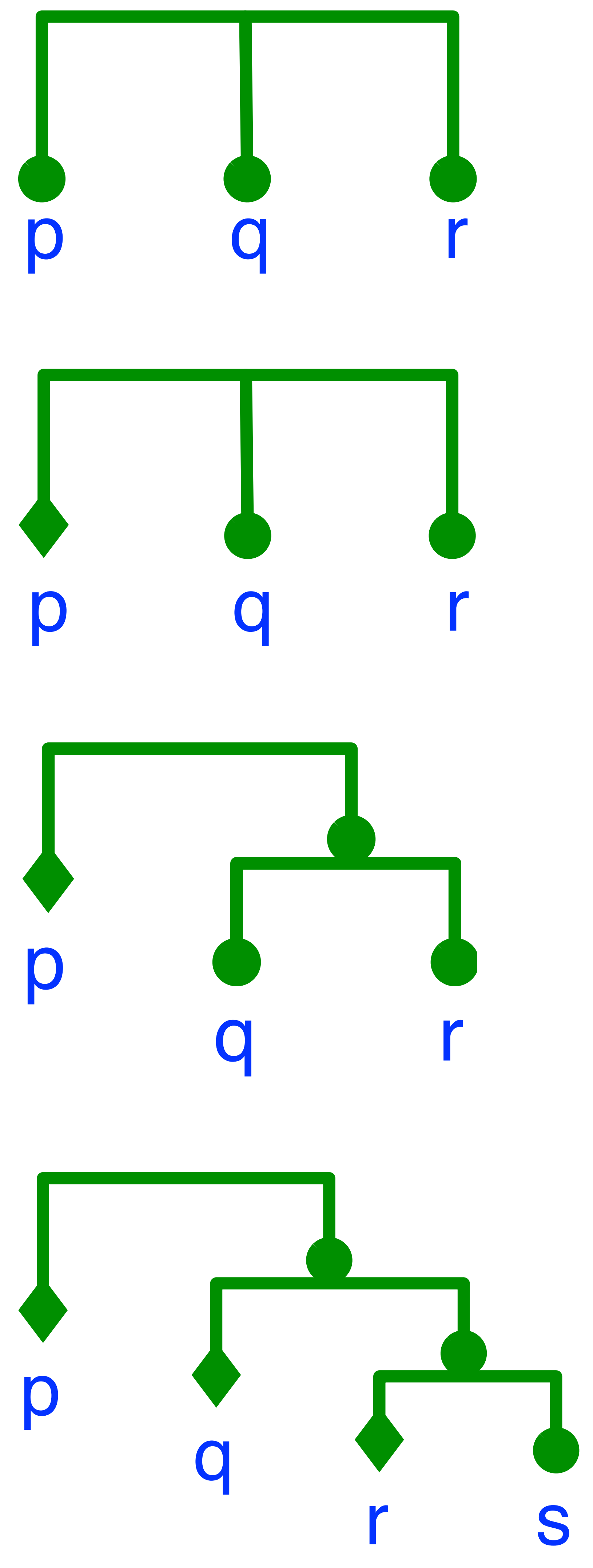
ports as leaves and nodes of two types

Triggers (triangles or diamonds) — nodes that can "initiate" an interaction

Synchrons (bullets) — nodes that can only "join" an interaction initiated by others

In practice, *maximal progress* is implicitly assumed

Connector examples



The Algebra of Connectors

Strong synchronisation:	pqr	pqr
Broadcast:	p + pq + pr + pqr	p’qr
Atomic broadcast:	p + pqr	p’[qr]
Causal chain:	p + pq + pqr + pqrs	p’[q’[r’s]]

The Algebra of Connectors

$$
\begin{aligned}
s &::= [0] \mid [1] \mid [p] \mid [x] && (synchrons)\\
t &::= [0]' \mid [1]' \mid [p]' \mid [x]' && (triggers)\\
x &::= s \mid t \mid x \cdot x \mid x + x \mid (x)
\end{aligned}
$$

Operators

Union (+) – idempotent, associative, commutative, identity [0]

Fusion ($\cdot$) – idempotent, associative, commutative, identity [1]
distributes over union ([0] is **not** absorbing)

Typing ([$\cdot$], [$\cdot$]')

Semantics: $|p'qr| \stackrel{def}{=} p(1+q)(1+r) = p + pq + pr + pqr$

Equivalence of connectors

$$x \simeq y \overset{def}{\Longleftrightarrow} |x| = |y|$$

Semantic equivalence is not a congruence

$p + pq \simeq p'q,$ but $pr + pqr \not\simeq p'qr \simeq p + pq + pr + pqr$

$p[qr] \simeq [pq]r,$ but $s'p[qr] \not\simeq s'[pq]r$

Consider ≅, the largest congruence contained in ≃

For any *x*, *y* and any typing

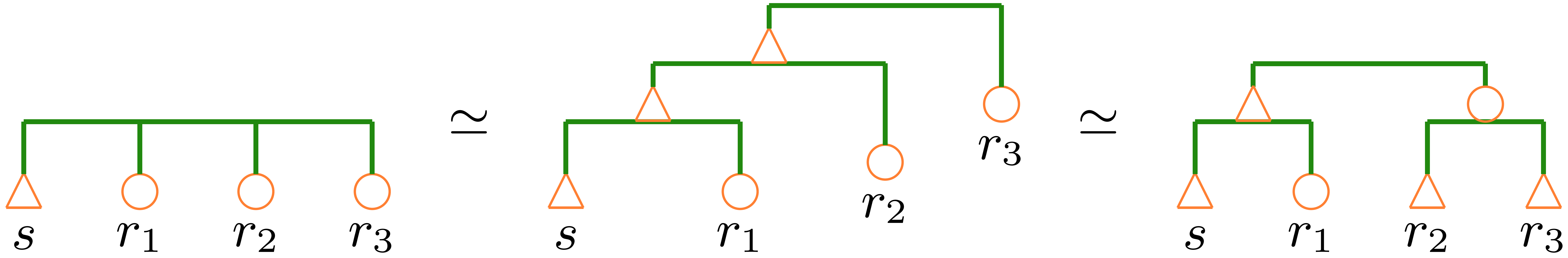
$$x \simeq y \Longleftrightarrow [x]^\alpha \cong [y]^\alpha$$

For monomial *x*, *y*

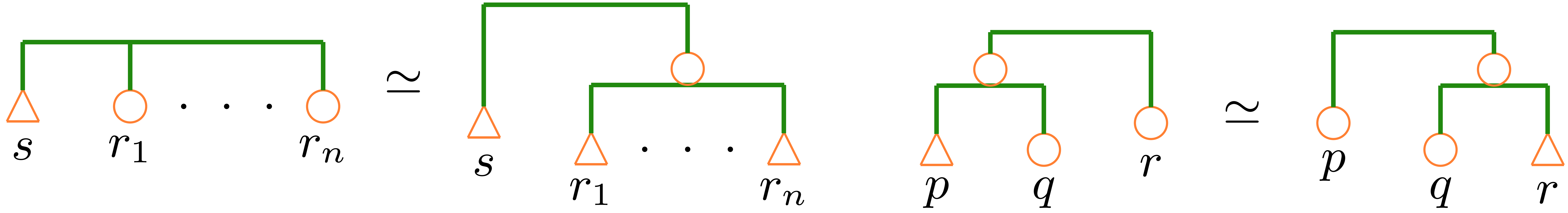
$$x \cong y \Longleftrightarrow \begin{cases} x \simeq y \\ x \cdot 1' \simeq y \cdot 1' \\ \#x > 0 \Leftrightarrow \#y > 0 \end{cases}$$

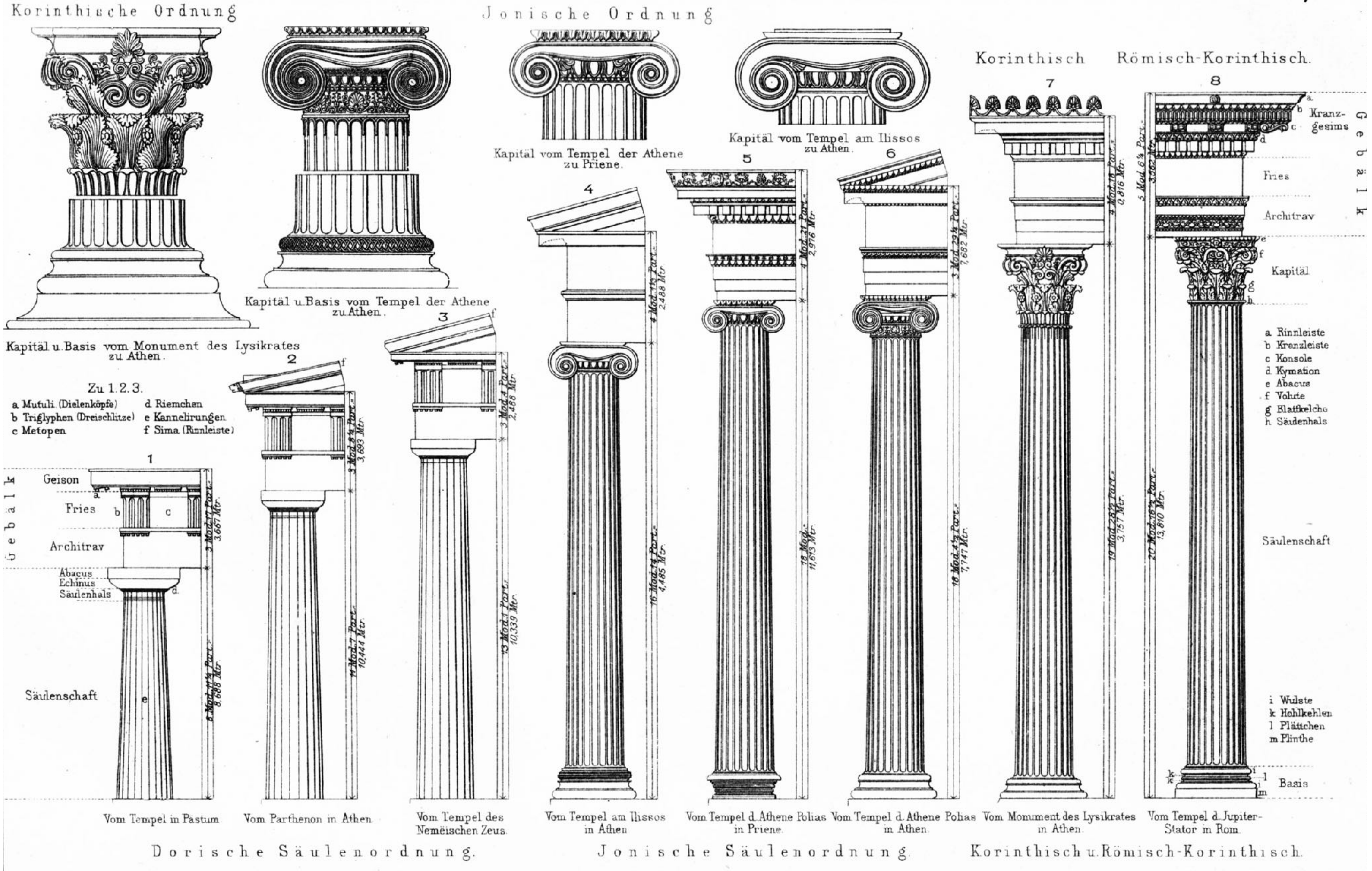
Incrementality & transformation of connectors

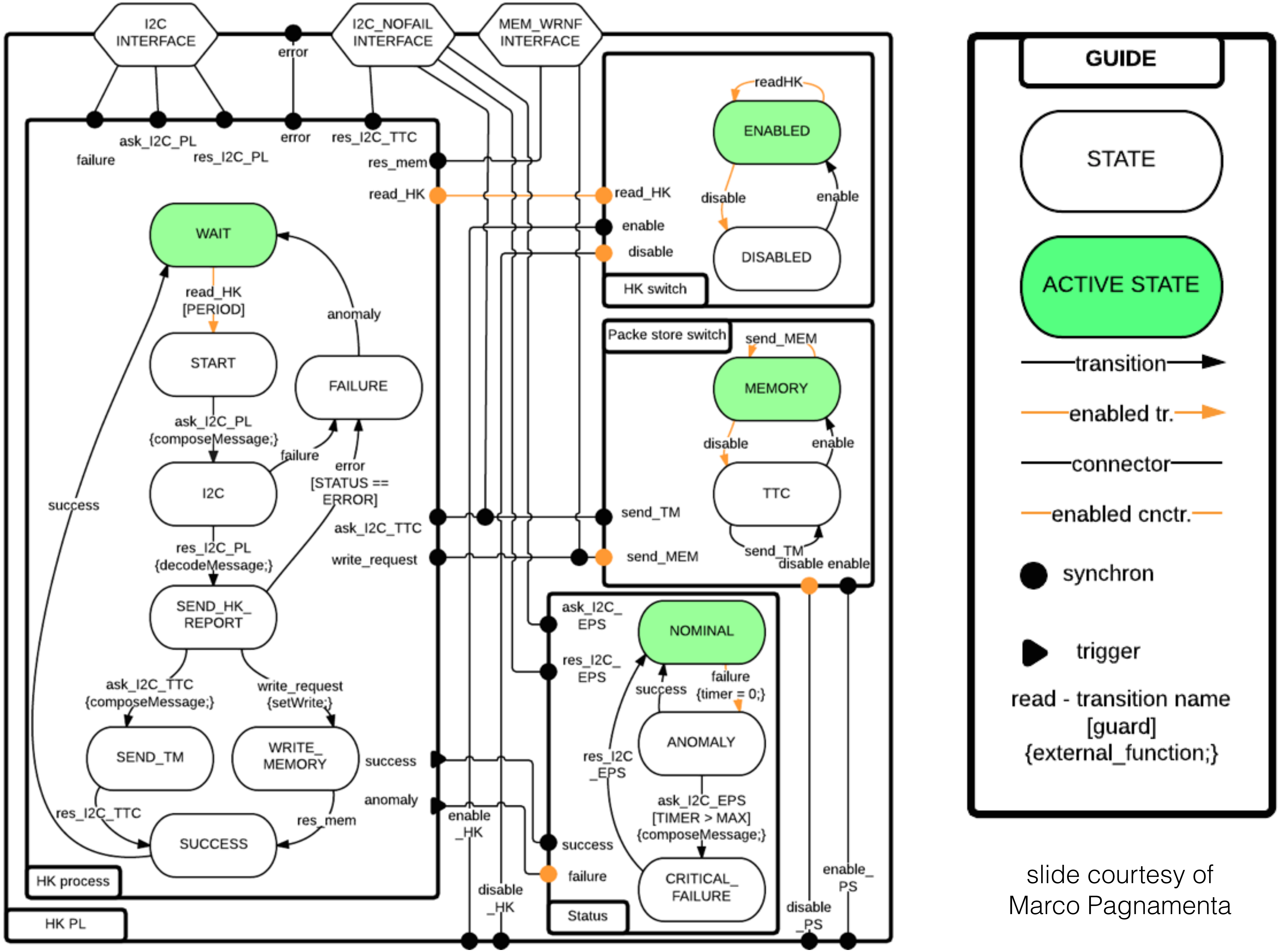
Incremental construction



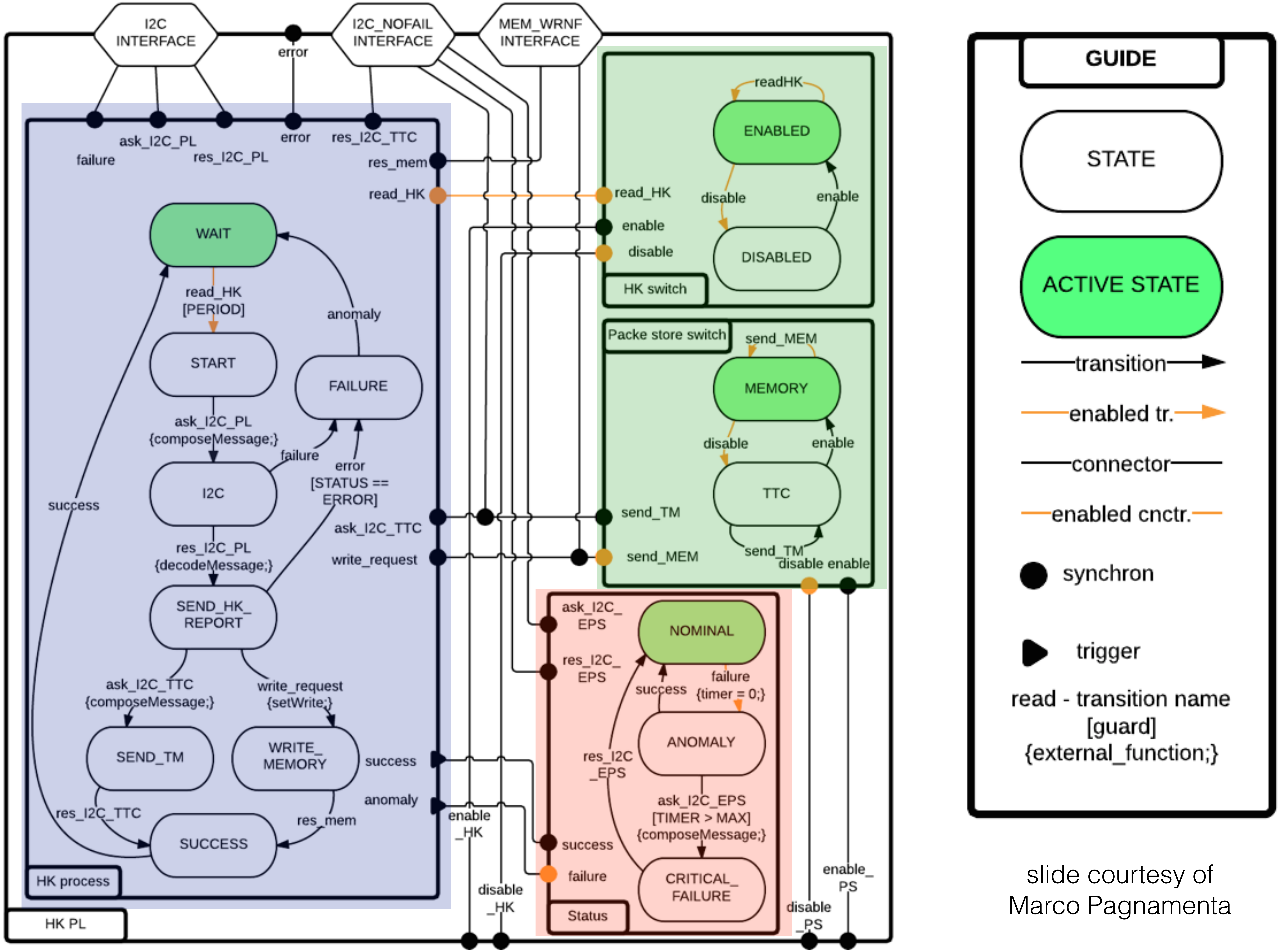
Transformation (separate one port from the connector)




Korinthische Ordnung
Jonische Ordnung
Korinthisch
Römisch-Korinthisch.
Kapitäl u. Basis vom Monument des Lysikrates zu Athen.
Kapitäl u. Basis vom Tempel der Athene zu Athen.
Kapitäl vom Tempel der Athene zu Priene.
Kapitäl vom Tempel am Ilissos zu Athen.
Zu 1.2.3.
a Mutuli (Dielenköpfe)
b Triglyphen (Dreischlitze)
c Metopen
d Riemchen
e Kannelirungen
f Sima (Rinnleiste)
1
2
3
4
5
6
7
8
Geison
Fries
Architrav
Abacus
Echinus
Säulenhals
Säulenschaft
Gebälk
Kranz-gesims
Fries
Architrav
Kapitäl
Säulenschaft
Basis
a Rinnleiste
b Kranzleiste
c Konsole
d Kymation
e Abacus
f Volute
g Blattkelche
h Säulenhals
i Wulste
k Hohlkehlen
l Plättchen
m Plinthe
Vom Tempel in Pästum
Vom Parthenon in Athen
Vom Tempel des Nemëischen Zeus.
Vom Tempel am Ilissos in Athen
Vom Tempel d. Athene Polias in Priene.
Vom Tempel d. Athene Polias in Athen
Vom Monument des Lysikrates in Athen.
Vom Tempel d. Jupiter-Stator in Rom.
Dorische Säulenordnung.
Jonische Säulenordnung.
Korinthisch u. Römisch-Korinthisch.



slide courtesy of Marco Pagnamenta



slide courtesy of
Marco Pagnamenta

Theory of architectures

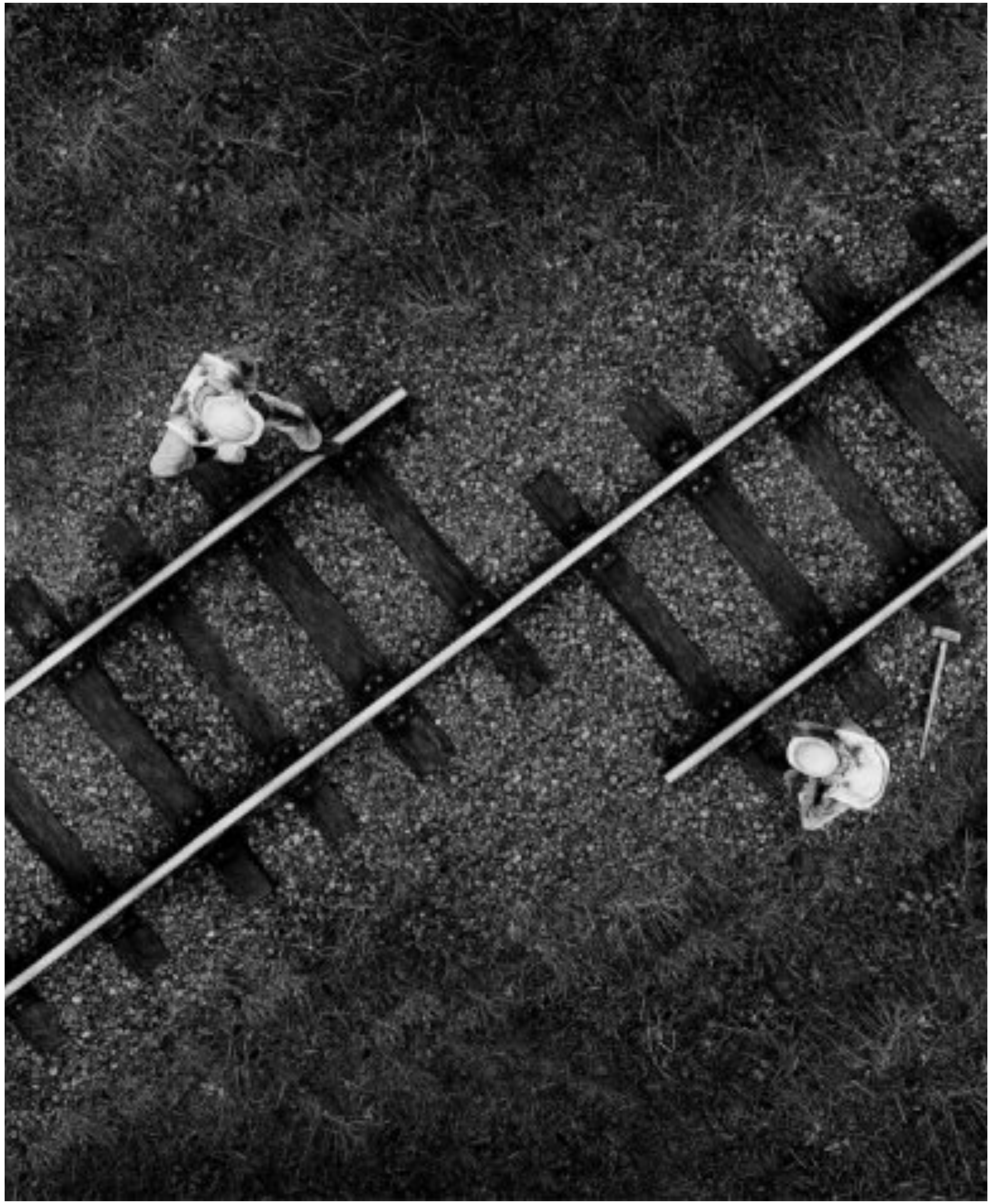
Design patterns for BIP

How to model?

How to combine?

How to specify?

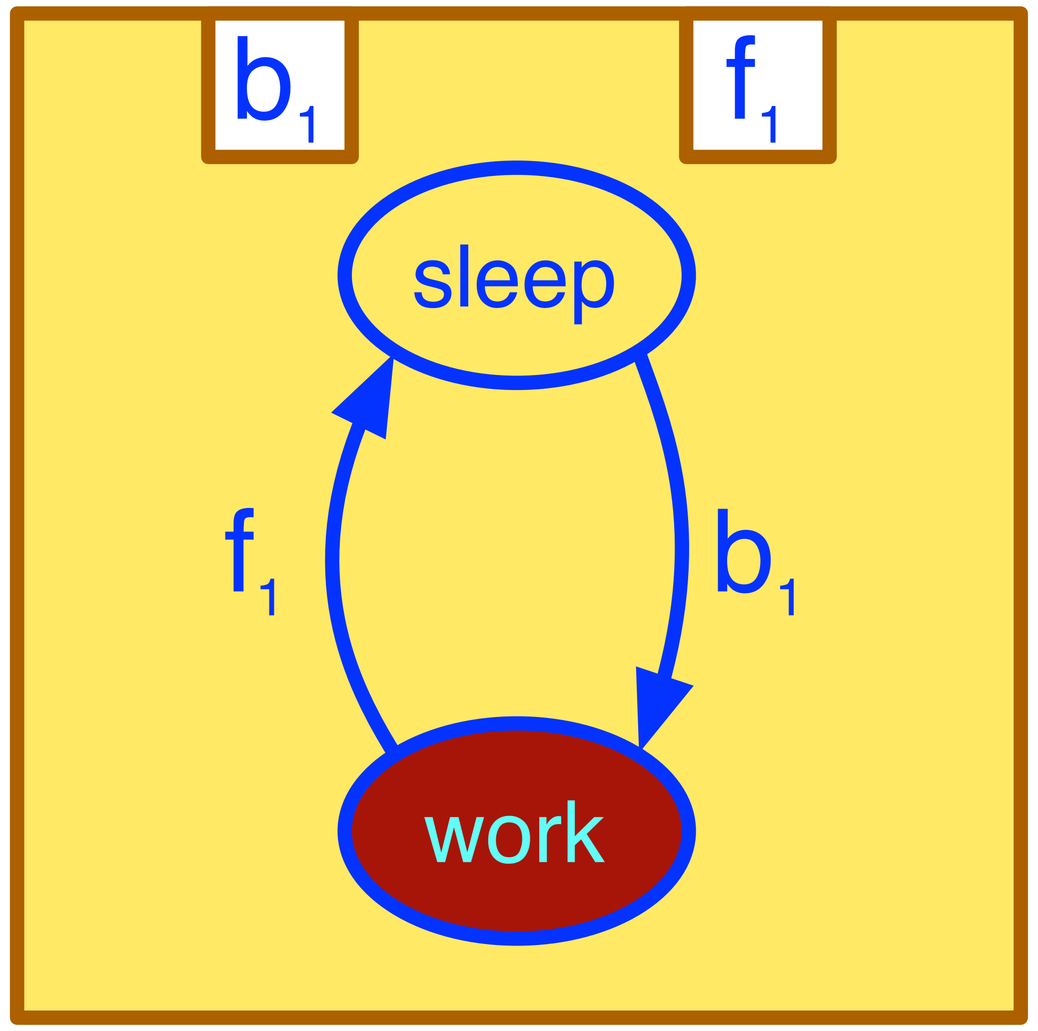
Architectures enforce characteristic properties. The crucial question is whether these are preserved by composition?

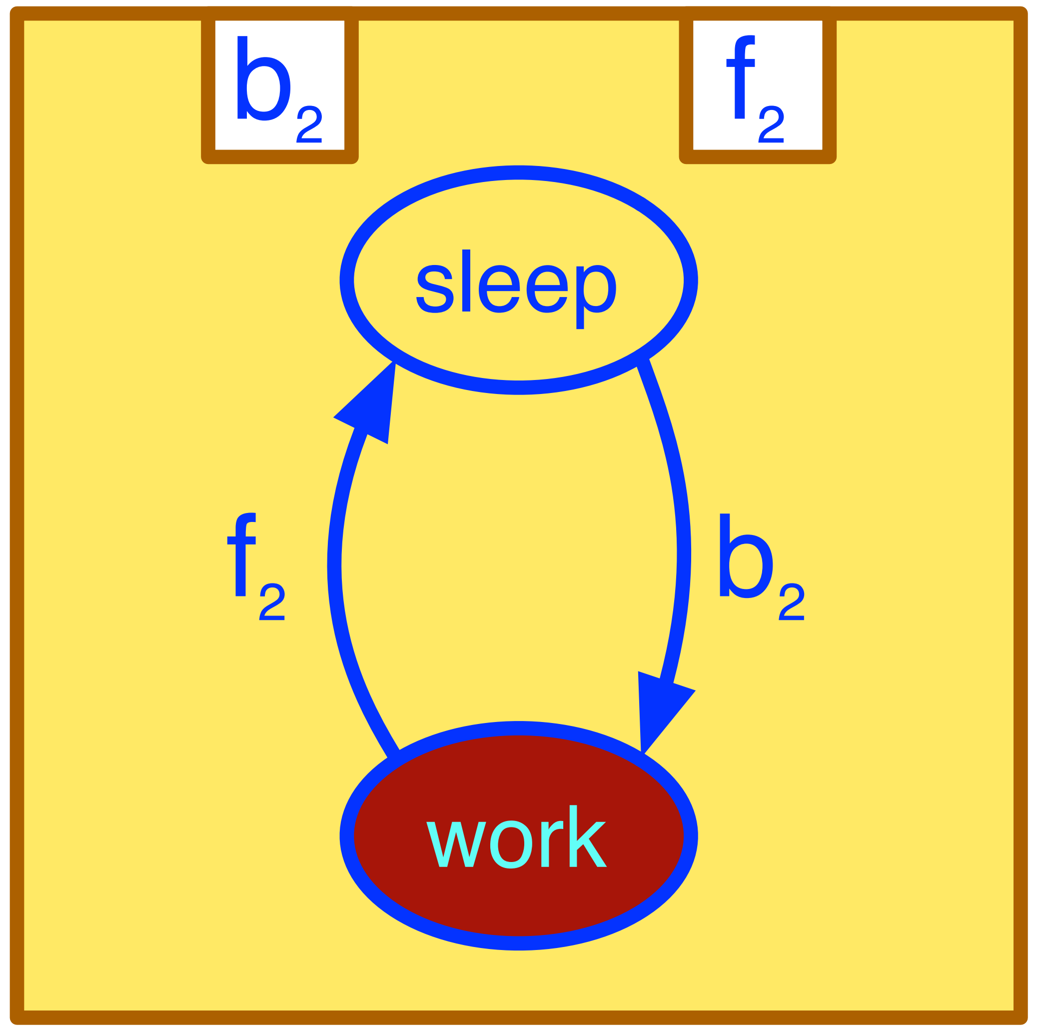


[Attie et al, SEFM '14]

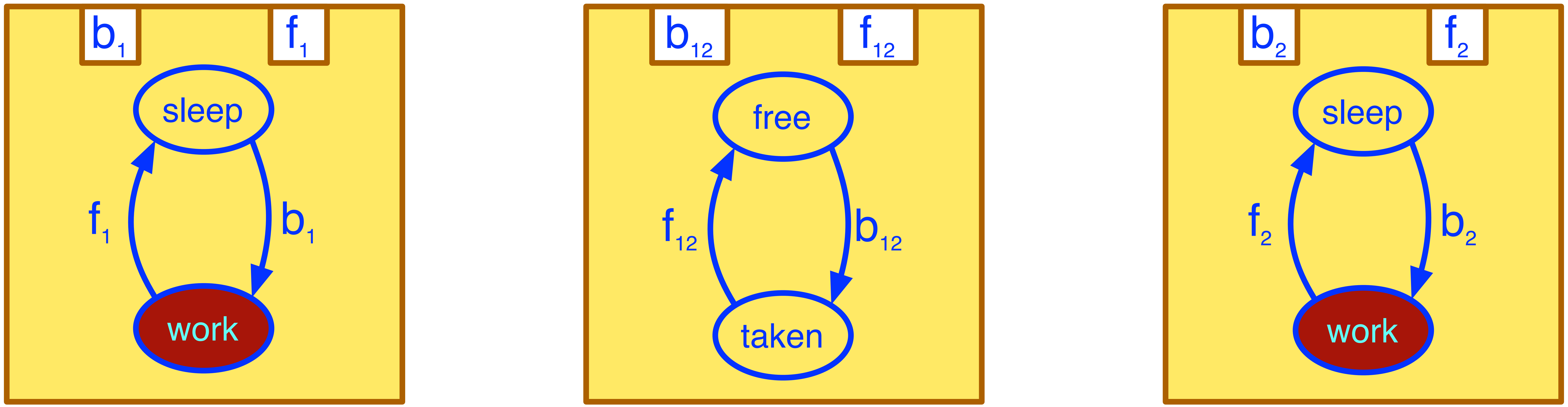
How to model?

Example: Lock

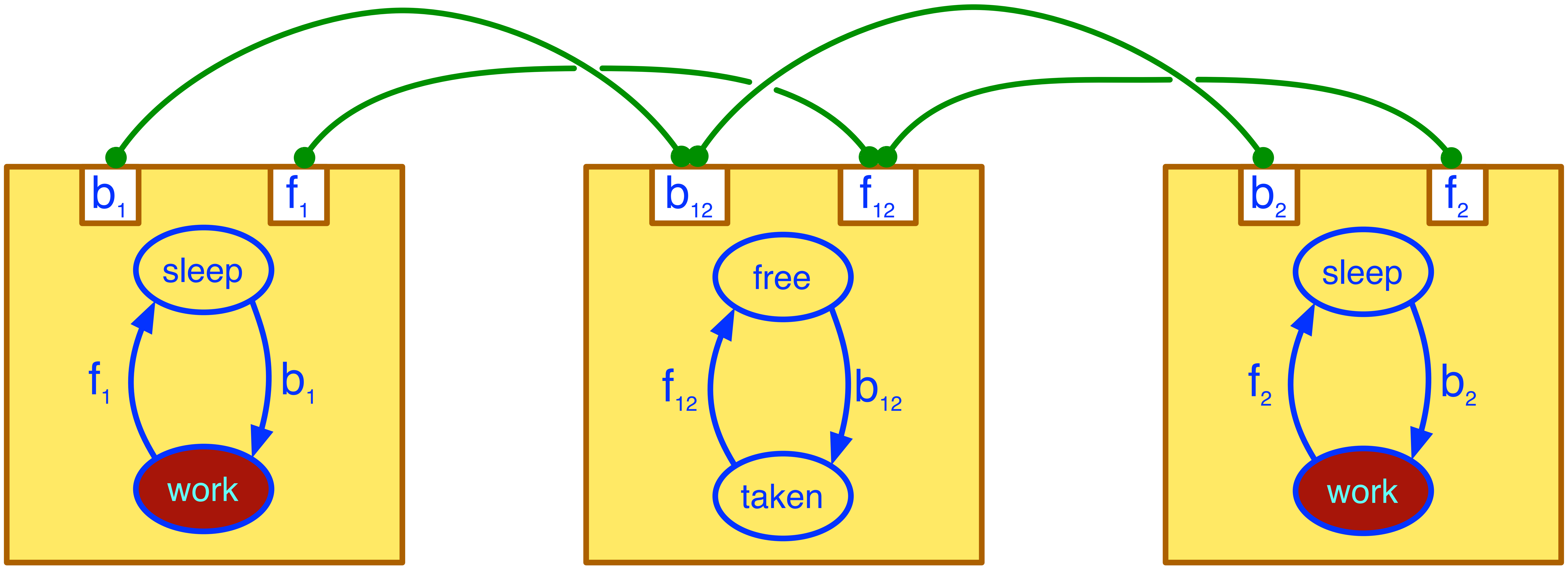




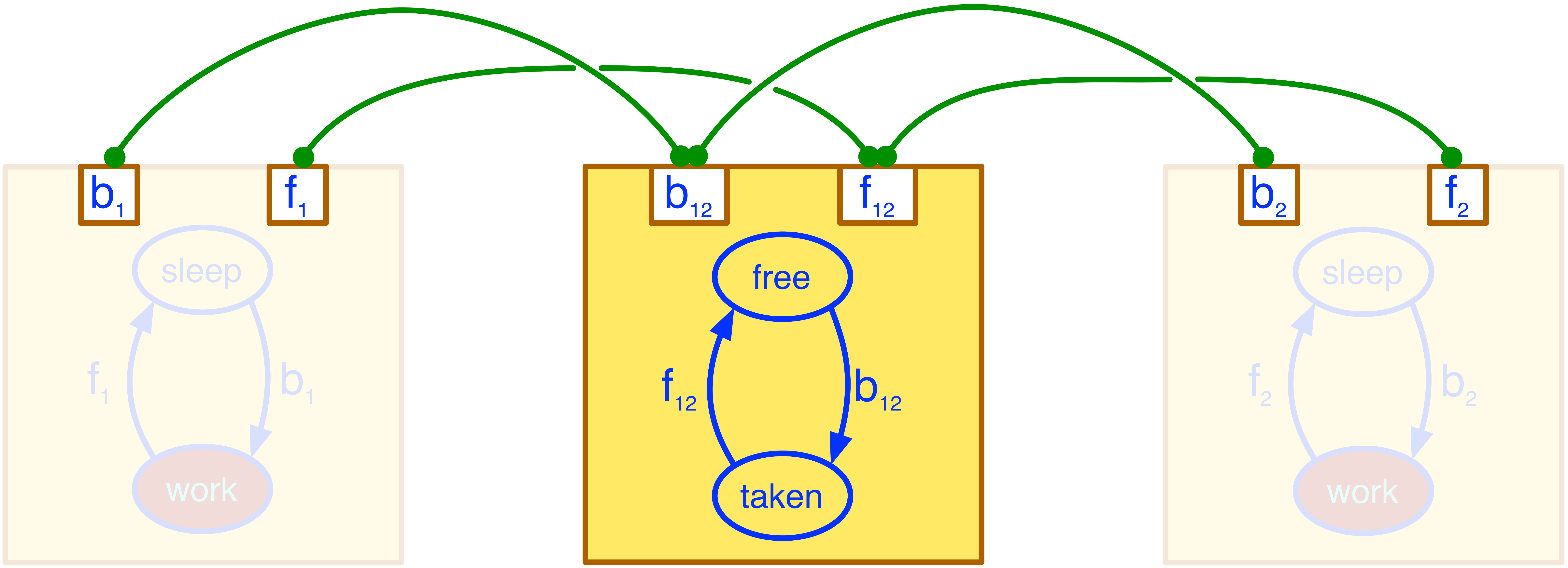
Example: Lock



Example: Lock



Example: Lock



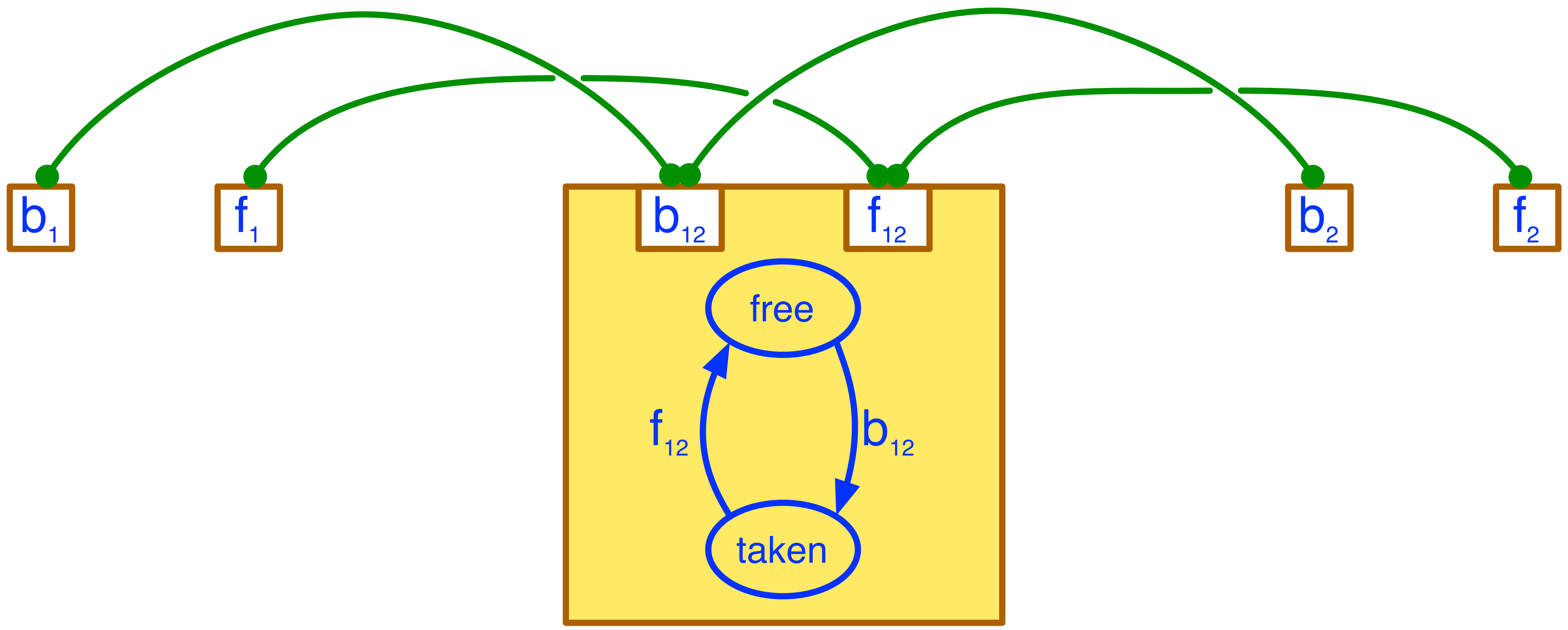
An architecture is...

$$A = (\mathcal{C}, P_A, \gamma)$$

Set of coordinating behaviours

Interface (ports)

Interaction model



...an operator…

$$A = (\mathcal{C}, P_A, \gamma)$$

…transforming

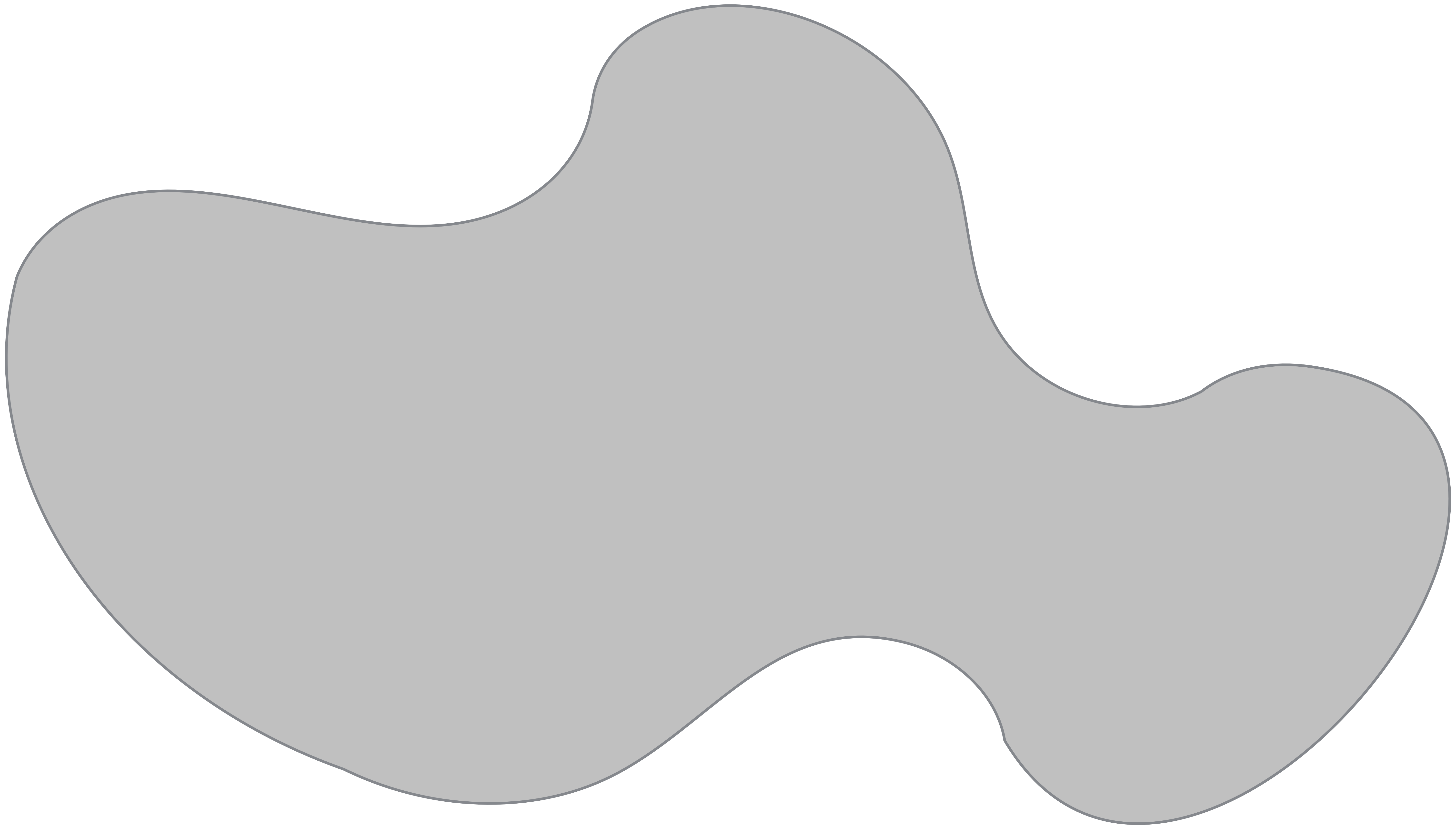
a set of components $\mathcal{B}$

into a composed BIP system $A(\mathcal{B}) \stackrel{def}{=} \Big(\gamma \ltimes P\Big)(\mathcal{B} \cup \mathcal{C})$

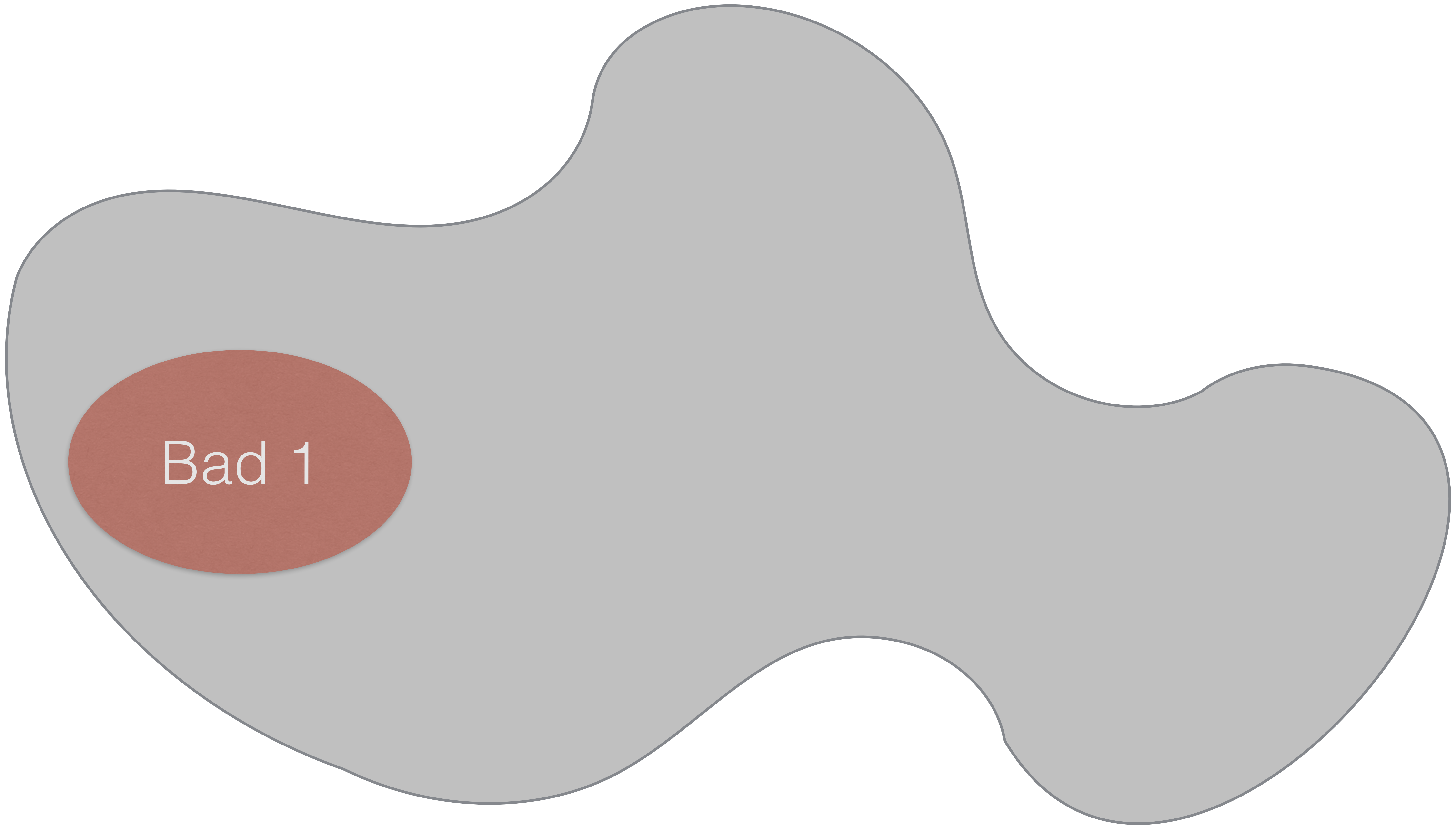
where $P \stackrel{def}{=} \bigcup_{B \in \mathcal{B} \cup \mathcal{C}} P_B, \quad \gamma \ltimes P \stackrel{def}{=} \left\{a \subseteq 2^P \,\middle|\, a \cap P_A \in \gamma\right\}$

How to combine?

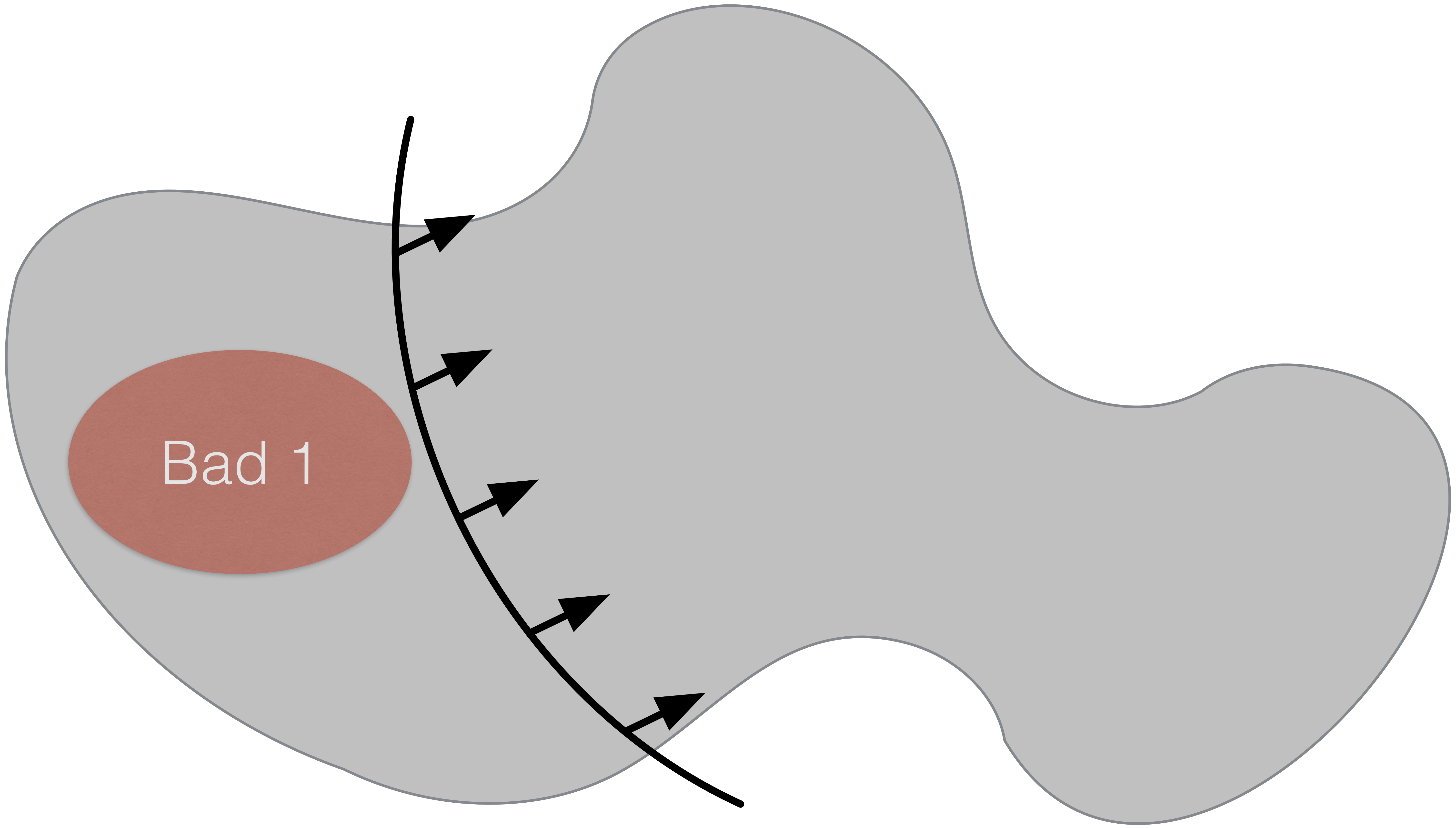
Constraints intuition



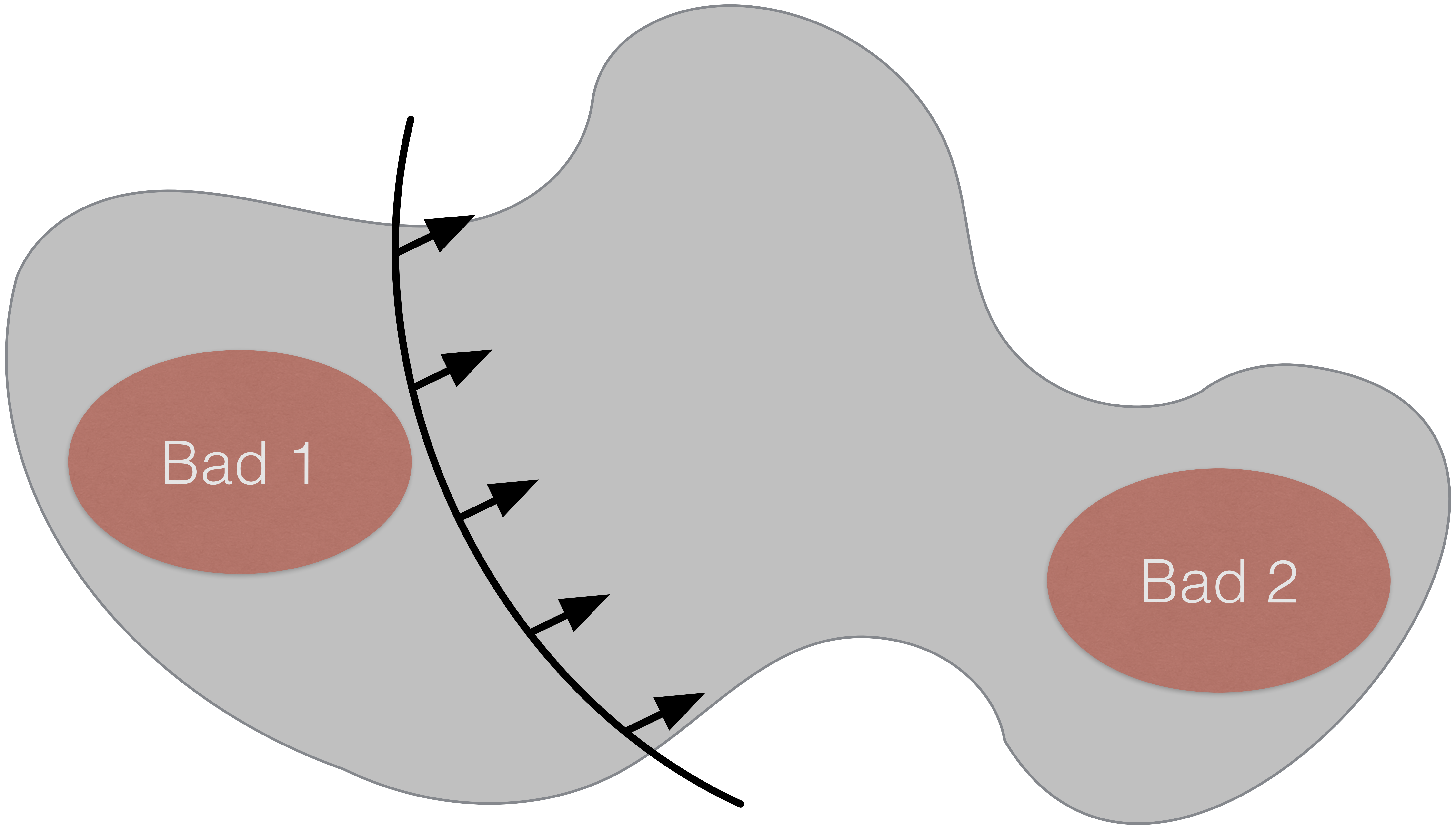
Constraints intuition



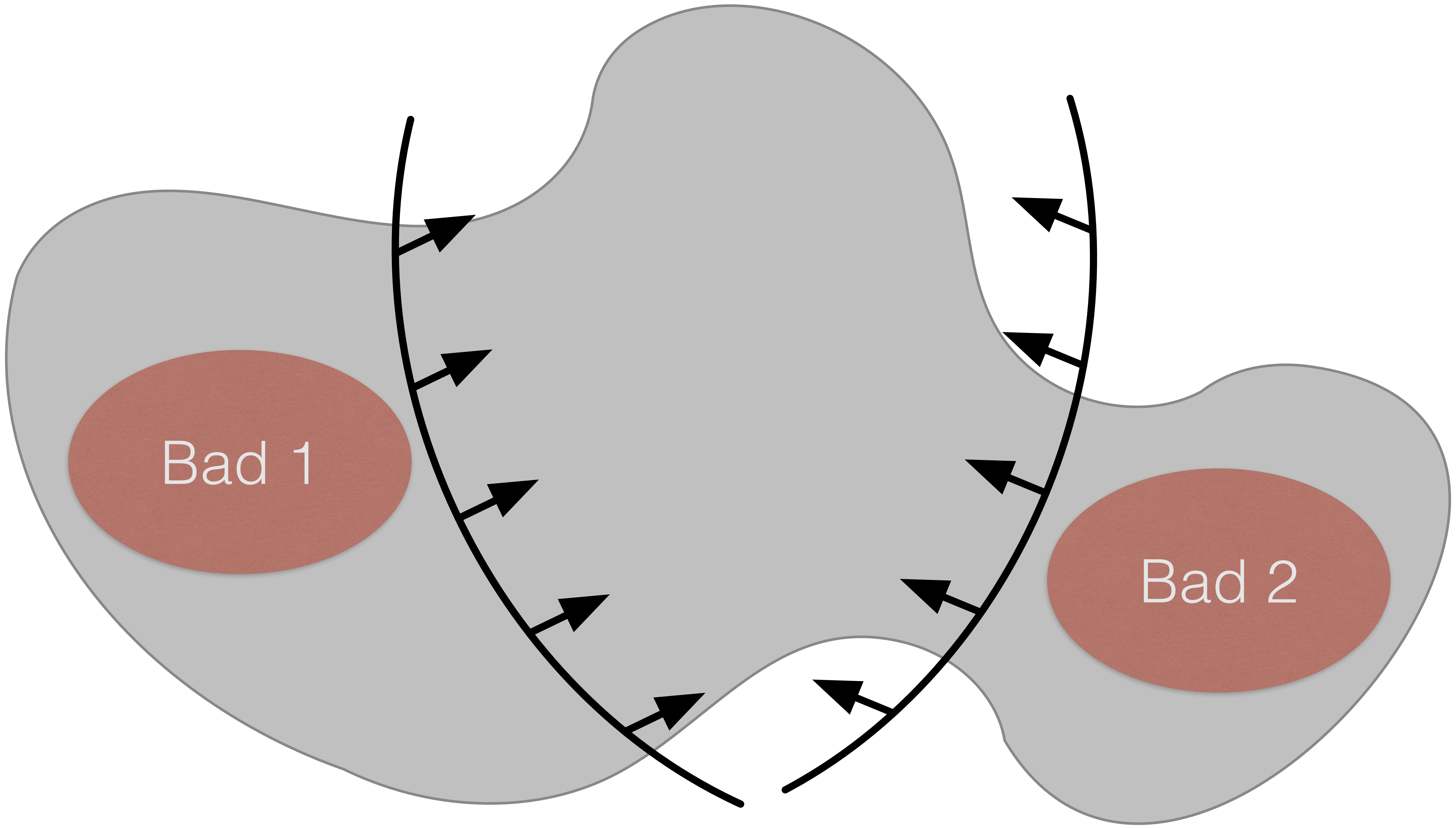
Constraints intuition



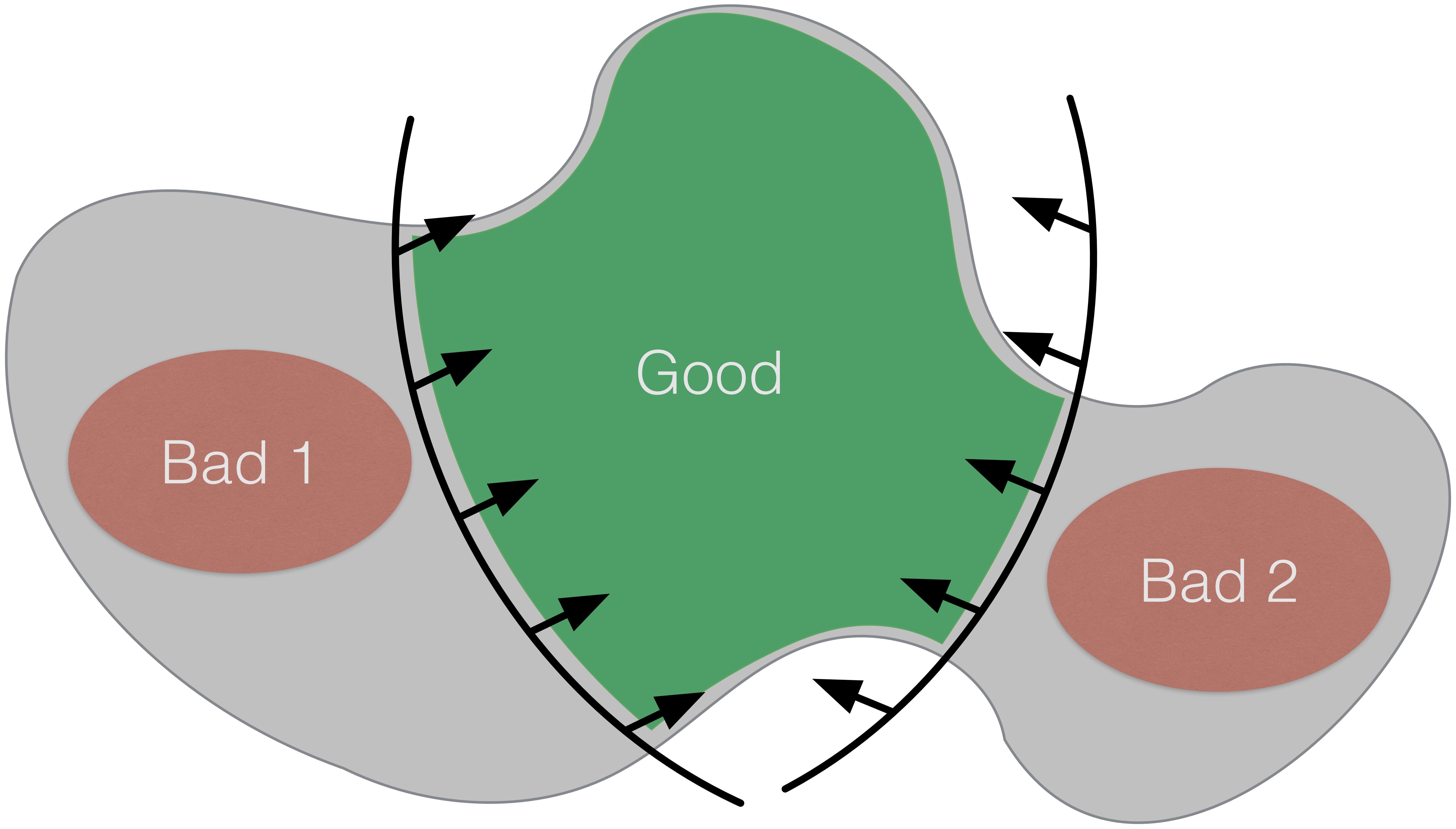
Constraints intuition



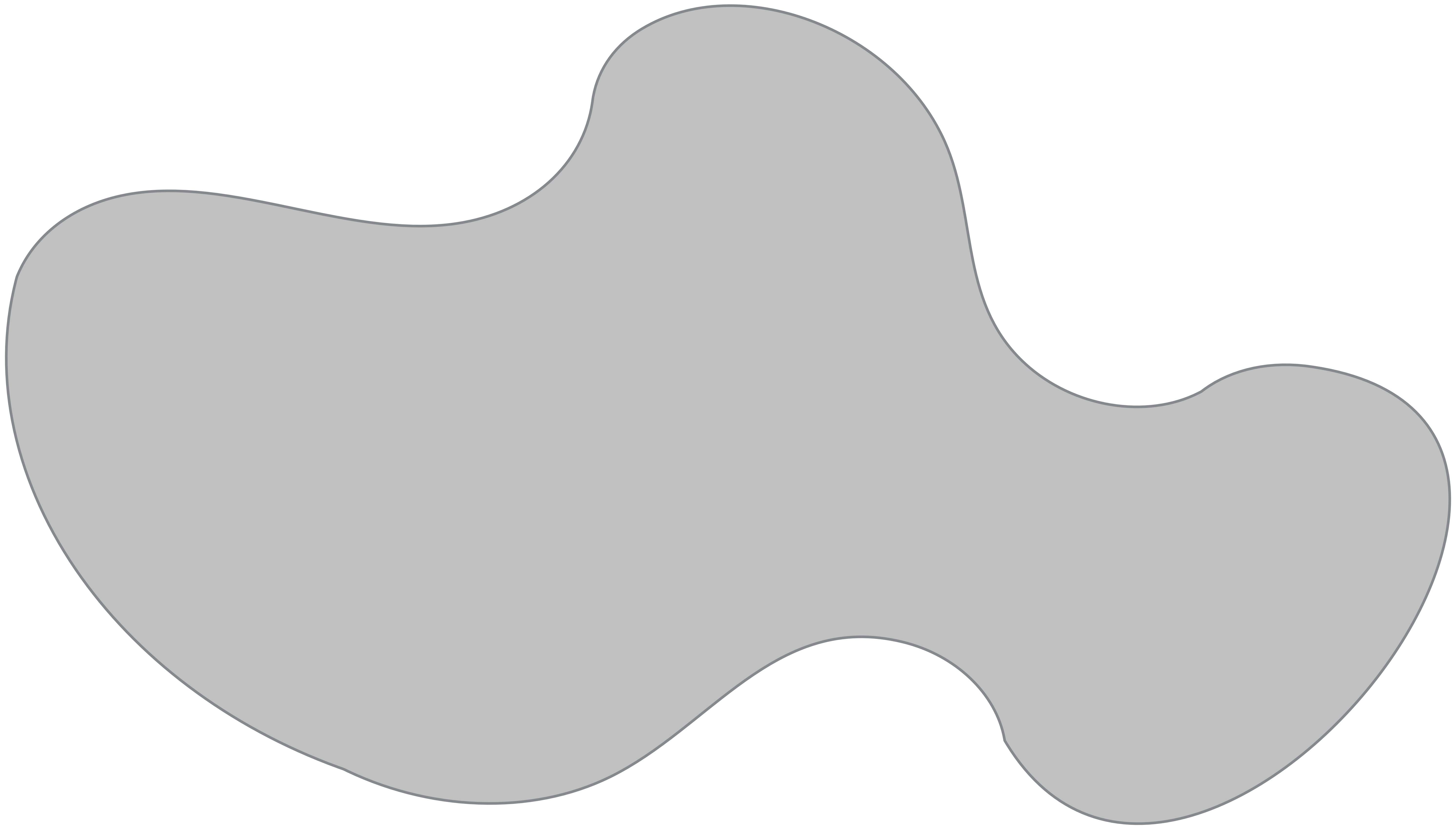
Constraints intuition



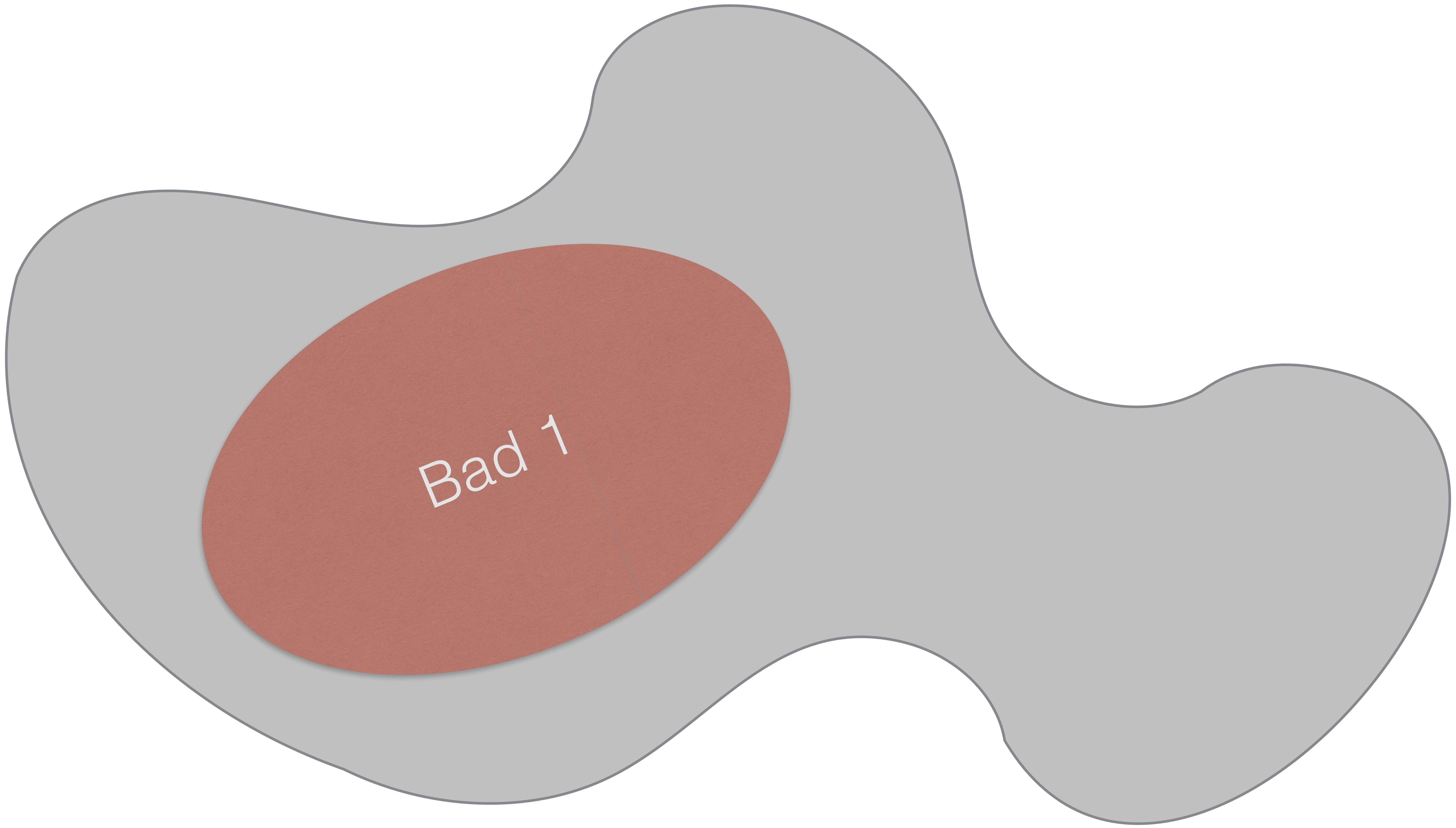
Constraints intuition



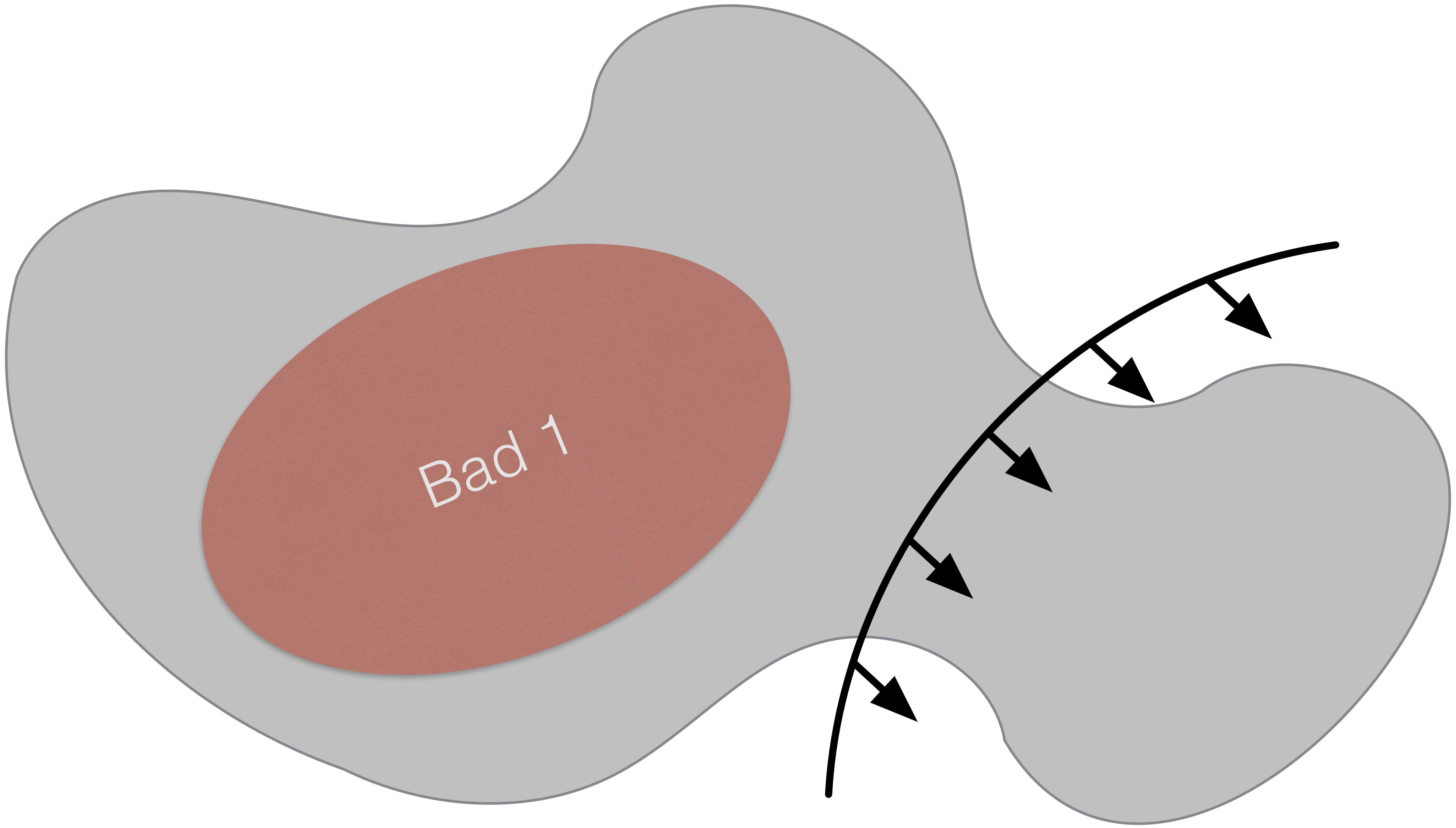
Limits of white magic



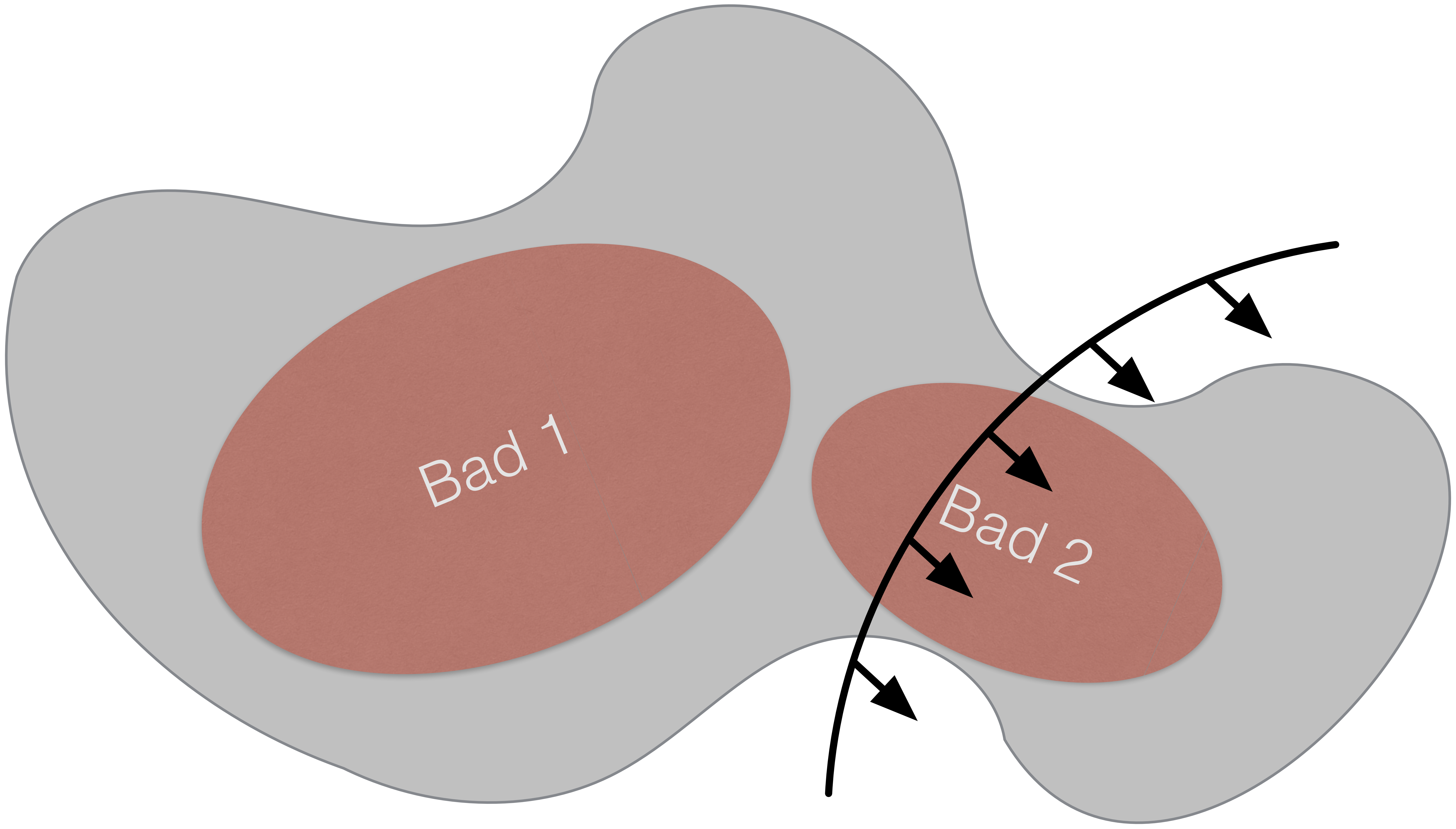
Limits of white magic



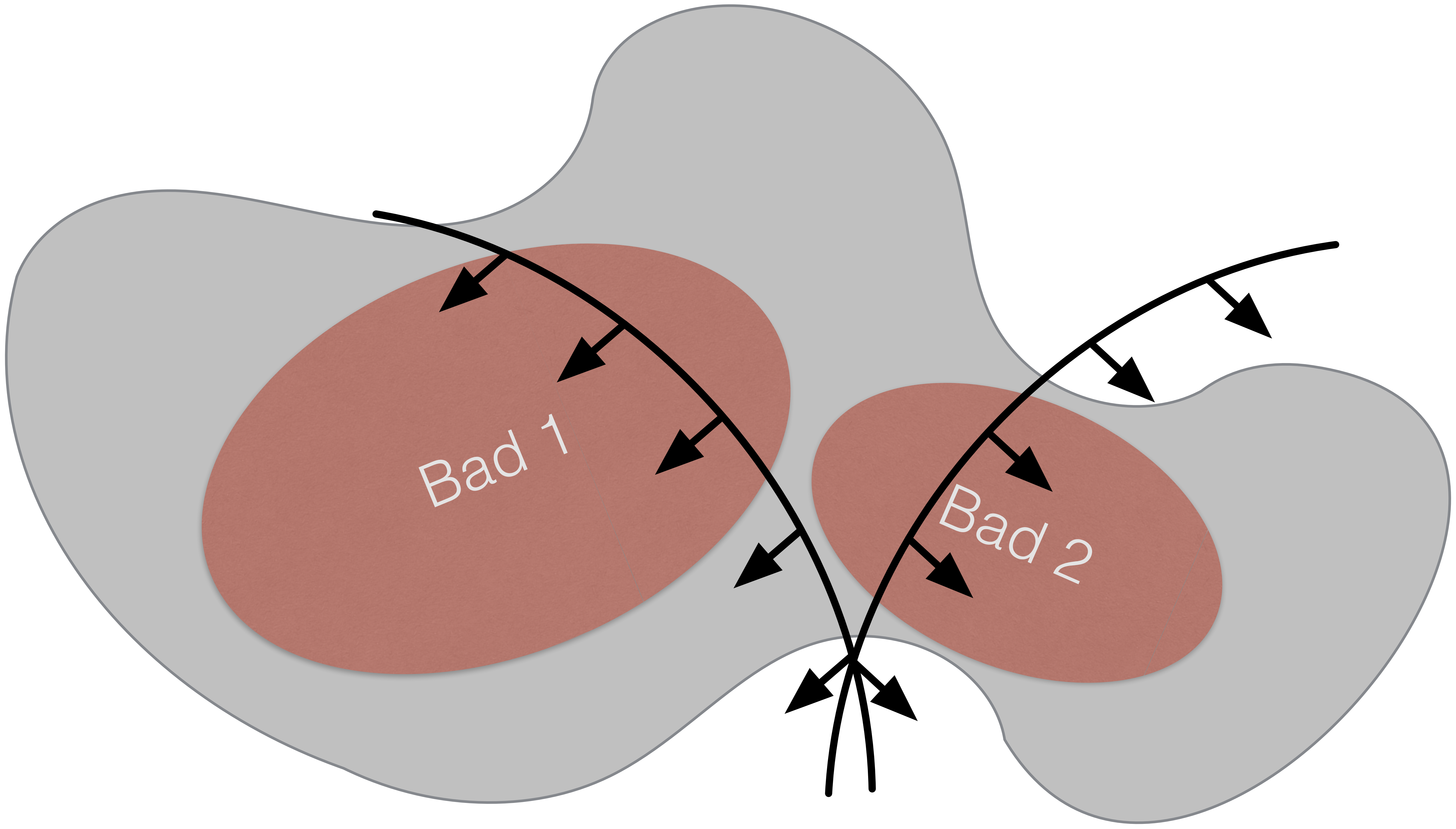
Limits of white magic



Limits of white magic



Limits of white magic



Formally

$$A_1 \oplus A_2 \stackrel{def}{=} (\mathcal{C}_1 \cup \mathcal{C}_2, P_1 \cup P_2, \gamma)$$

$$\begin{aligned}\gamma &\stackrel{def}{=} \left\{a \subseteq 2^P \,\middle|\, a \cap P_1 \in \gamma_1 \;\wedge\; a \cap P_2 \in \gamma_2\right\} \\ &= (\gamma_1 \ltimes P) \cap (\gamma_2 \ltimes P)\end{aligned}$$

Main idea

Characteristic predicate for $\gamma \subseteq 2^P$

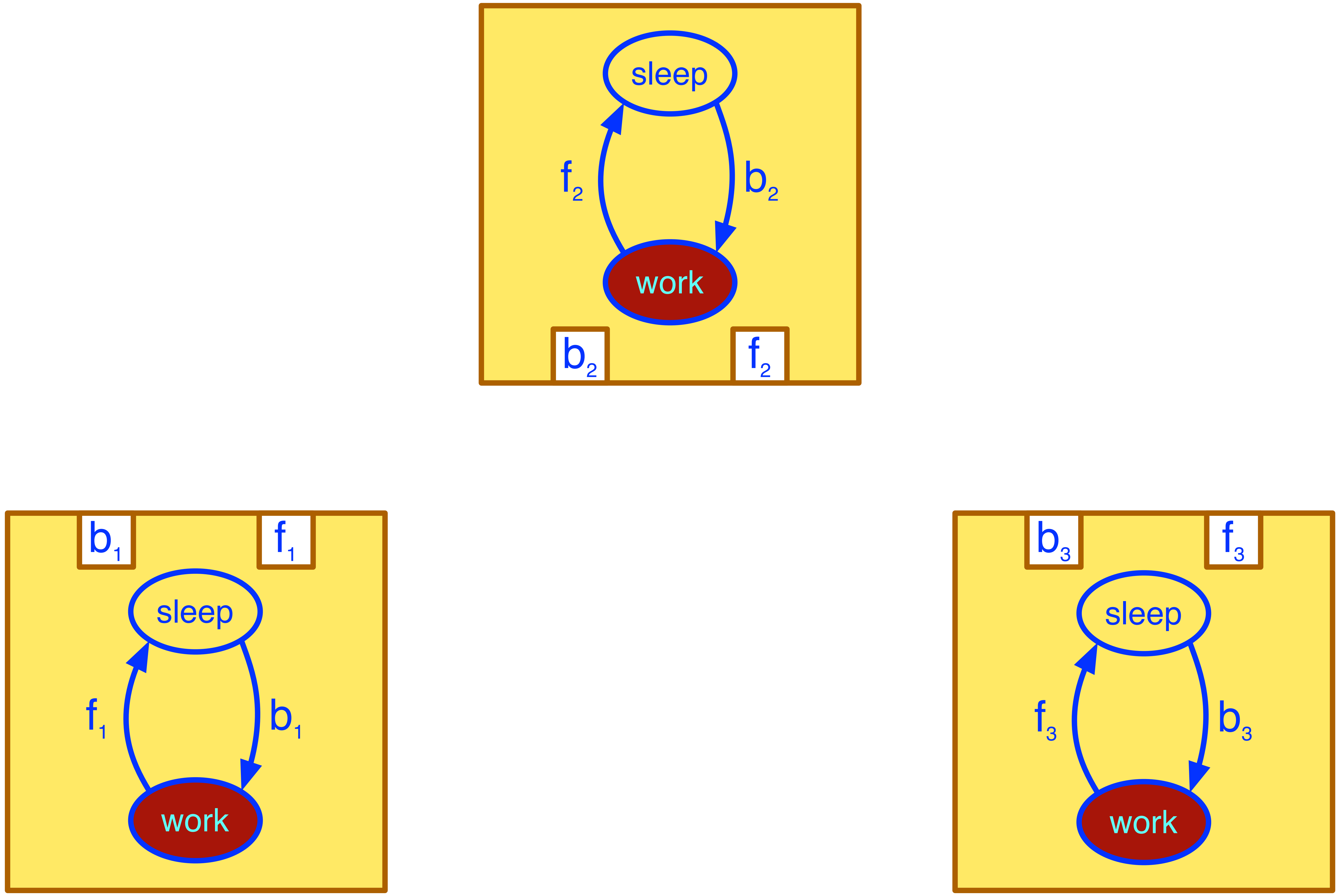
$$\varphi_\gamma : \mathbb{B}^P \to \mathbb{B} \qquad\qquad \varphi_\gamma \triangleq \bigvee_{a \in \gamma} \left(\bigwedge_{p \in a} p \wedge \bigwedge_{p \notin a} \overline{p} \right)$$

Interaction models to predicates and back

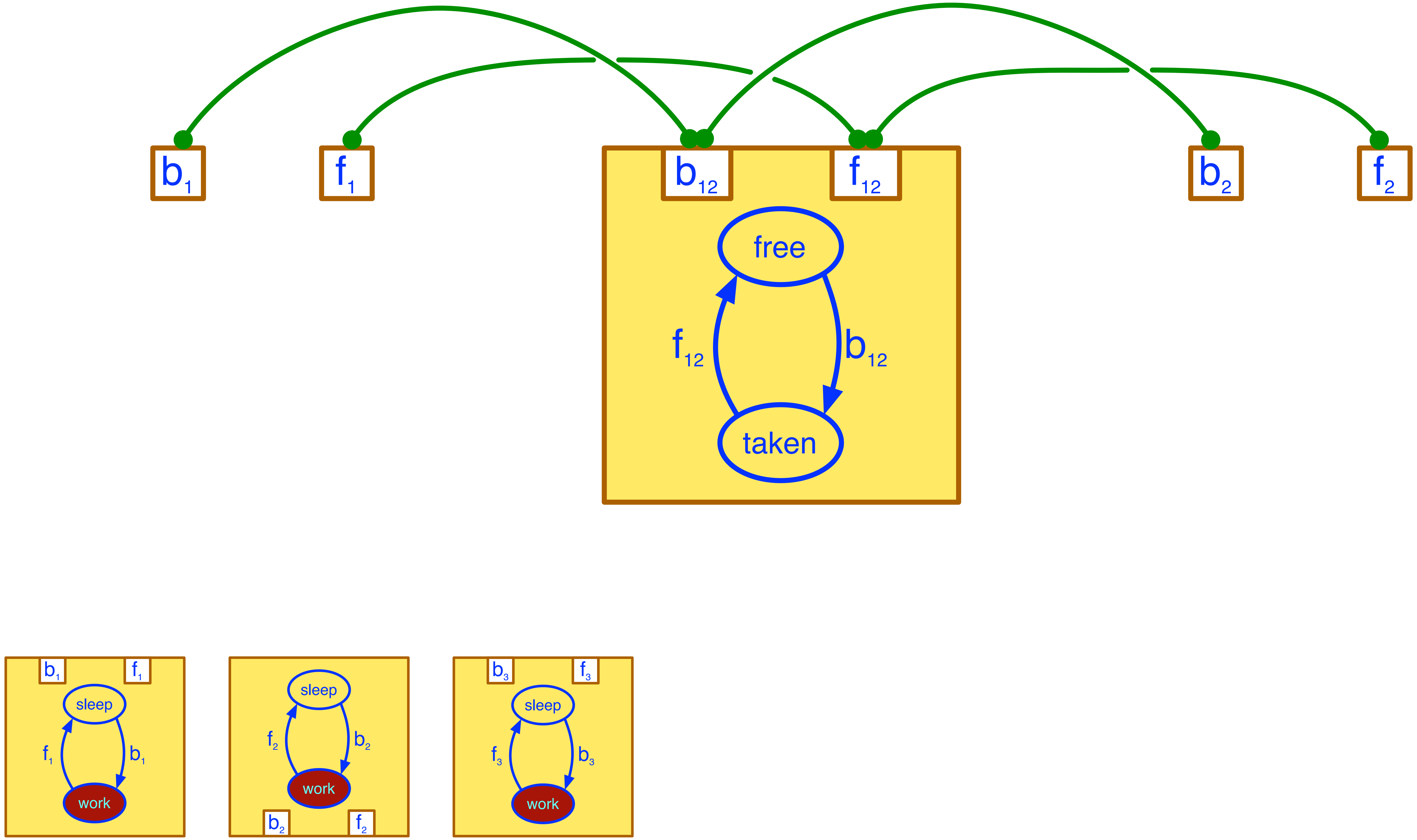
$$v : P \to \mathbb{B}, \qquad \varphi(v) = \mathtt{tt} \iff \{p \in P \,|\, v(p) = \mathtt{tt}\} \in \gamma$$

$$A_1 \oplus A_2 = (\mathcal{C}_1 \cup \mathcal{C}_2, P_1 \cup P_2, \gamma_\varphi) \qquad \varphi = \varphi_{\gamma_1} \wedge \varphi_{\gamma_2}$$

Example continued

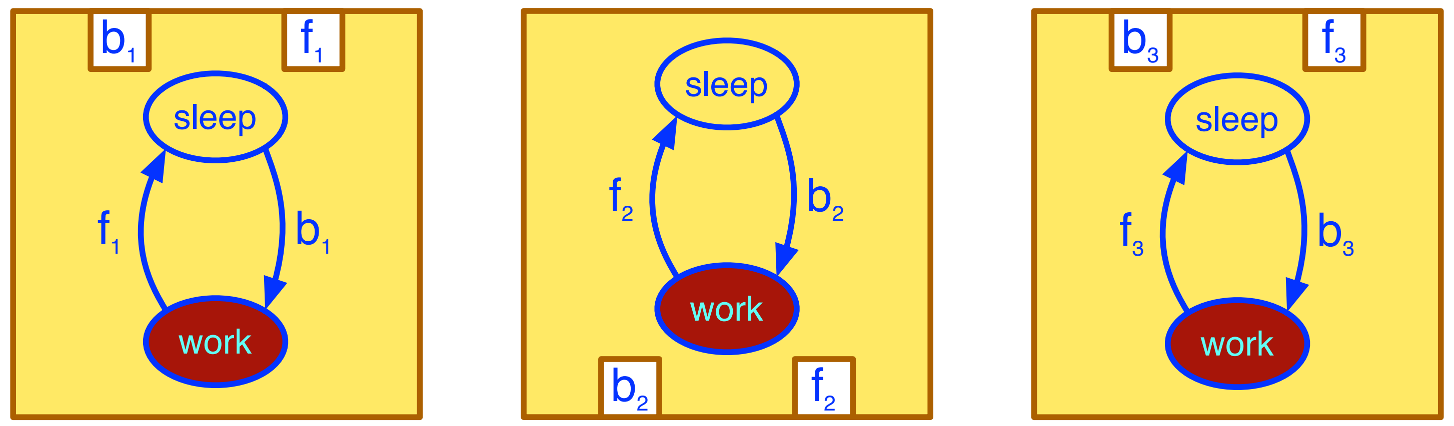


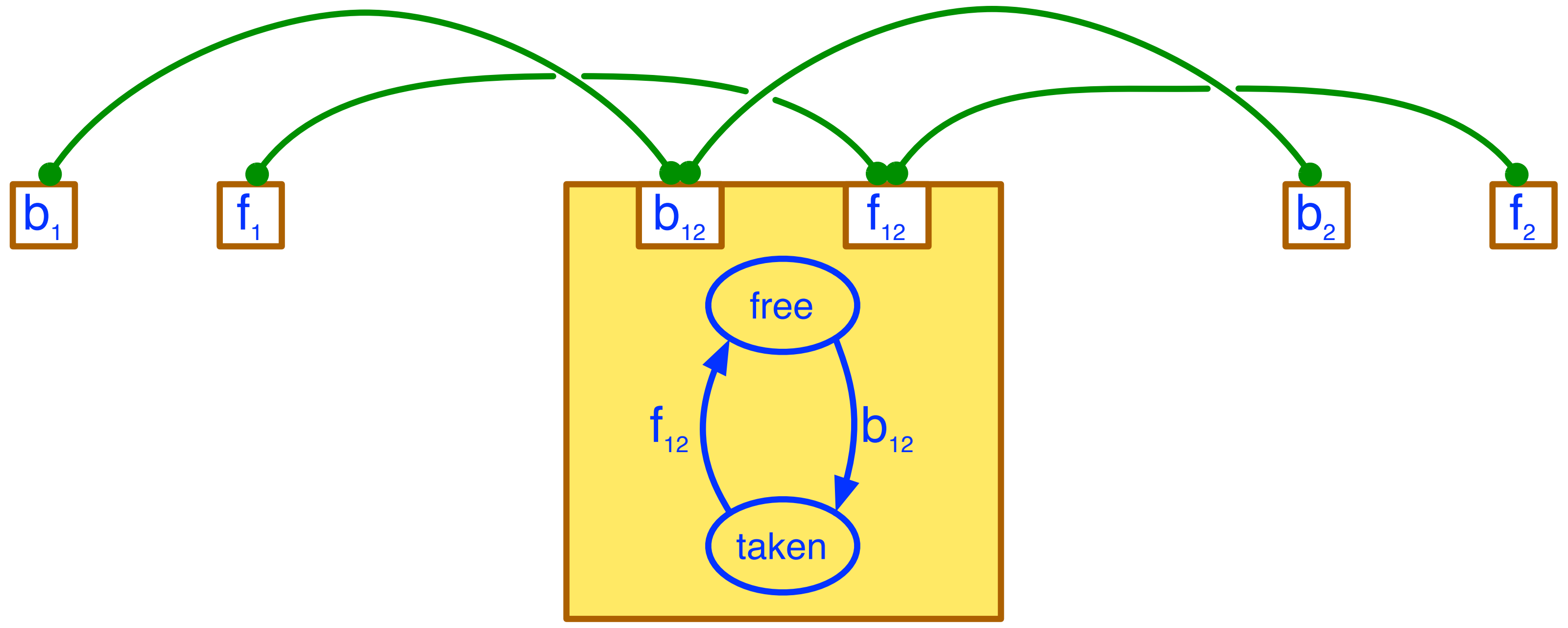
Example continued



Example continued

$$\varphi_{\gamma_{12}} \equiv (b_1 \Rightarrow b_{12}) \wedge (f_1 \Rightarrow f_{12}) \wedge (b_2 \Rightarrow b_{12}) \wedge (f_2 \Rightarrow f_{12}) \wedge$$
$$(b_{12} \Rightarrow b_1 \,\texttt{XOR}\, b_2) \wedge (f_{12} \Rightarrow f_1 \,\texttt{XOR}\, f_2) \wedge (b_{12} \Rightarrow \overline{f_{12}})$$

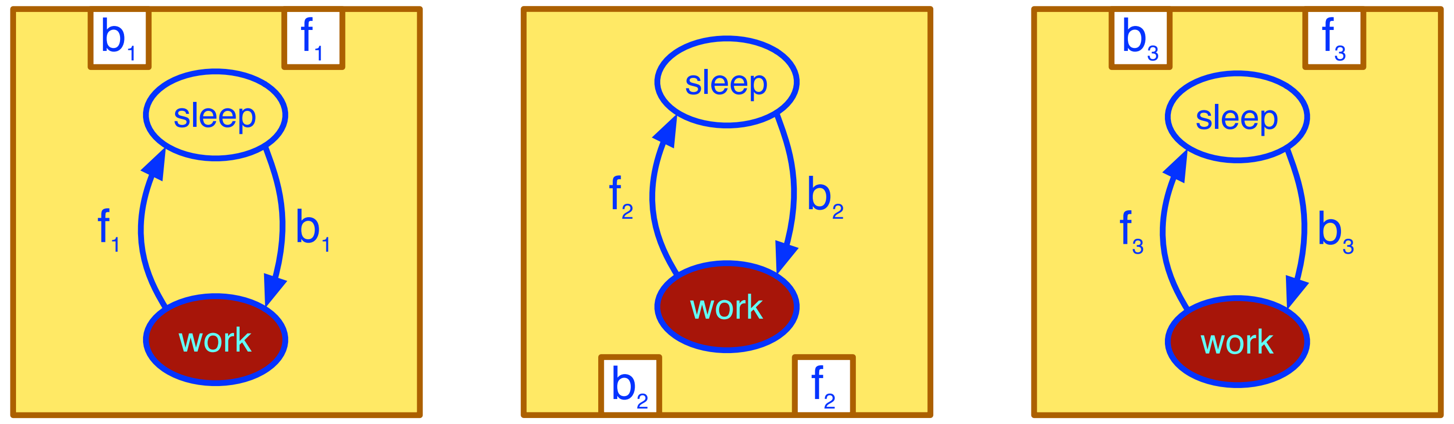


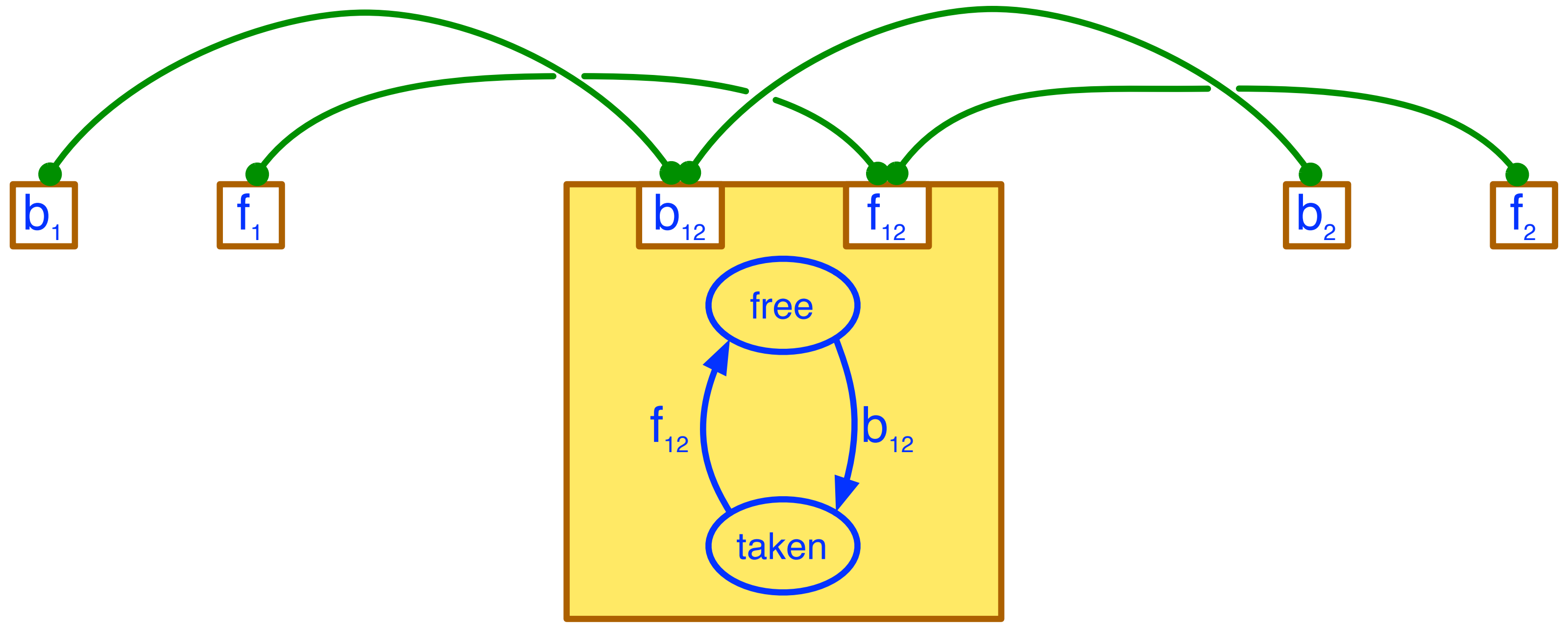


Example continued

$$\varphi_{\gamma_{12}} \equiv (b_1 \Rightarrow b_{12}) \wedge (f_1 \Rightarrow f_{12}) \wedge (b_2 \Rightarrow b_{12}) \wedge (f_2 \Rightarrow f_{12}) \wedge$$
$$(b_{12} \Rightarrow b_1 \,\mathtt{XOR}\, b_2) \wedge (f_{12} \Rightarrow f_1 \,\mathtt{XOR}\, f_2) \wedge (b_{12} \Rightarrow \overline{f_{12}})$$

$$\begin{array}{lllll}
b_1 \Rightarrow b_{12} \wedge b_{13}\,, & f_1 \Rightarrow f_{12} \wedge f_{13}\,, & b_{12} \Rightarrow b_1 \,\mathtt{XOR}\, b_2\,, & f_{12} \Rightarrow f_1 \,\mathtt{XOR}\, f_2\,, & b_{12} \Rightarrow \overline{f_{12}} \\
b_2 \Rightarrow b_{12} \wedge b_{23}\,, & f_2 \Rightarrow f_{12} \wedge f_{23}\,, & b_{13} \Rightarrow b_1 \,\mathtt{XOR}\, b_3\,, & f_{13} \Rightarrow f_1 \,\mathtt{XOR}\, f_3\,, & b_{13} \Rightarrow \overline{f_{13}} \\
b_3 \Rightarrow b_{13} \wedge b_{23}\,, & f_3 \Rightarrow f_{13} \wedge f_{23}\,, & b_{23} \Rightarrow b_2 \,\mathtt{XOR}\, b_3\,, & f_{23} \Rightarrow f_2 \,\mathtt{XOR}\, f_3\,, & b_{23} \Rightarrow \overline{f_{23}}
\end{array}$$



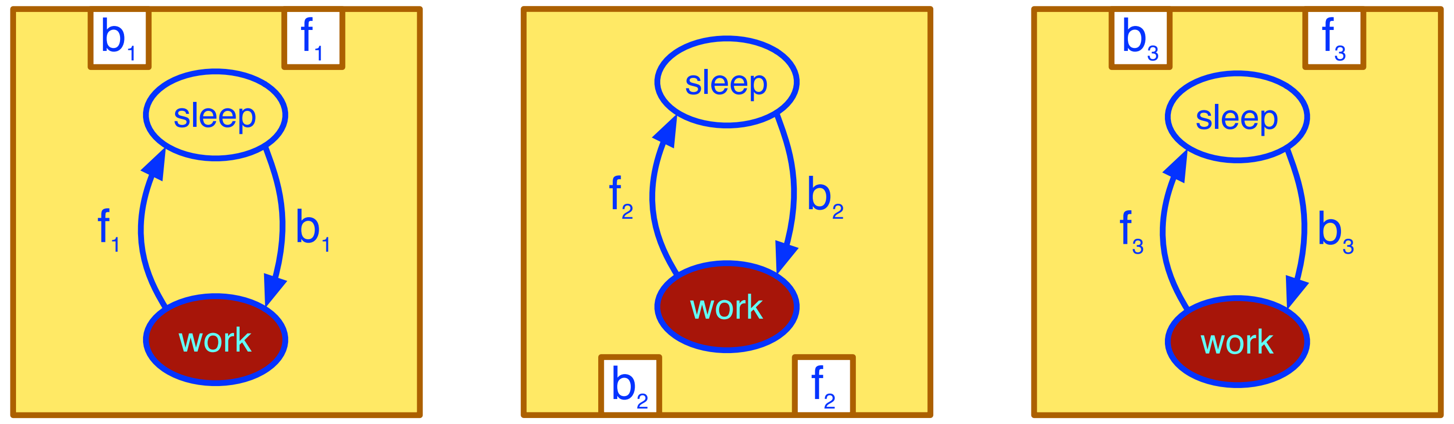


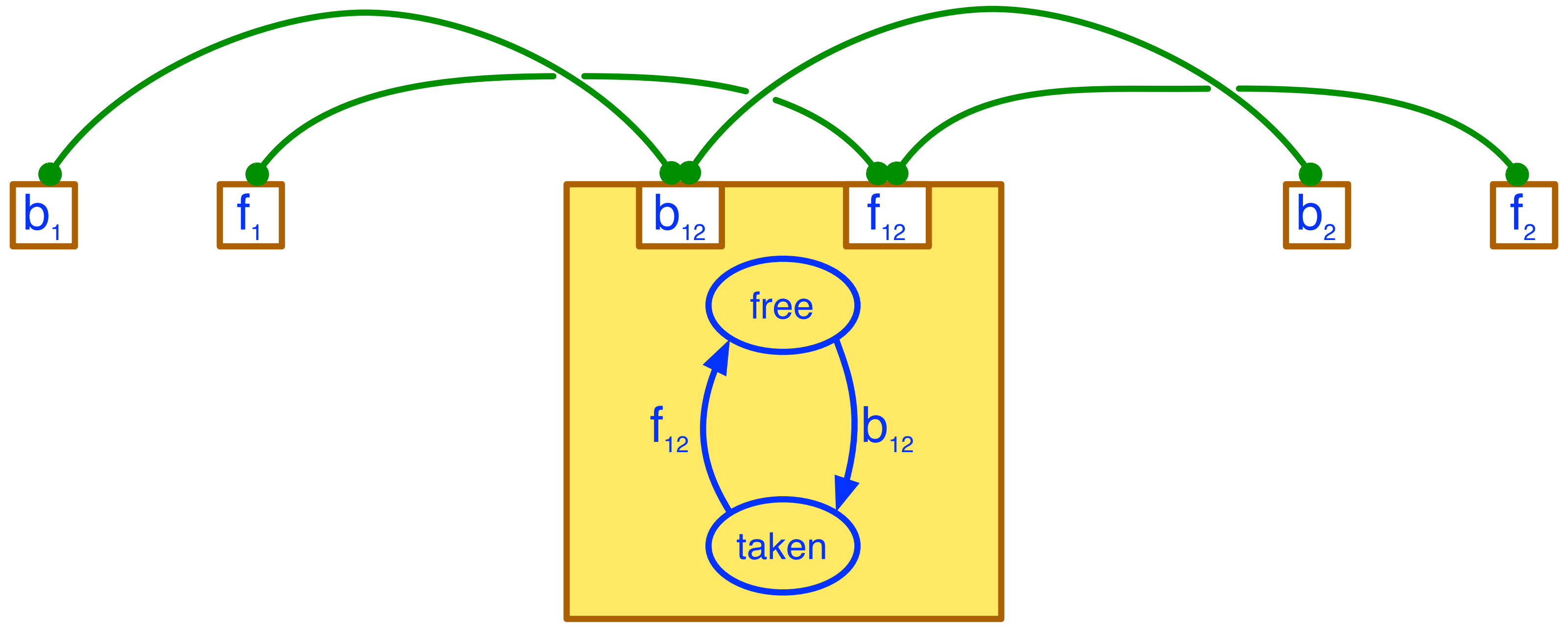
Example continued

$$\varphi_{\gamma_{12}} \equiv (b_1 \Rightarrow b_{12}) \wedge (f_1 \Rightarrow f_{12}) \wedge (b_2 \Rightarrow b_{12}) \wedge (f_2 \Rightarrow f_{12}) \wedge \\ (b_{12} \Rightarrow b_1 \,\texttt{XOR}\, b_2) \wedge (f_{12} \Rightarrow f_1 \,\texttt{XOR}\, f_2) \wedge (b_{12} \Rightarrow \overline{f_{12}})$$

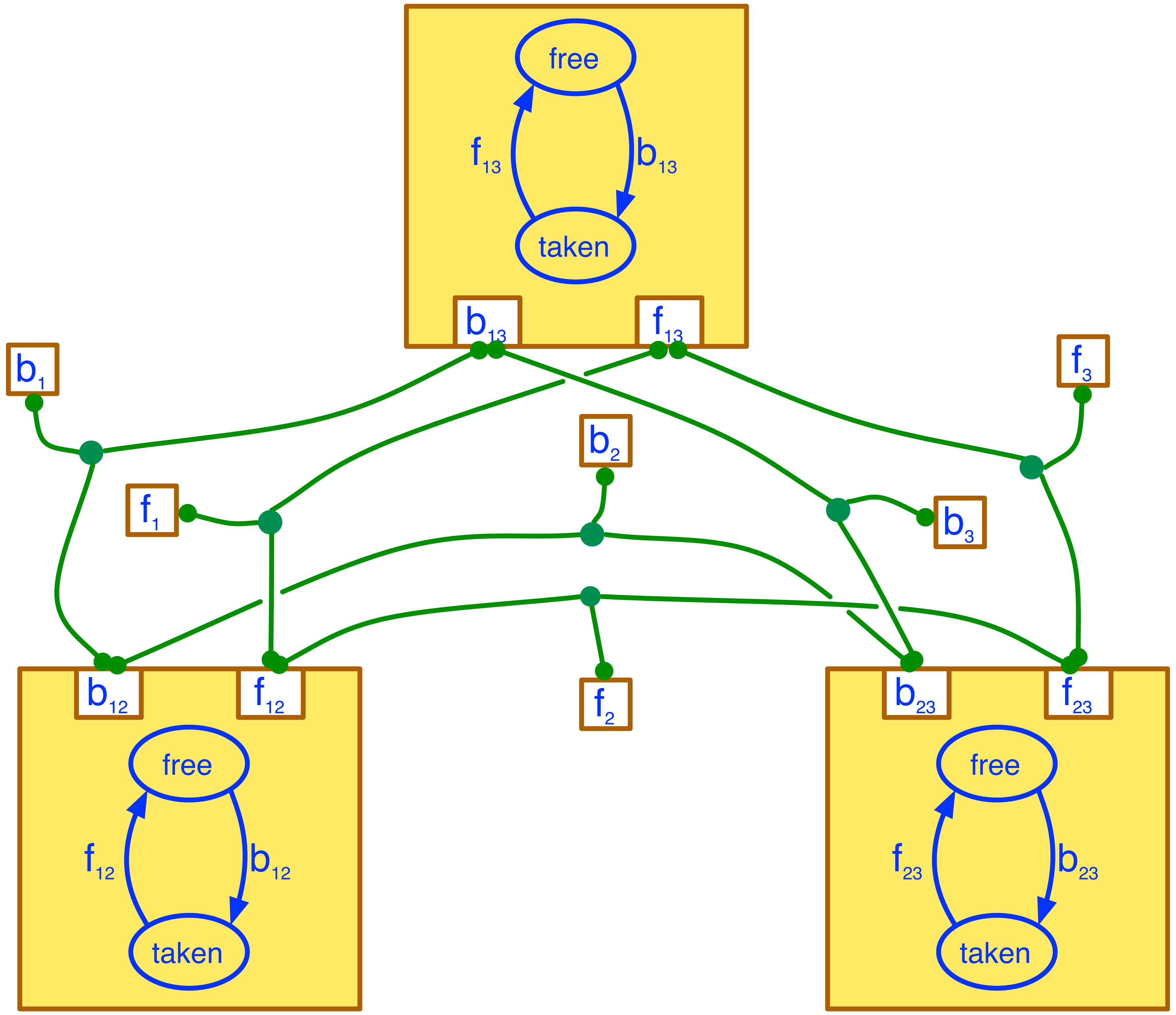
$$\begin{array}{lllll}
b_1 \Rightarrow b_{12} \wedge b_{13}\,, & f_1 \Rightarrow f_{12} \wedge f_{13}\,, & b_{12} \Rightarrow b_1 \,\texttt{XOR}\, b_2\,, & f_{12} \Rightarrow f_1 \,\texttt{XOR}\, f_2\,, & b_{12} \Rightarrow \overline{f_{12}} \\
b_2 \Rightarrow b_{12} \wedge b_{23}\,, & f_2 \Rightarrow f_{12} \wedge f_{23}\,, & b_{13} \Rightarrow b_1 \,\texttt{XOR}\, b_3\,, & f_{13} \Rightarrow f_1 \,\texttt{XOR}\, f_3\,, & b_{13} \Rightarrow \overline{f_{13}} \\
b_3 \Rightarrow b_{13} \wedge b_{23}\,, & f_3 \Rightarrow f_{13} \wedge f_{23}\,, & b_{23} \Rightarrow b_2 \,\texttt{XOR}\, b_3\,, & f_{23} \Rightarrow f_2 \,\texttt{XOR}\, f_3\,, & b_{23} \Rightarrow \overline{f_{23}}
\end{array}$$

$$\{\emptyset\,,\ b_1b_{12}b_{13}\,,\ f_1f_{12}f_{13}\,,\ b_2b_{12}b_{23}\,,\ f_2f_{12}f_{23}\,,\ b_3b_{13}b_{23}\,,\ f_3f_{13}f_{23}\}$$





Example continued



$$\{\emptyset\,,\ b_1b_{12}b_{13}\,,\ f_1f_{12}f_{13}\,,\ b_2b_{12}b_{23}\,,\ f_2f_{12}f_{23}\,,\ b_3b_{13}b_{23}\,,\ f_3f_{13}f_{23}\}$$

Main results: Safety

$$\left.\begin{array}{l} A_1(\mathcal{B}) \models \Phi_1 \\ A_2(\mathcal{B}) \models \Phi_2 \end{array}\right\} \quad \Longrightarrow \quad \big(A_1 \oplus A_2\big)(\mathcal{B}) \models \Phi_1 \wedge \Phi_2$$

Safety = *"Something bad never happens"*

Liveness: Computation

An infinite computation is live iff each coordinator is executed sufficiently often

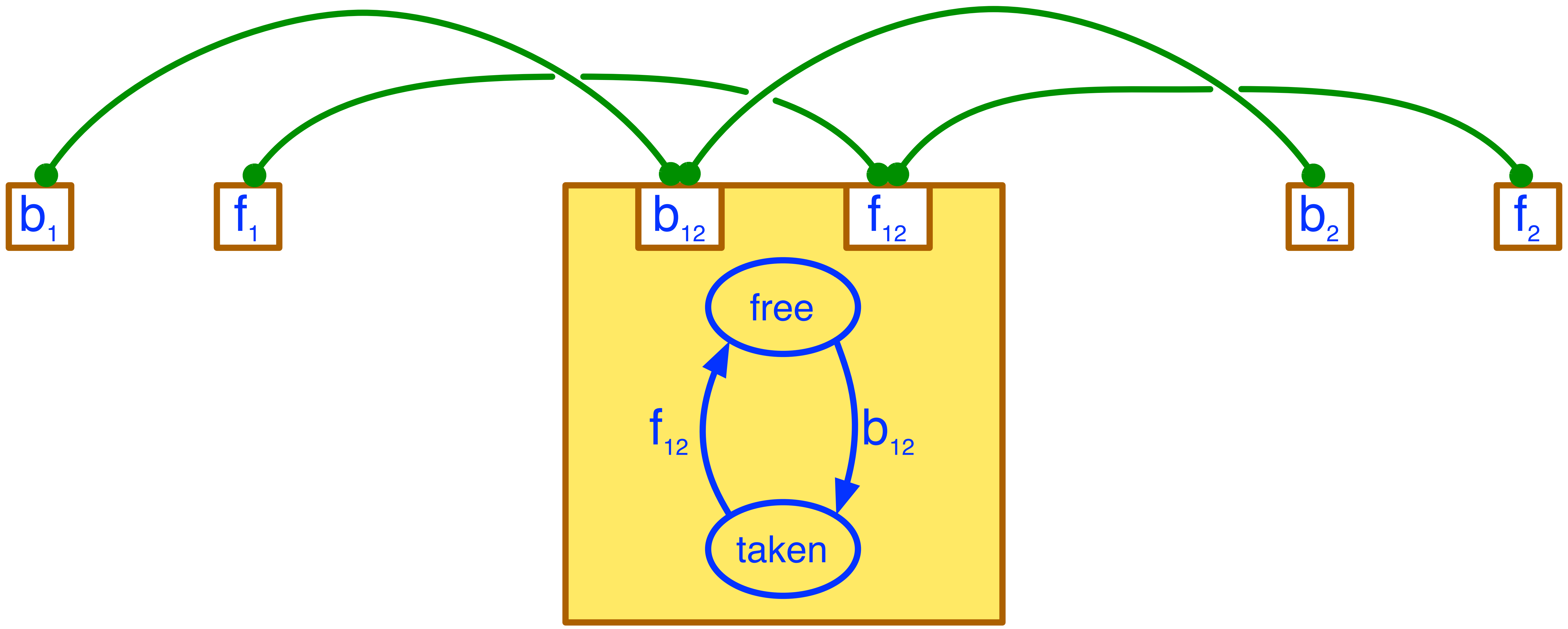
A set of idle states $Q_{idle} \subseteq Q$

Each coordinator not in an idle state must eventually be executed

Intuition: idle states do not have “pending eventuality”

Example (mutex):

$$Q_{idle} = \{\texttt{free}\}$$



Liveness = *"Something good does happen eventually"*

Liveness: Architecture

An architecture is live w.r.t. a set of components iff every computation can be extended to an infinite live one

Non-interference

An architecture can **interfere** with the liveness of another

Examples:

- A_1 repeatedly preempts components that A_2 needs to interact with
- Two architectures “conspire” against a third one

A_1 is non-interfering with A_2 w.r.t. $\mathcal{B}$ iff, for every infinite computation α of $(A_1 \oplus A_2)(\mathcal{B})$,

- α executes C_1 infinitely often => α executes C_2 sufficiently often

Main results: Liveness

$$\underbrace{\left.\begin{array}{r}\mathcal{A} \qquad \text{live} \\ \text{pairwise non-interfering}\end{array}\right\} \implies \bigoplus \mathcal{A} \quad \text{live}}_{\text{w.r.t. } \mathcal{B}}$$

Liveness = *"Something good does happen eventually"*

Architectures as operators

Applying an architecture to a set of behaviours

$$A = (\mathcal{C}, P_A, \gamma) \qquad\qquad P_A \subseteq P \stackrel{def}{=} \bigcup_{B \in \mathcal{B} \cup \mathcal{C}} P_B$$

$$A(\mathcal{B}) \stackrel{def}{=} \Big(\gamma \ltimes P\Big)(\mathcal{B} \cup \mathcal{C})$$

Architectures as operators

Applying an architecture to a set of behaviours

$$A = (\mathcal{C}, P_A, \gamma) \qquad P_A \subseteq P \stackrel{def}{=} \bigcup_{B \in \mathcal{B} \cup \mathcal{C}} P_B$$

$$A(\mathcal{B}) \stackrel{def}{=} \Big(\gamma \ltimes P\Big)(\mathcal{B} \cup \mathcal{C})$$

Partial application is a new architecture

$$A[\mathcal{B}] \stackrel{def}{=} \big(B', P \cup P_A, \gamma \ltimes (P \cup P_A)\big)$$

$$B' \stackrel{def}{=} \Big(\gamma_P \ltimes (P \cup P_A)\Big)(\mathcal{B} \cup \mathcal{C}) \quad \gamma_P = \{a \cap P \,|\, a \in \gamma\}$$

Nice properties

Under suitable conditions

Architectures can be composed before applying

$$A_2(A_1(\mathcal{B})) = (A_1 \oplus A_2)(\mathcal{B})$$

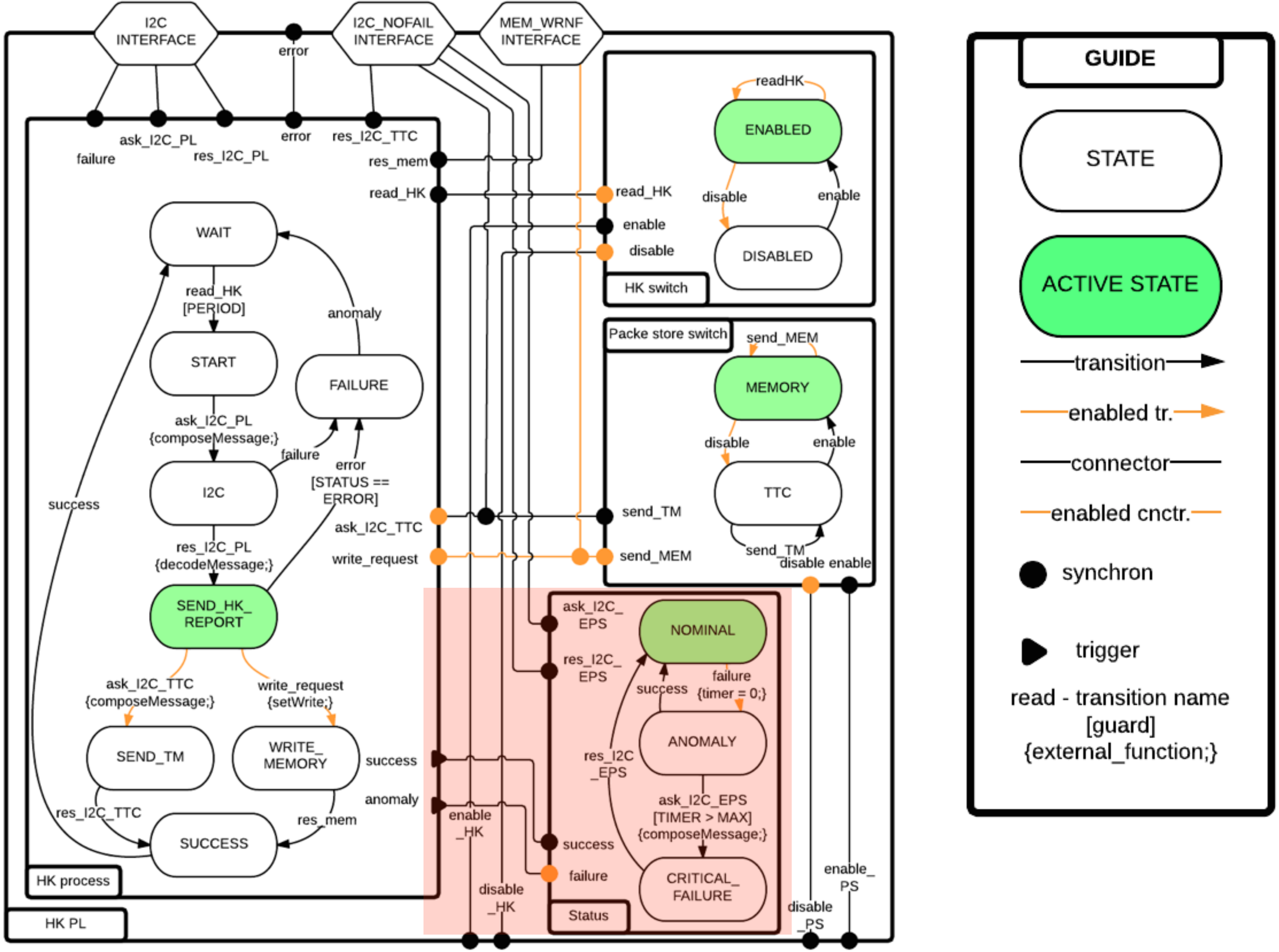
Architecture application can be restricted

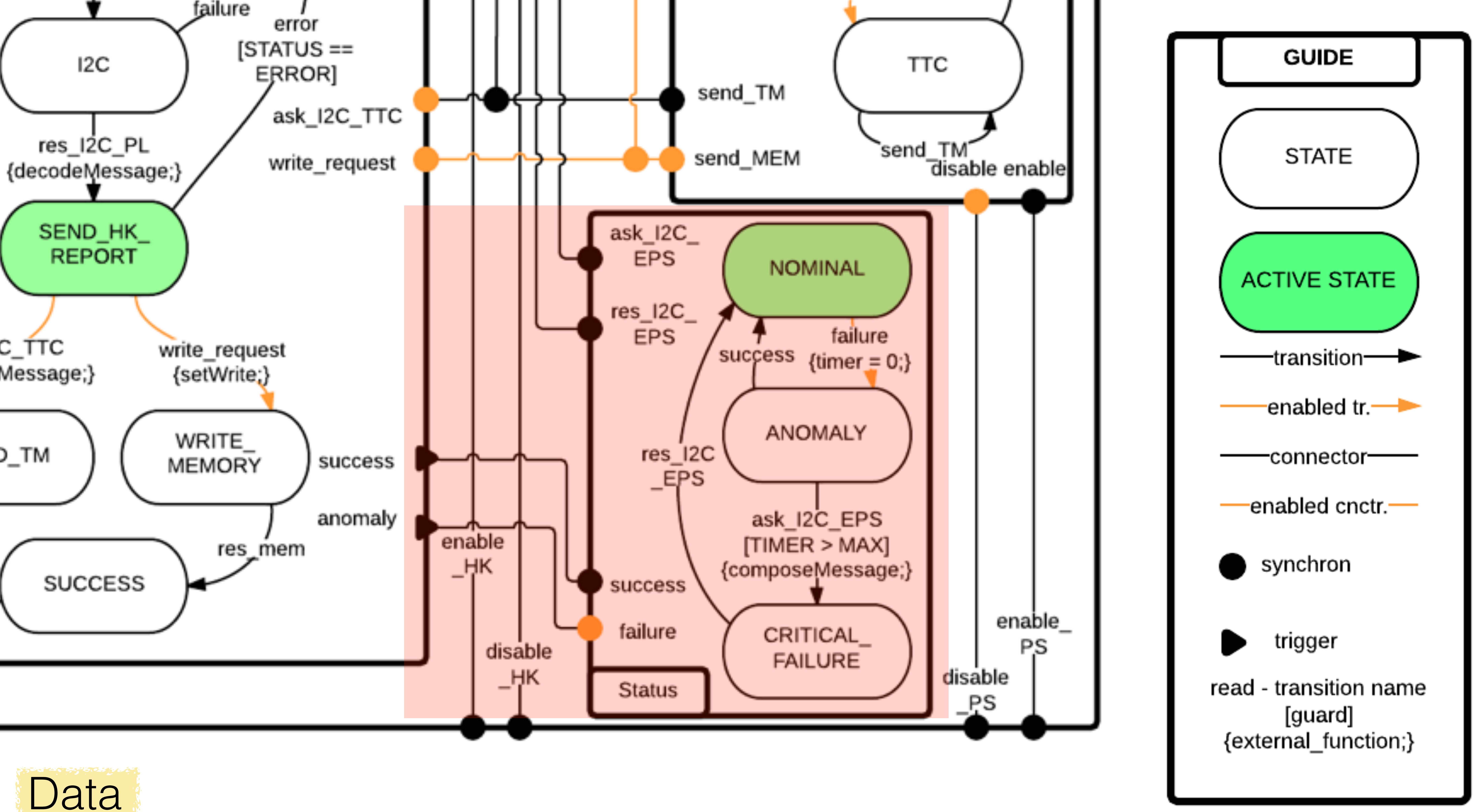
$$A_2(A_1(\mathcal{B}_1, \mathcal{B}_2)) = A_2(A_1(\mathcal{B}_1), \mathcal{B}_2)$$

Architecture can be applied partially

$$A(\mathcal{B}_1, \mathcal{B}_2) = A[\mathcal{B}_1](\mathcal{B}_2)$$

Will that still work with data?


I2C INTERFACE
I2C_NOFAIL INTERFACE
MEM_WRNF INTERFACE
error
failure
ask_I2C_PL
res_I2C_PL
error
res_I2C_TTC
res_mem
read_HK
WAIT
read_HK [PERIOD]
anomaly
START
FAILURE
ask_I2C_PL {composeMessage;}
failure
error [STATUS == ERROR]
I2C
success
ask_I2C_TTC
res_I2C_PL {decodeMessage;}
write_request
SEND_HK_ REPORT
ask_I2C_TTC {composeMessage;}
write_request {setWrite;}
SEND_TM
WRITE_ MEMORY
success
anomaly
res_I2C_TTC
res_mem
SUCCESS
HK process
HK PL
readHK
ENABLED
read_HK
disable
enable
enable
disable
DISABLED
HK switch
Packe store switch
send_MEM
MEMORY
disable
enable
TTC
send_TM
send_MEM
send_TM
disable enable
ask_I2C_ EPS
NOMINAL
res_I2C_ EPS
failure {timer = 0;}
success
ANOMALY
res_I2C _EPS
ask_I2C_EPS [TIMER > MAX] {composeMessage;}
enable _HK
success
failure
CRITICAL_ FAILURE
disable _HK
Status
enable_ PS
disable _PS
GUIDE
STATE
ACTIVE STATE
transition
enabled tr.
connector
enabled cnctr.
synchron
trigger
read - transition name
[guard]
{external_function;}



Data

Maximal progress

Composing controllers with data

Between 20^o and 25^o

Between 18^o and 23^o

$$[20^o, 25^o] \cap [18^o, 23^o] = [20^o, 23^o]$$

Somewhat stronger safety

$$\big((q, \sigma) \models \Phi\big) \wedge (\sigma' \leqslant \sigma) \implies (q, \sigma') \models \Phi$$

Safety

$$\left.\begin{array}{l} A_1(\mathcal{B}) \models \Phi_1 \\ A_2(\mathcal{B}) \models \Phi_2 \end{array}\right\} \quad \Longrightarrow \quad \big(A_1 \oplus A_2\big)(\mathcal{B}) \models \Phi_1 \wedge \Phi_2$$

is preserved by composition of architectures

with **data**

with **maximal progress**

(* technical constraints apply)

Generalised safety

Lemma

$$ss_1s_2 \xrightarrow{a,\sigma} s's_1's_2' \implies ss_1 \xrightarrow{a\cap P_1,\tilde{\sigma}} s''s_1' \text{ with } s' \leqslant s''$$

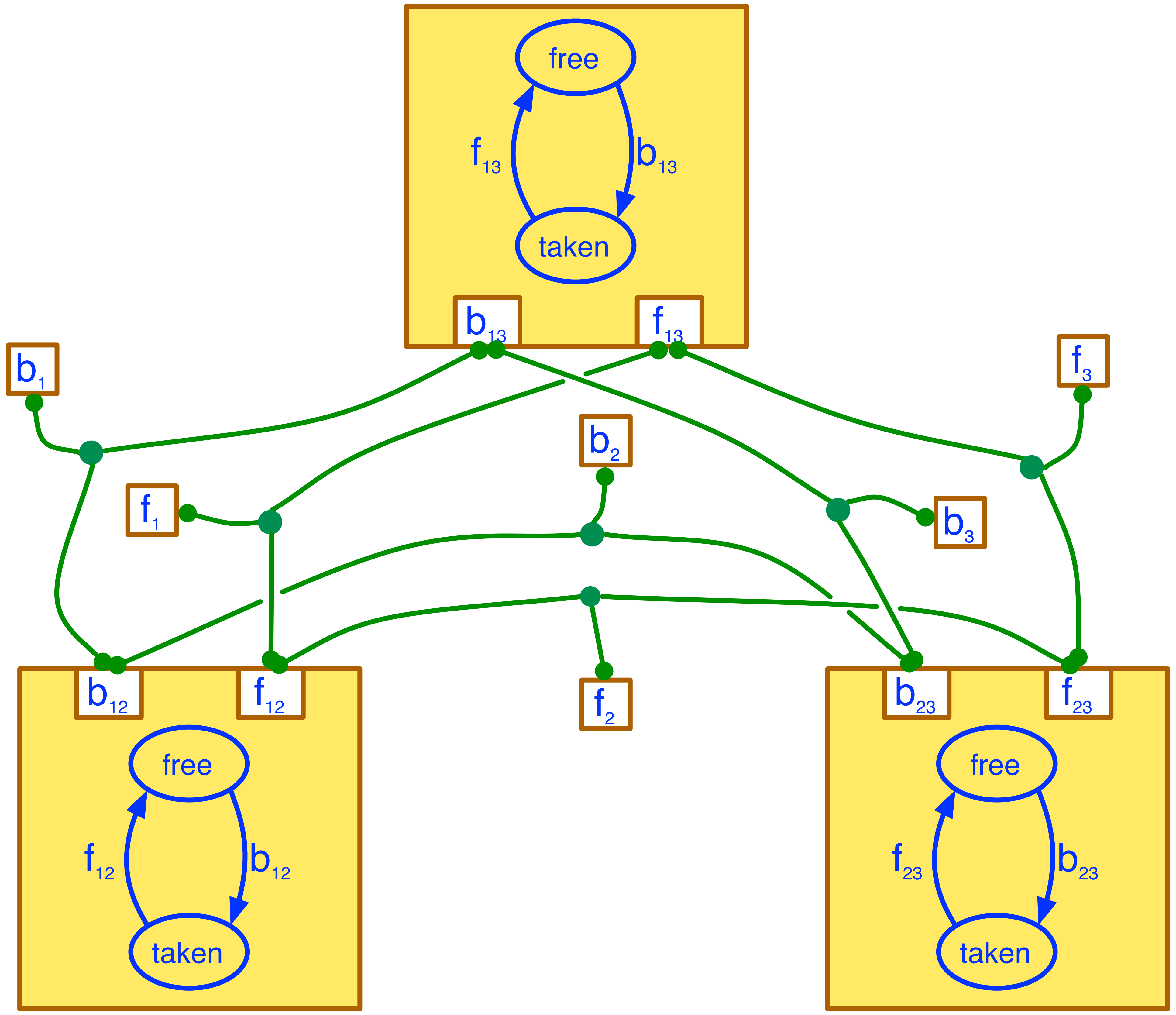
Lemma

$$s \xrightarrow{a,\sigma} s' \wedge s \leqslant \tilde{s} \implies \tilde{s} \xrightarrow{a,\sigma} s'$$

Key assumption: monotonic guards and update expressions

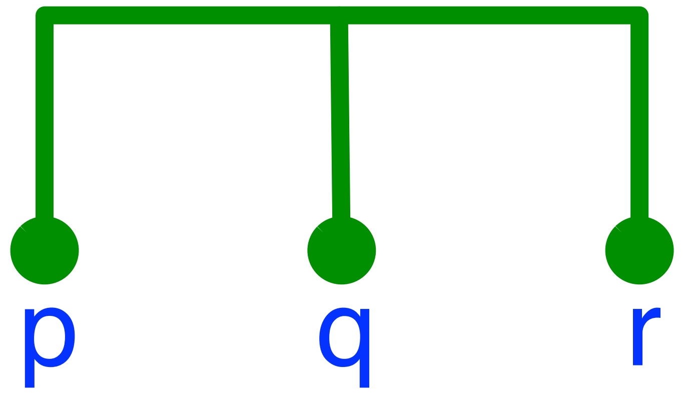
Wait, what about connectors?

MUX composition example



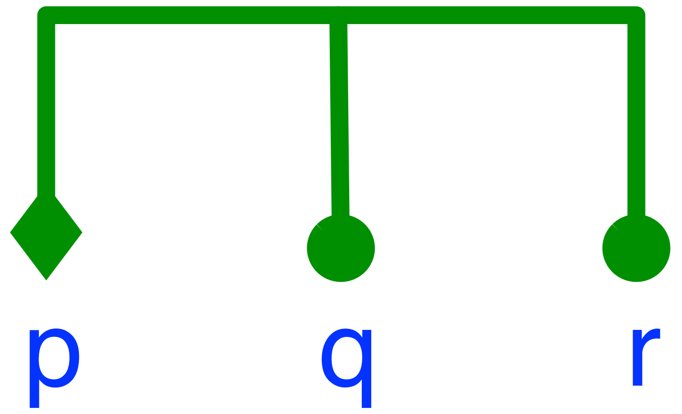
$$\{\emptyset\,,\ b_1b_{12}b_{13}\,,\ f_1f_{12}f_{13}\,,\ b_2b_{12}b_{23}\,,\ f_2f_{12}f_{23}\,,\ b_3b_{13}b_{23}\,,\ f_3f_{13}f_{23}\}$$

Causal interaction trees: Basic examples

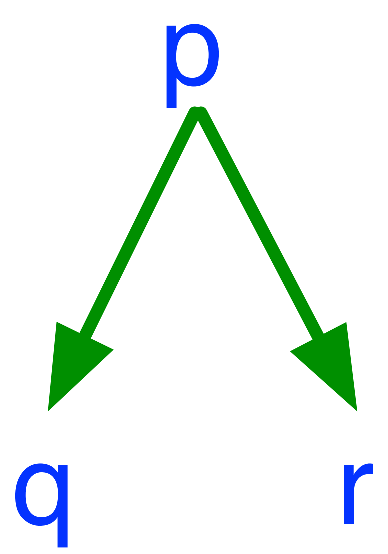


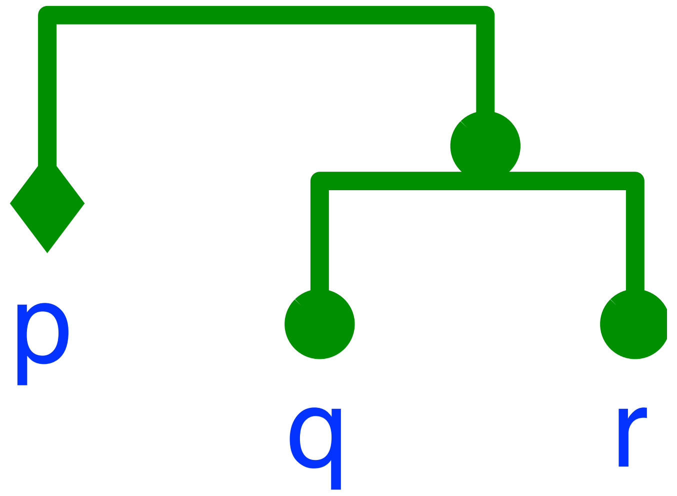
Strong synchronisation
pqr

p q r

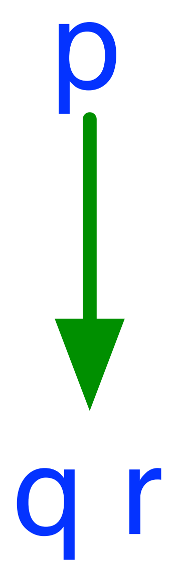


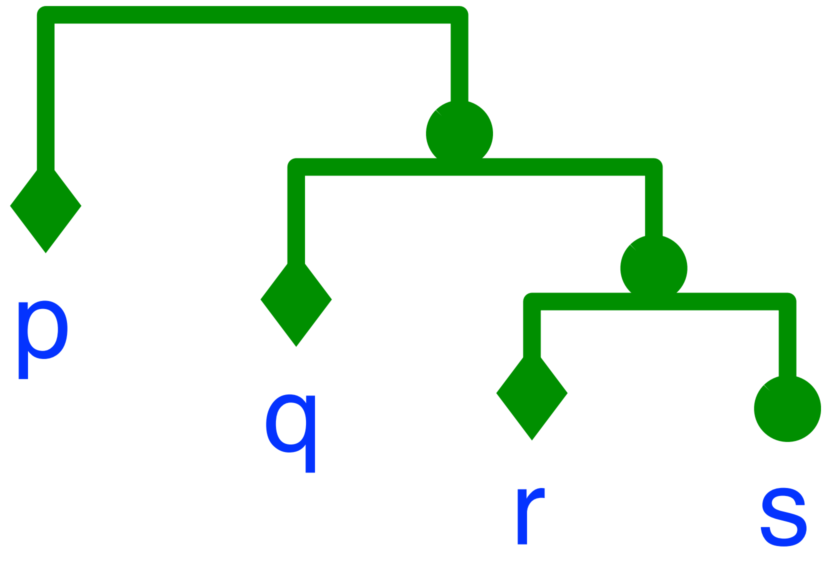
Broadcast
p’qr



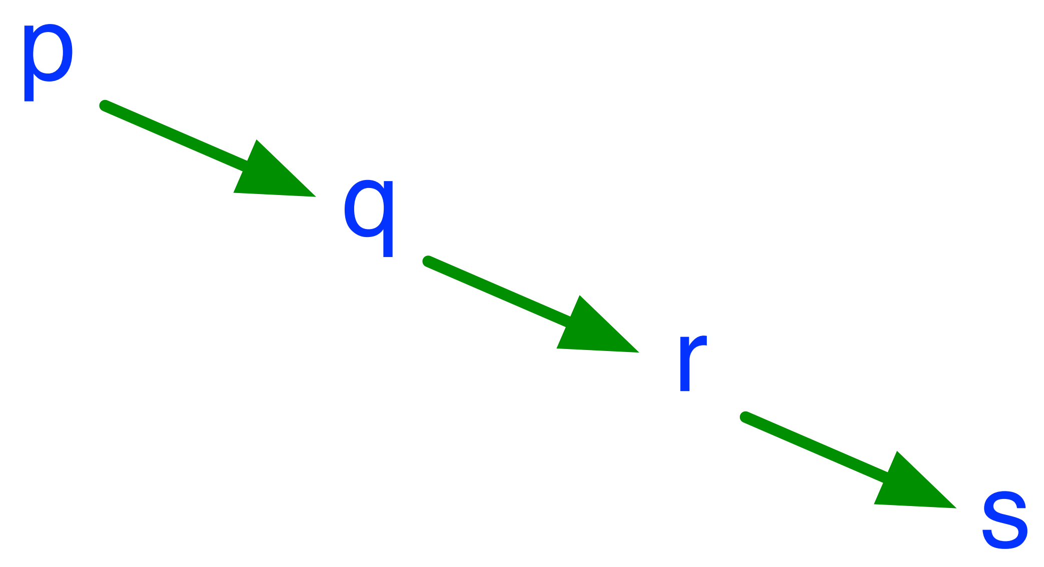


Atomic broadcast
p’[qr]

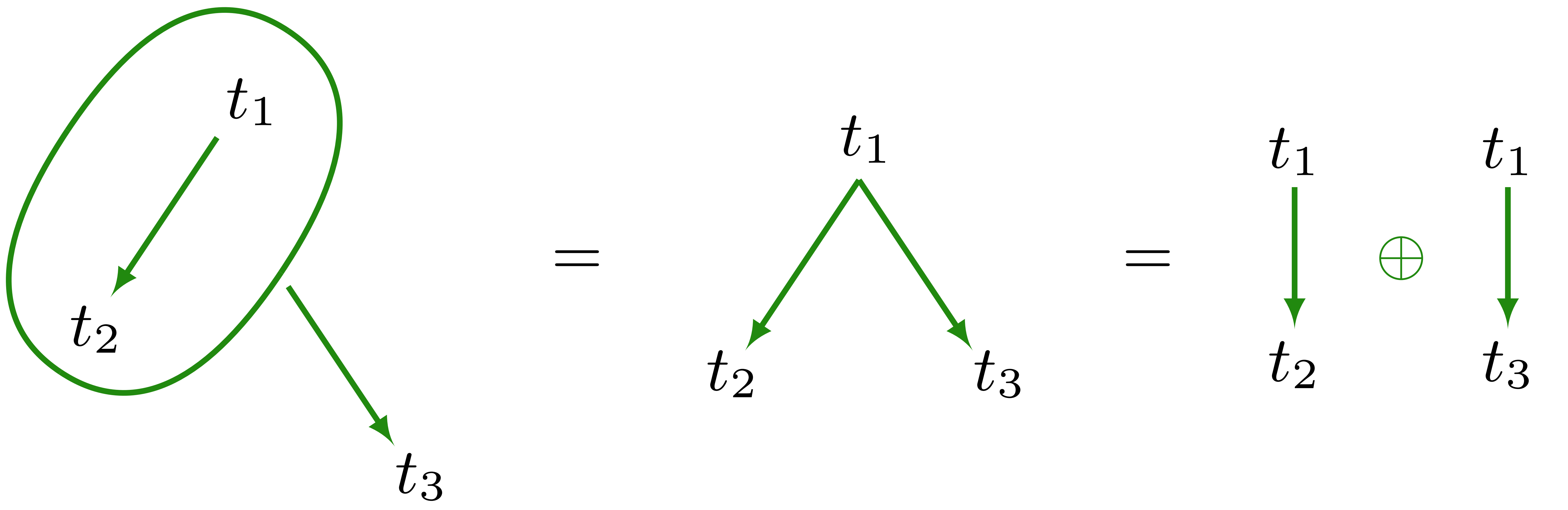




Causal chain
p’[q’[r’s]]



Causal interaction trees: The algebra



Syntax: $t ::= a \mid t \to t \mid t \oplus t$

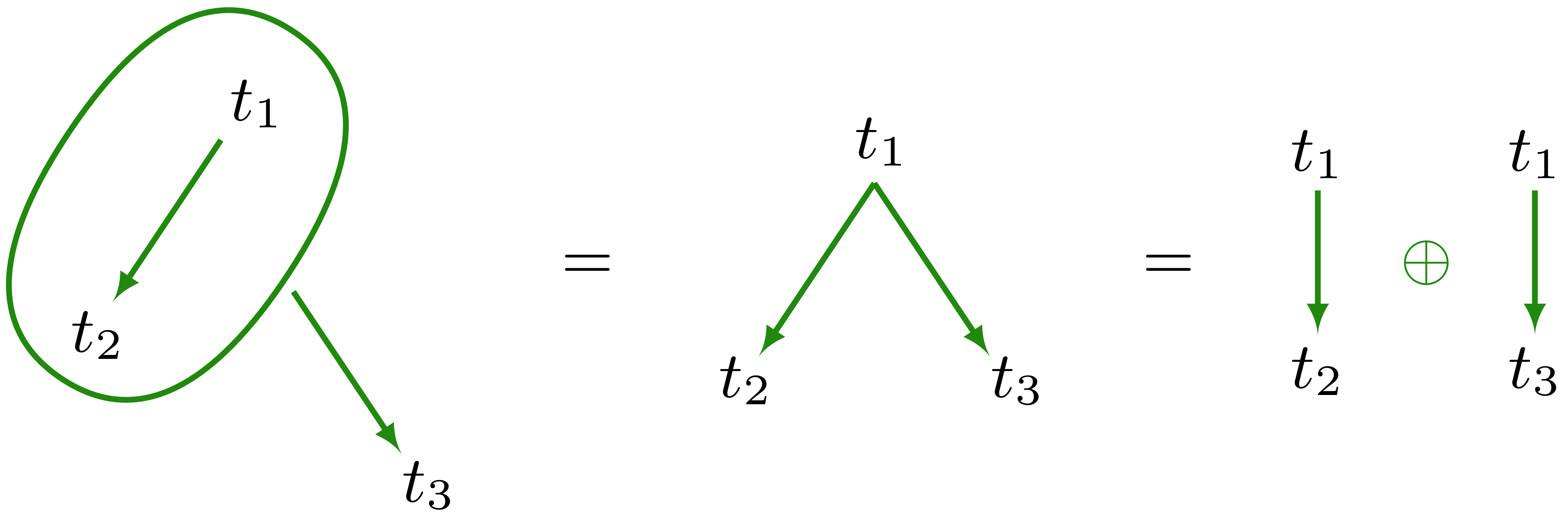
Essential axioms:

$$(t_1 \to t_2) \to t_3 = t_1 \to (t_2 \oplus t_3),$$
$$t_1 \to (t_2 \oplus t_3) = t_1 \to t_2 \;\oplus\; t_1 \to t_3,$$
$$(t_1 \oplus t_2) \to t_3 = t_1 \to t_3 \;\oplus\; t_2 \to t_3.$$

Semantics:

$$|a| = a\,,$$
$$|a \to t| = a\Big(1 + |t|\Big)\,,$$
$$|t_1 \oplus t_2| = |t_1| + |t_2| + |t_1||t_2|\,.$$

Causal interaction trees: The algebra



Syntax: $t ::= a \mid t \rightarrow t \mid t \oplus t$

Essential axioms:

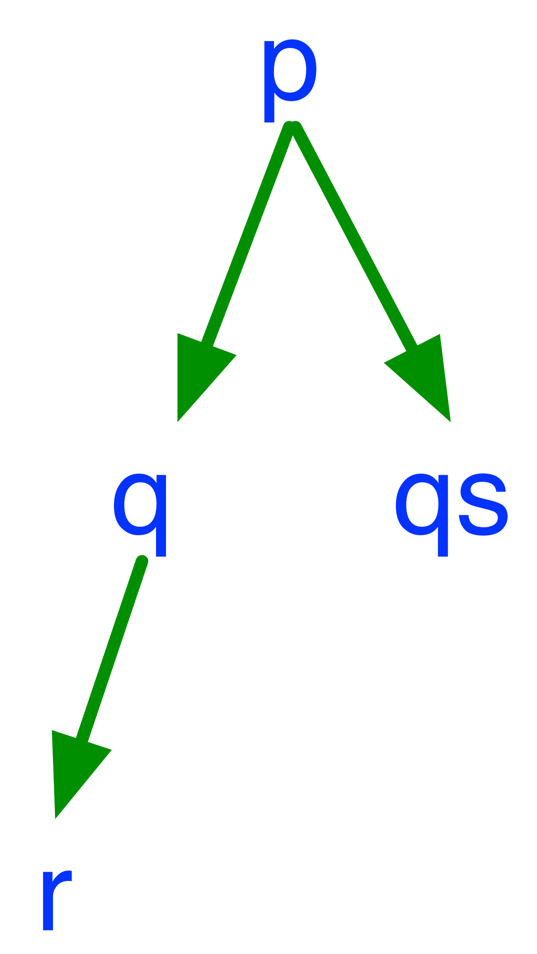
$$(t_1 \rightarrow t_2) \rightarrow t_3 = t_1 \rightarrow (t_2 \oplus t_3),$$
$$t_1 \rightarrow (t_2 \oplus t_3) = t_1 \rightarrow t_2 \;\oplus\; t_1 \rightarrow t_3,$$
$$(t_1 \oplus t_2) \rightarrow t_3 = t_1 \rightarrow t_3 \;\oplus\; t_2 \rightarrow t_3.$$

Semantics:

$$|a| = a\,,$$
$$|a \rightarrow t| = a\Big(1 + |t|\Big)\,,$$
$$|t_1 \oplus t_2| = |t_1| + |t_2| + |t_1||t_2|\,.$$

Transformations between *AC(P)* and *CT(P)* are straightforward.

Boolean representation of connectors



Causal interaction trees

$$
\begin{aligned}
true &\Rightarrow p\,, \\
p &\Rightarrow true\,, \\
q &\Rightarrow p\,, \\
r &\Rightarrow pq\,, \\
s &\Rightarrow pq
\end{aligned}
$$

Causal rules

Notice that: $(q \Rightarrow p \vee ps) \equiv (q \Rightarrow p)\,.$

Boolean formula corresponding to the connector:

$$(true \Rightarrow p) \wedge (q \Rightarrow p) \wedge (r \Rightarrow p\,q) \wedge (s \Rightarrow p\,q)$$

Connector synthesis (1/2)

$$\begin{aligned}
true &\Rightarrow p\,,\\
p &\Rightarrow true\,,\\
q &\Rightarrow p\,,\\
r &\Rightarrow q\,,\\
s &\Rightarrow q\,,\\
t &\Rightarrow r + s
\end{aligned}$$

Connector synthesis (1/2)

$$
\begin{aligned}
true &\Rightarrow p\,,\\
p &\Rightarrow true\,,\\
q &\Rightarrow p\,,\\
r &\Rightarrow q\,,\\
s &\Rightarrow q\,,\\
t &\Rightarrow r + s
\end{aligned}
$$

Connector synthesis (1/2)

$$\begin{aligned}
true &\Rightarrow p\,, \\
p &\Rightarrow true\,, \\
q &\Rightarrow p\,, \\
r &\Rightarrow q\,, \\
s &\Rightarrow q\,, \\
t &\Rightarrow r + s
\end{aligned}$$

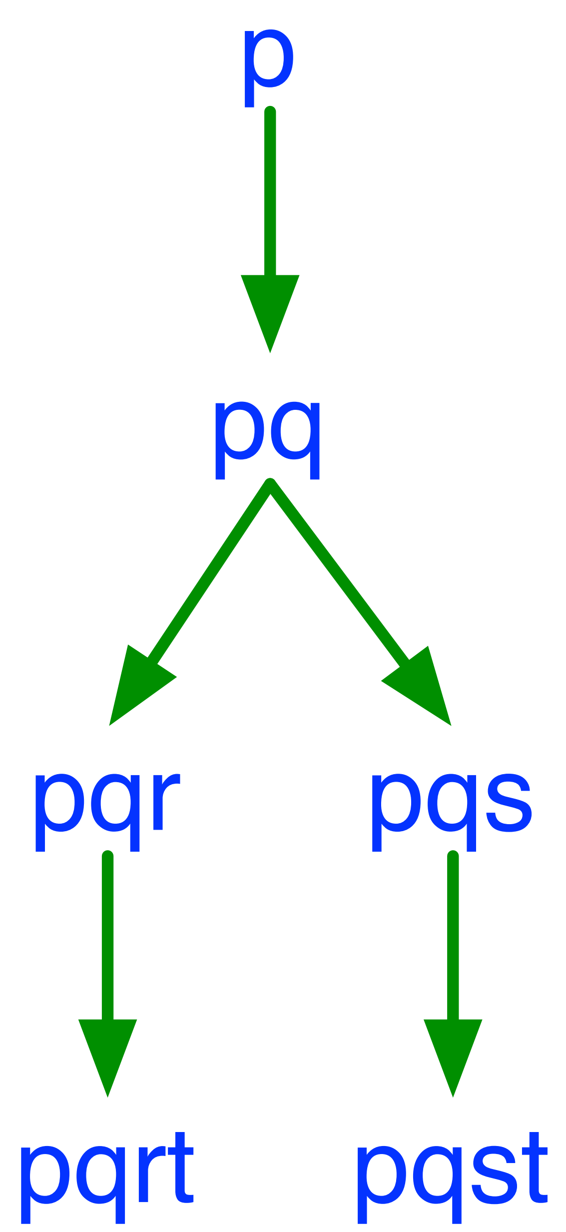
$$\begin{aligned}
true &\Rightarrow p\,, \\
p &\Rightarrow true\,, \\
q &\Rightarrow p\,, \\
r &\Rightarrow pq\,, \\
s &\Rightarrow pq\,, \\
t &\Rightarrow pqr + pqs
\end{aligned}$$

Connector synthesis (1/2)

$$
\begin{aligned}
true &\Rightarrow p\,, \\
p &\Rightarrow true\,, \\
q &\Rightarrow p\,, \\
r &\Rightarrow q\,, \\
s &\Rightarrow q\,, \\
t &\Rightarrow r + s
\end{aligned}
\qquad\qquad
\begin{aligned}
true &\Rightarrow p\,, \\
p &\Rightarrow true\,, \\
q &\Rightarrow p\,, \\
r &\Rightarrow pq\,, \\
s &\Rightarrow pq\,, \\
t &\Rightarrow pqr + pqs
\end{aligned}
\qquad\qquad
\begin{aligned}
&p \\
&p \\
&pq \\
&pqr \\
&pqs \\
&pqrt, pqst
\end{aligned}
$$

Connector synthesis (1/2)

$$
\begin{aligned}
true &\Rightarrow p\,,\\
p &\Rightarrow true\,,\\
q &\Rightarrow p\,,\\
r &\Rightarrow q\,,\\
s &\Rightarrow q\,,\\
t &\Rightarrow r + s
\end{aligned}
$$



$$
\begin{aligned}
true &\Rightarrow p\,,\\
p &\Rightarrow true\,,\\
q &\Rightarrow p\,,\\
r &\Rightarrow pq\,,\\
s &\Rightarrow pq\,,\\
t &\Rightarrow pqr + pqs
\end{aligned}
$$

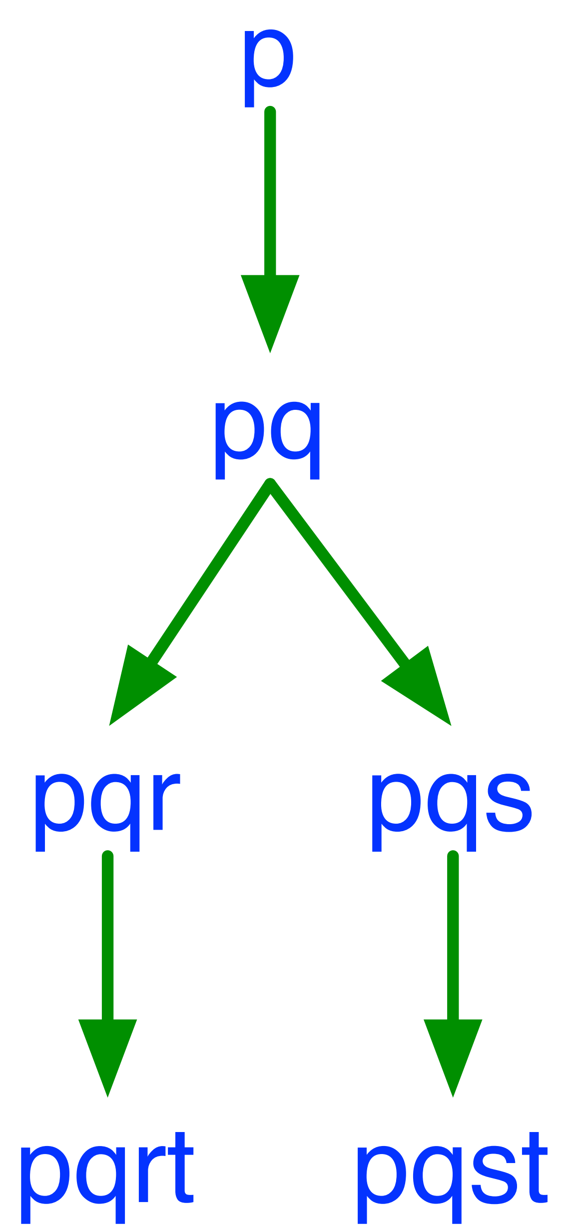
$$
\begin{array}{l}
p\\
p\\
pq\\
pqr\\
pqs\\
pqrt, pqst
\end{array}
$$

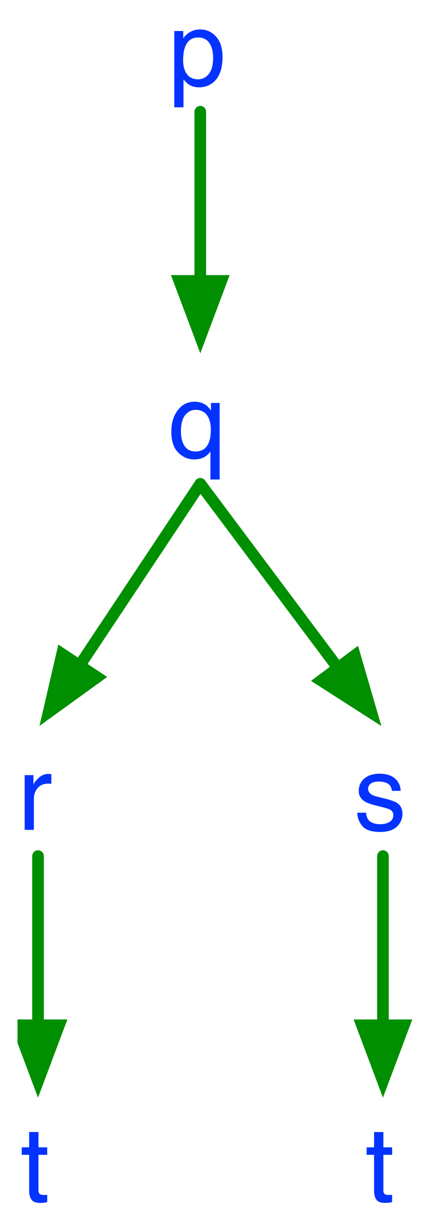
Connector synthesis (1/2)

$$\begin{aligned} true &\Rightarrow p\,, \\ p &\Rightarrow true\,, \\ q &\Rightarrow p\,, \\ r &\Rightarrow q\,, \\ s &\Rightarrow q\,, \\ t &\Rightarrow r + s \end{aligned}$$

$$\begin{aligned} true &\Rightarrow p\,, \\ p &\Rightarrow true\,, \\ q &\Rightarrow p\,, \\ r &\Rightarrow pq\,, \\ s &\Rightarrow pq\,, \\ t &\Rightarrow pqr + pqs \end{aligned}$$

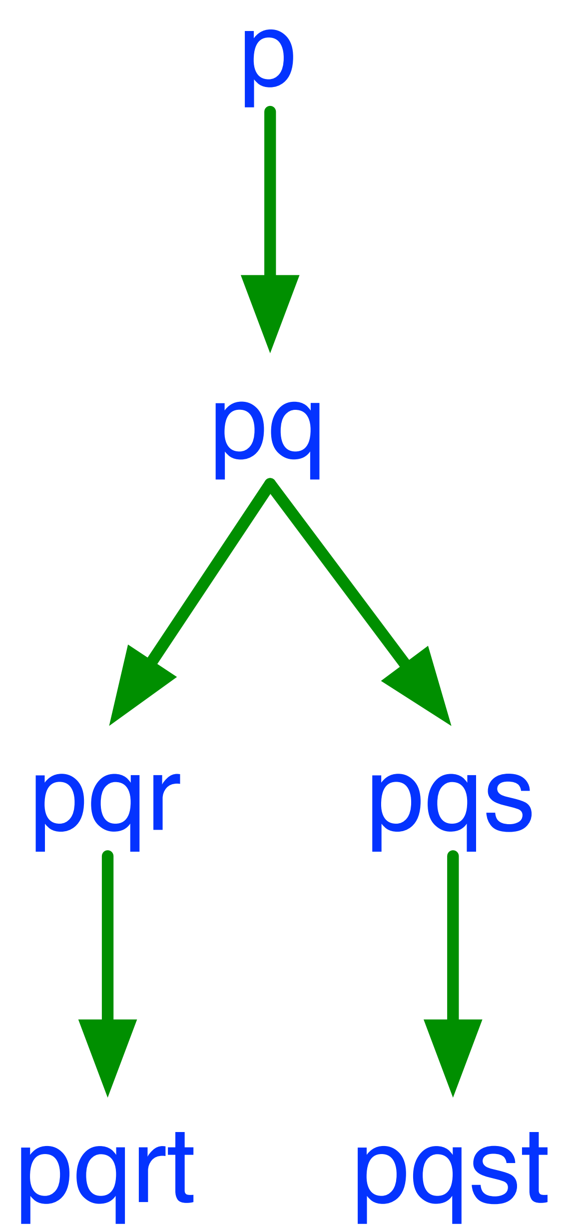
$$\begin{array}{l} p \\ p \\ pq \\ pqr \\ pqs \\ pqrt, pqst \end{array}$$



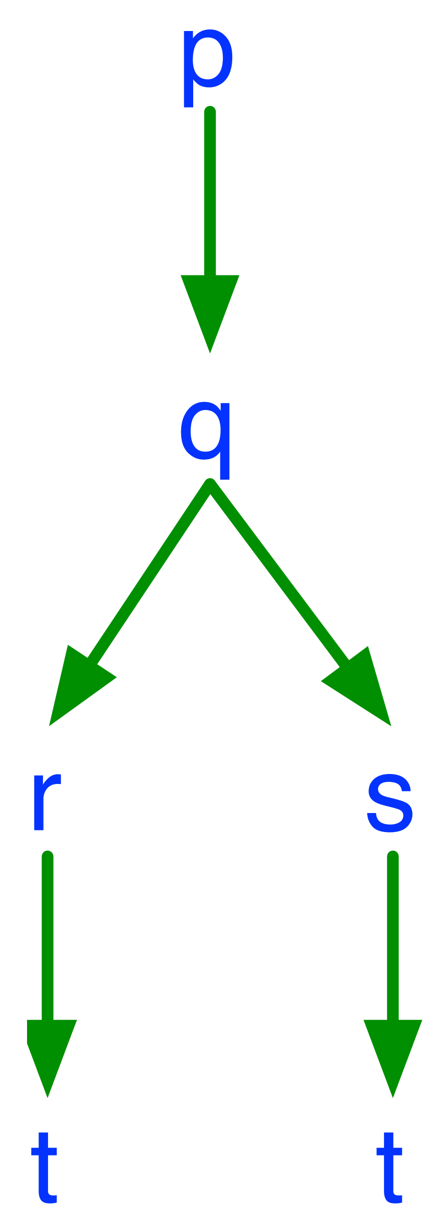


Connector synthesis (1/2)

$$
\begin{aligned}
true &\Rightarrow p\,,\\
p &\Rightarrow true\,,\\
q &\Rightarrow p\,,\\
r &\Rightarrow q\,,\\
s &\Rightarrow q\,,\\
t &\Rightarrow r + s
\end{aligned}
\qquad\qquad
\begin{aligned}
true &\Rightarrow p\,,\\
p &\Rightarrow true\,,\\
q &\Rightarrow p\,,\\
r &\Rightarrow pq\,,\\
s &\Rightarrow pq\,,\\
t &\Rightarrow pqr + pqs
\end{aligned}
\qquad\qquad
\begin{aligned}
&p\\
&p\\
&pq\\
&pqr\\
&pqs\\
&pqrt, pqst
\end{aligned}
$$



$$p'\Big[q'[r't][s't]\Big]$$



Connector synthesis (2/2)

Consider a CNF formula $\varphi = C_1 \wedge C_2 \wedge \cdots \wedge C_n \in \mathbb{B}[P]$

$$C_k = \bigvee_{i \in I_k} p_i \vee \bigvee_{j \in J_k} \overline{p_j} = \bigvee_{j \in J_k} \left(\overline{p_j} \vee \bigvee_{i \in I_k} p_i \right) .$$

(disjunction of dual-Horn clauses)

Connector synthesis (2/2)

Consider a CNF formula $\varphi = C_1 \wedge C_2 \wedge \cdots \wedge C_n \in \mathbb{B}[P]$

$$C_k = \bigvee_{i \in I_k} p_i \vee \bigvee_{j \in J_k} \overline{p_j} = \bigvee_{j \in J_k} \left(\overline{p_j} \vee \bigvee_{i \in I_k} p_i \right) .$$

(disjunction of dual-Horn clauses)

By distributivity, after combining the clauses with the same negative variable,

$$\varphi = R_1 \vee R_2 \vee \cdots \vee R_m$$

$$R_k = \bigwedge_{j \in \tilde{J}_k} \left(\overline{p_j} \vee \bigvee_{i \in \tilde{I}_{k,j}} a_i \right) = \bigwedge_{j \in \tilde{J}_k} \left(p_j \Rightarrow \bigvee_{i \in \tilde{I}_{k,j}} a_i \right) .$$

Connector synthesis (2/2)

Consider a CNF formula $\varphi = C_1 \wedge C_2 \wedge \cdots \wedge C_n \in \mathbb{B}[P]$

$$C_k = \bigvee_{i \in I_k} p_i \vee \bigvee_{j \in J_k} \overline{p_j} = \bigvee_{j \in J_k} \left(\overline{p_j} \vee \bigvee_{i \in I_k} p_i \right) .$$

(disjunction of dual-Horn clauses)

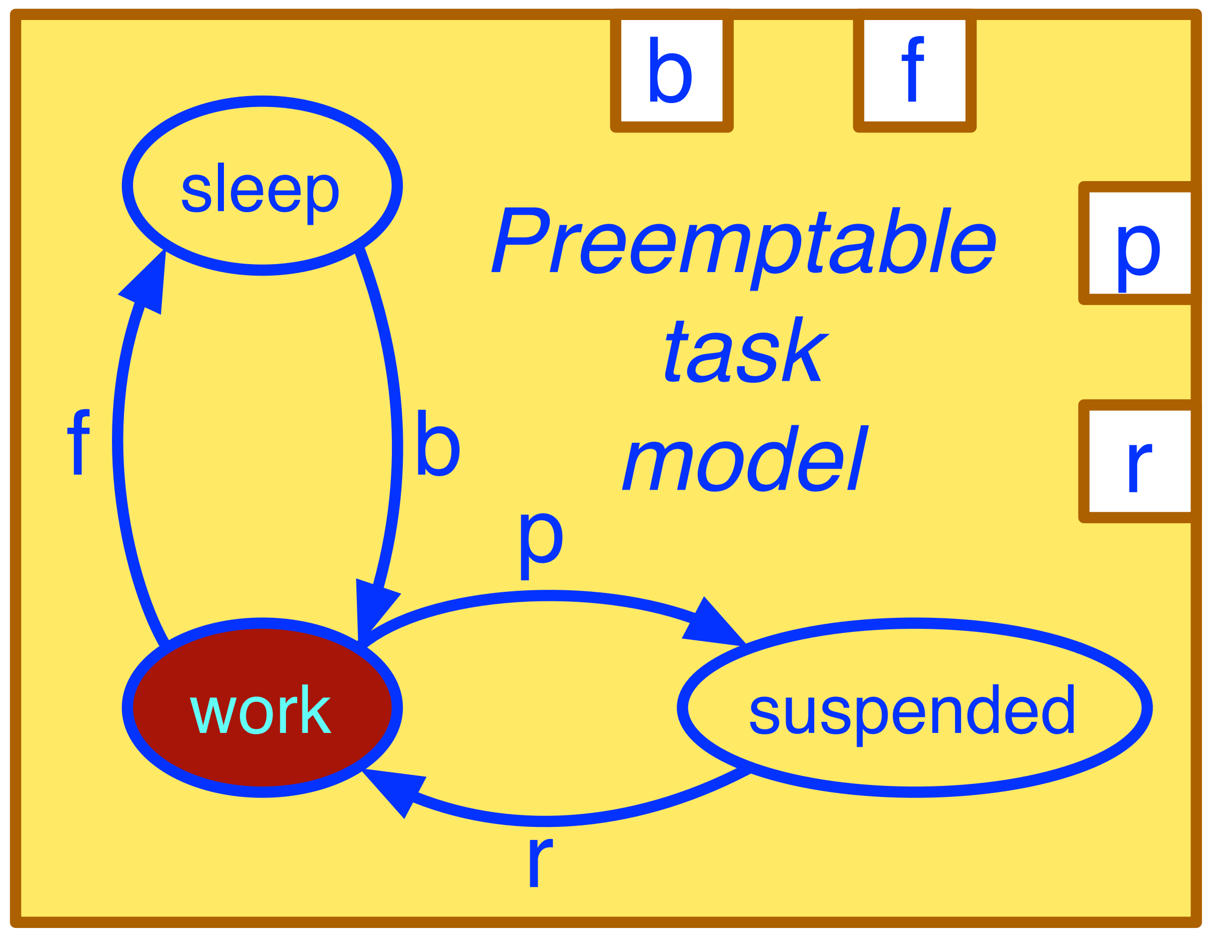
By distributivity, after combining the clauses with the same negative variable,

$$\varphi = R_1 \vee R_2 \vee \cdots \vee R_m$$

$$R_k = \bigwedge_{j \in \tilde{J}_k} \left(\overline{p_j} \vee \bigvee_{i \in \tilde{I}_{k,j}} a_i \right) = \bigwedge_{j \in \tilde{J}_k} \left(p_j \Rightarrow \bigvee_{i \in \tilde{I}_{k,j}} a_i \right) .$$

Each R_k is a system of causal rules.

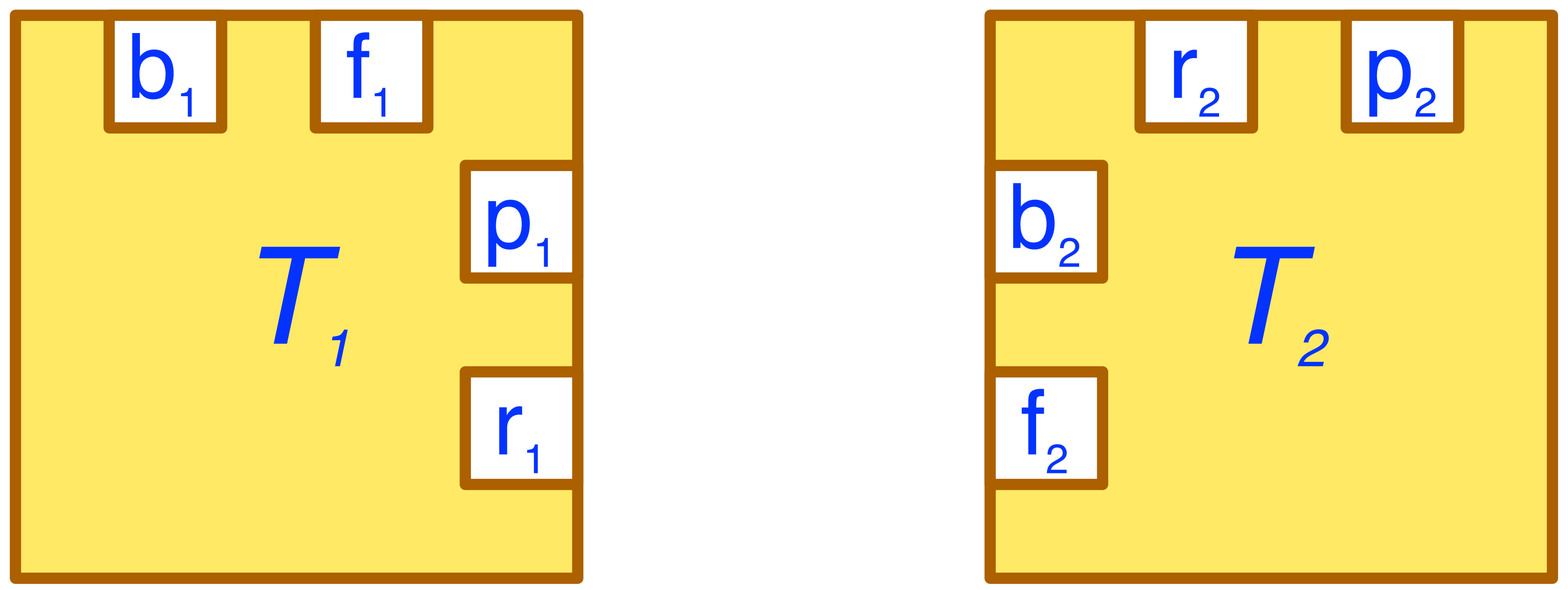
Example: 2 tasks with preemption



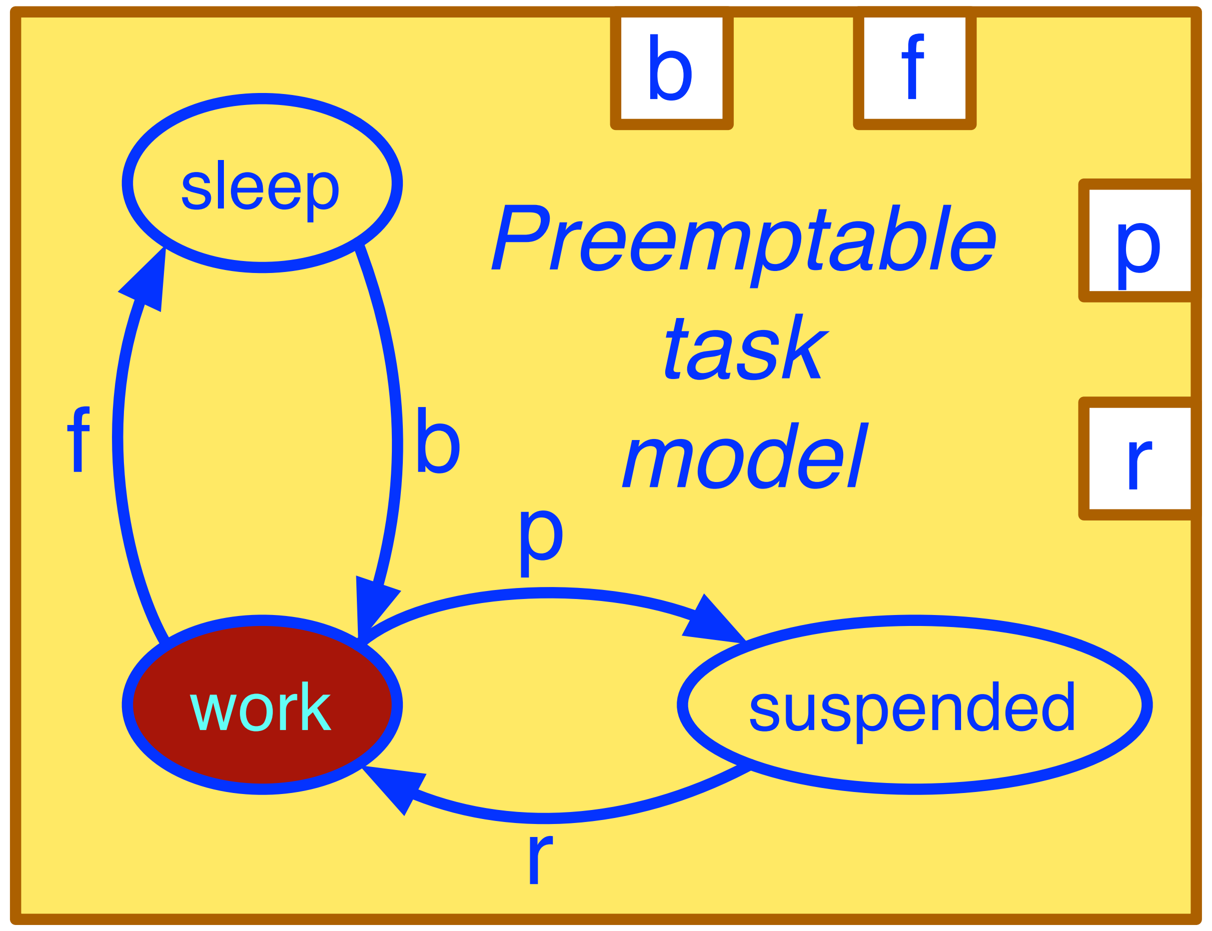
Mutual preemption

A running task is preemtped, when the other begins computation.

A preempted task resumes computation, when the other one finishes.



Example: 2 tasks with preemption



Mutual preemption

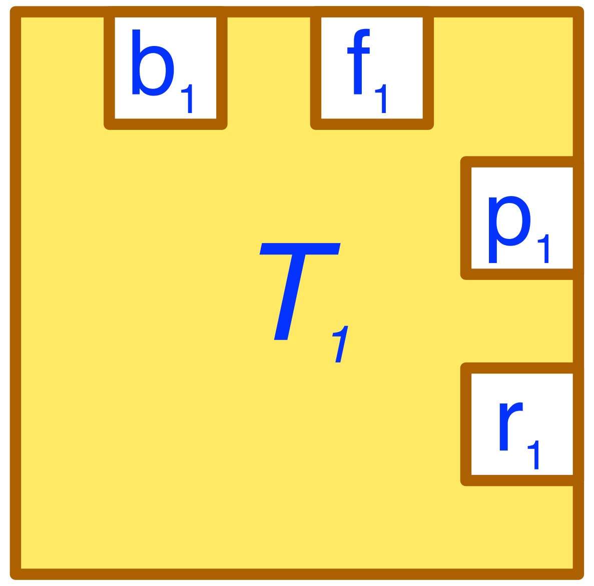
A running task is preemtped, when the other begins computation.

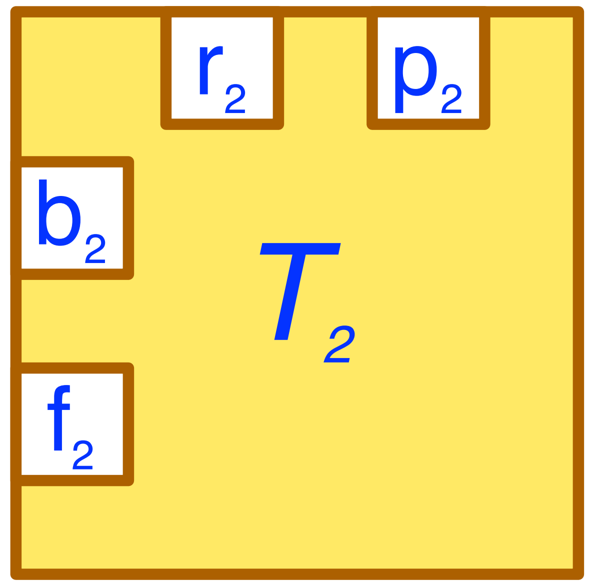
A preempted task resumes computation, when the other one finishes.

$$true \Rightarrow b_1 \vee f_1 \vee b_2 \vee f_2$$

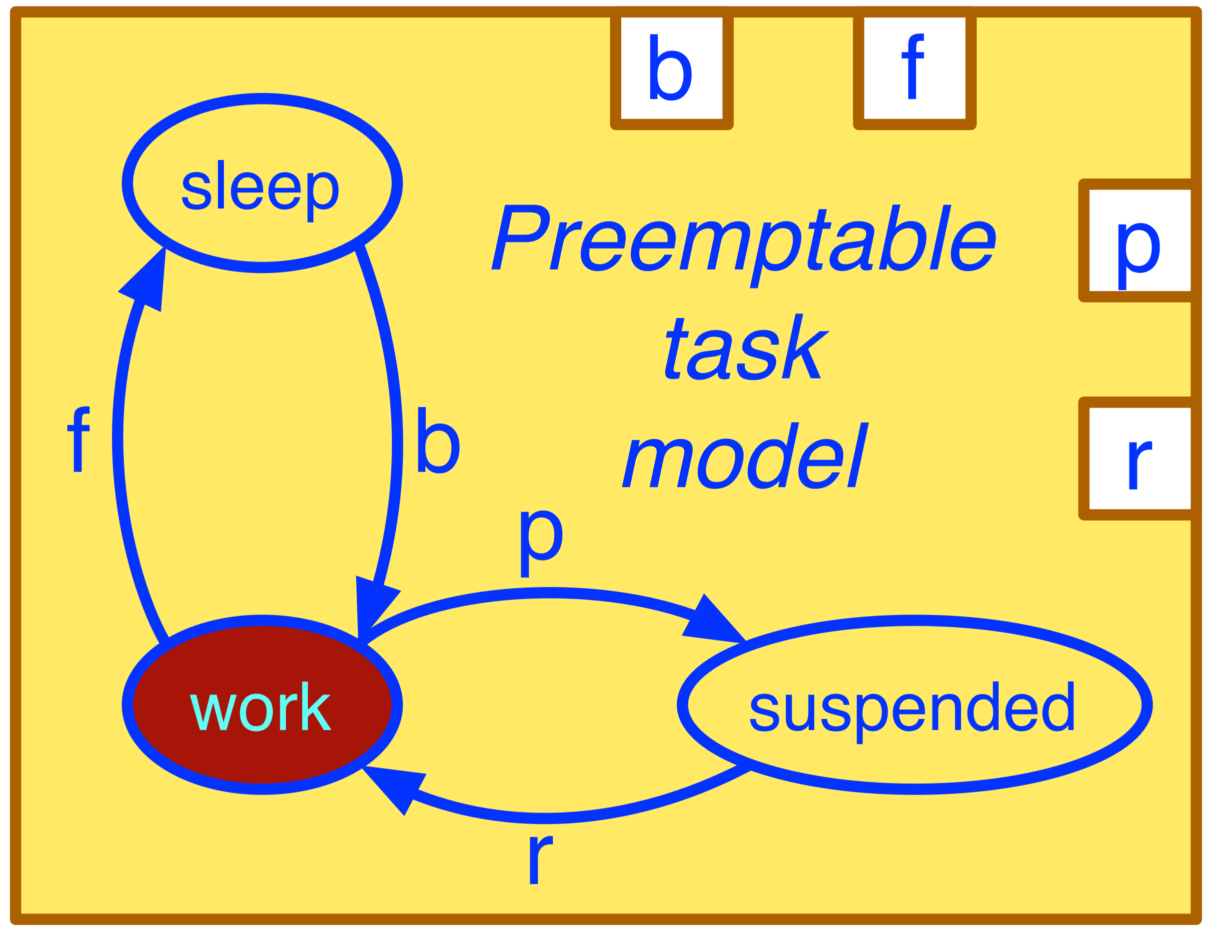
$$p_1 \Rightarrow b_2 \qquad p_2 \Rightarrow b_1$$

$$r_1 \Rightarrow f_2 \qquad r_2 \Rightarrow f_1$$





Example: 2 tasks with preemption



Mutual preemption

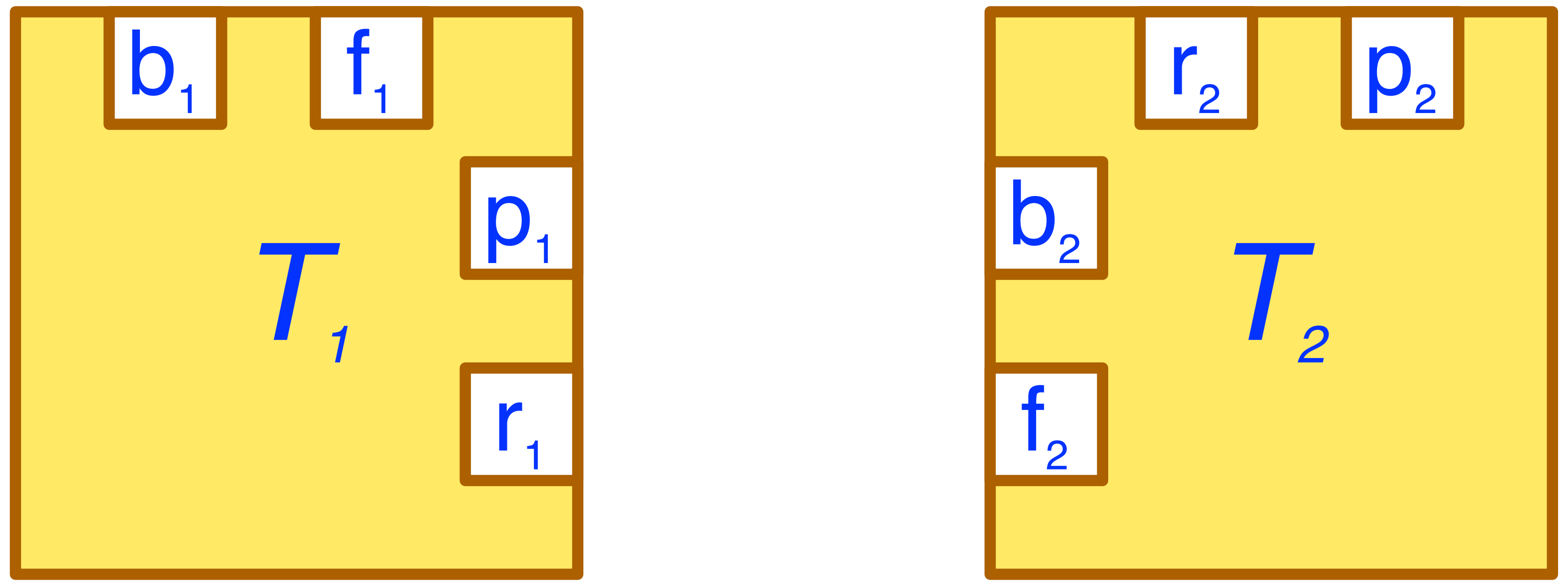
A running task is preemtped, when the other begins computation.

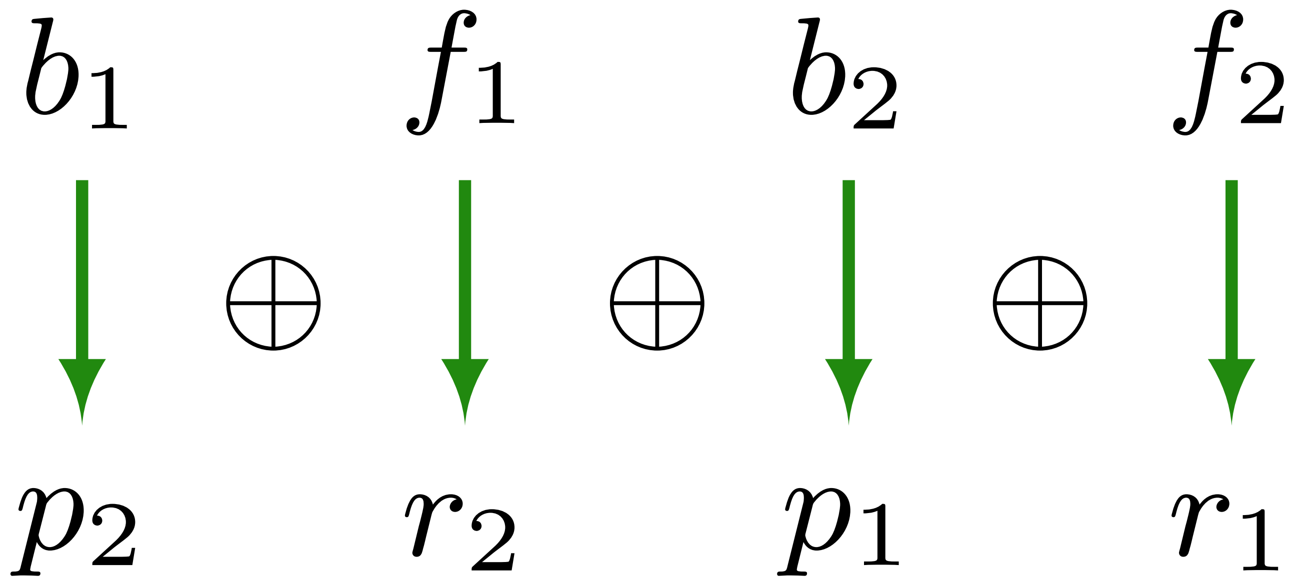
A preempted task resumes computation, when the other one finishes.

$$true \Rightarrow b_1 \vee f_1 \vee b_2 \vee f_2$$

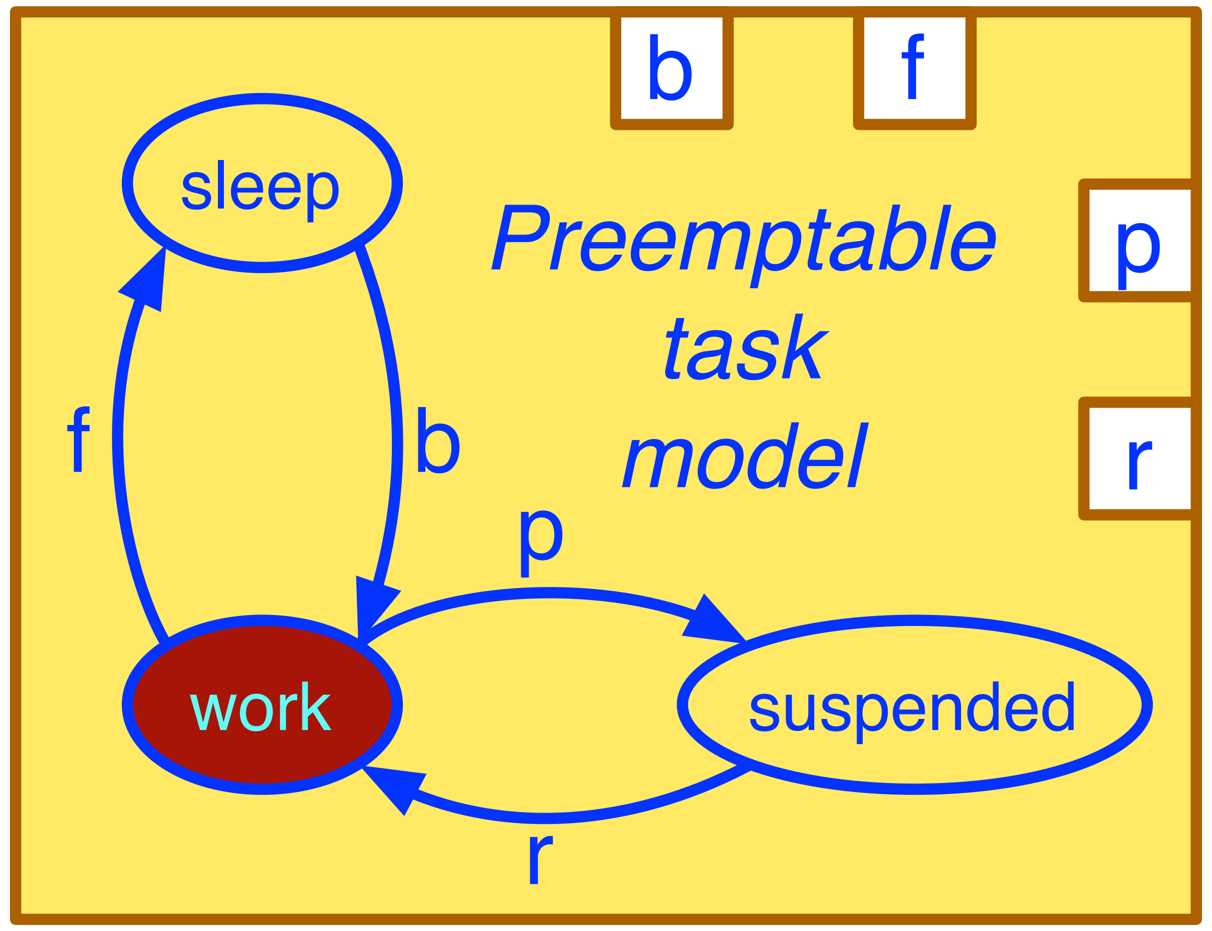
$$p_1 \Rightarrow b_2 \qquad p_2 \Rightarrow b_1$$

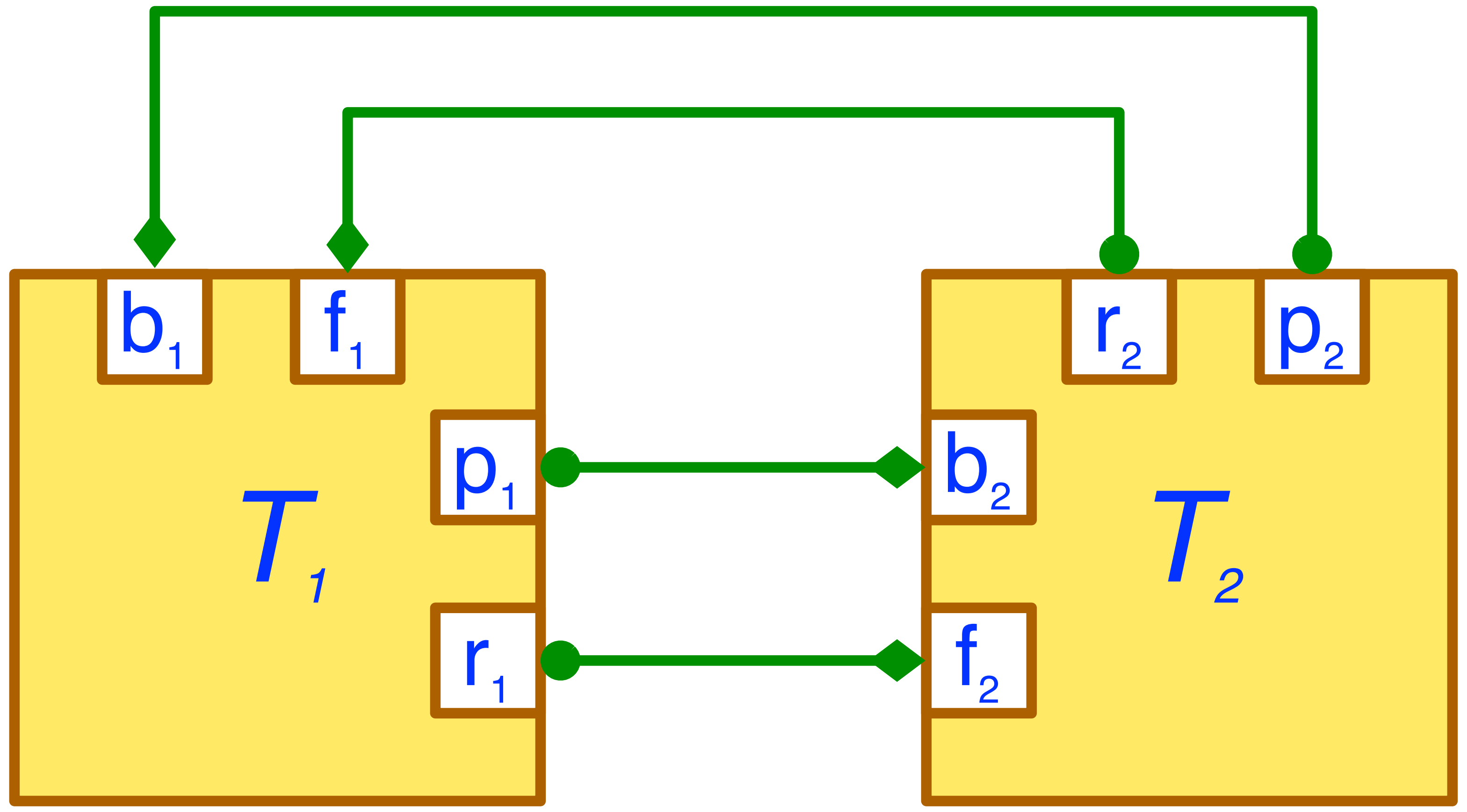
$$r_1 \Rightarrow f_2 \qquad r_2 \Rightarrow f_1$$





Example: 2 tasks with preemption





Mutual preemption

A running task is preemtped, when the other begins computation.

A preempted task resumes computation, when the other one finishes.

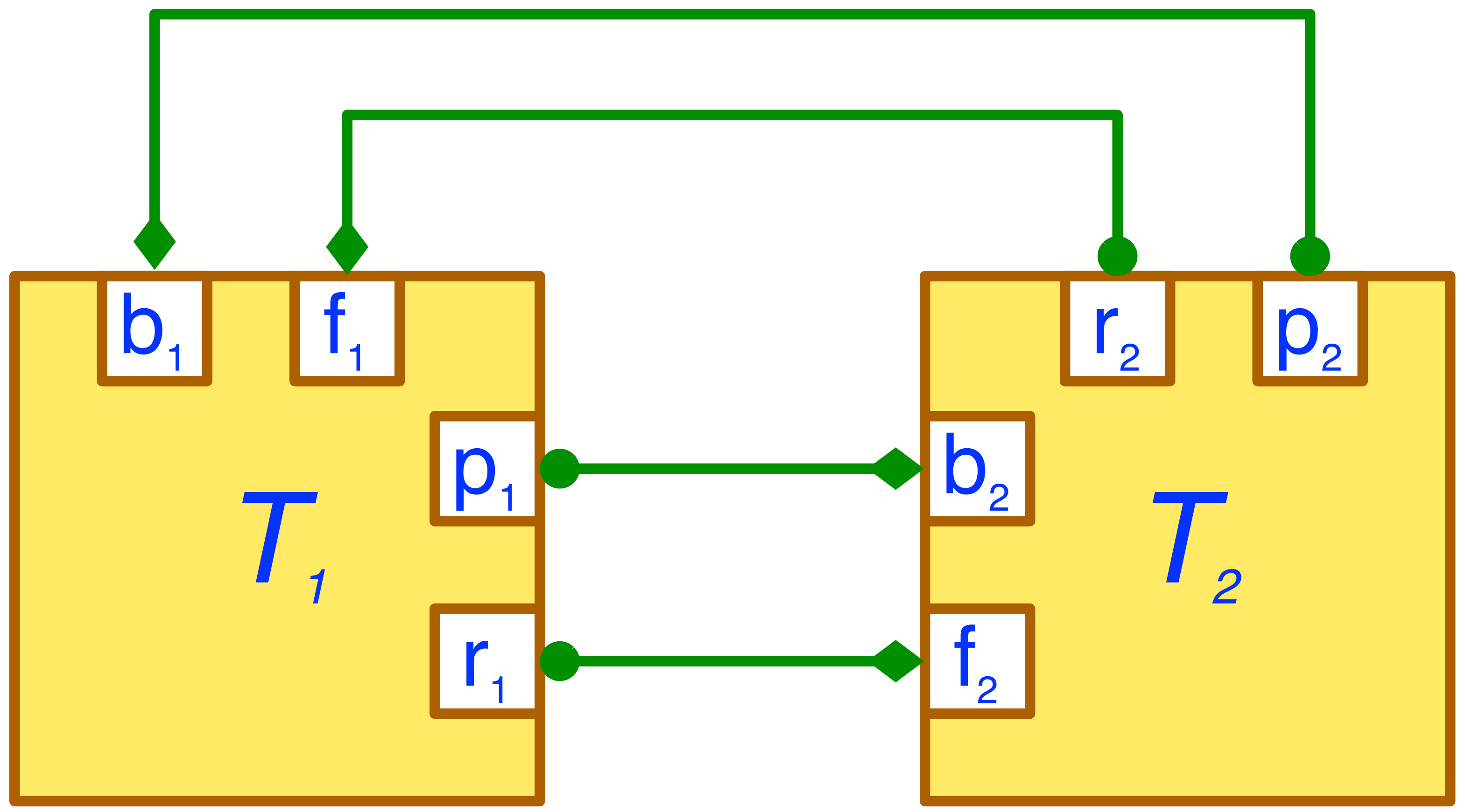
$$true \Rightarrow b_1 \vee f_1 \vee b_2 \vee f_2$$

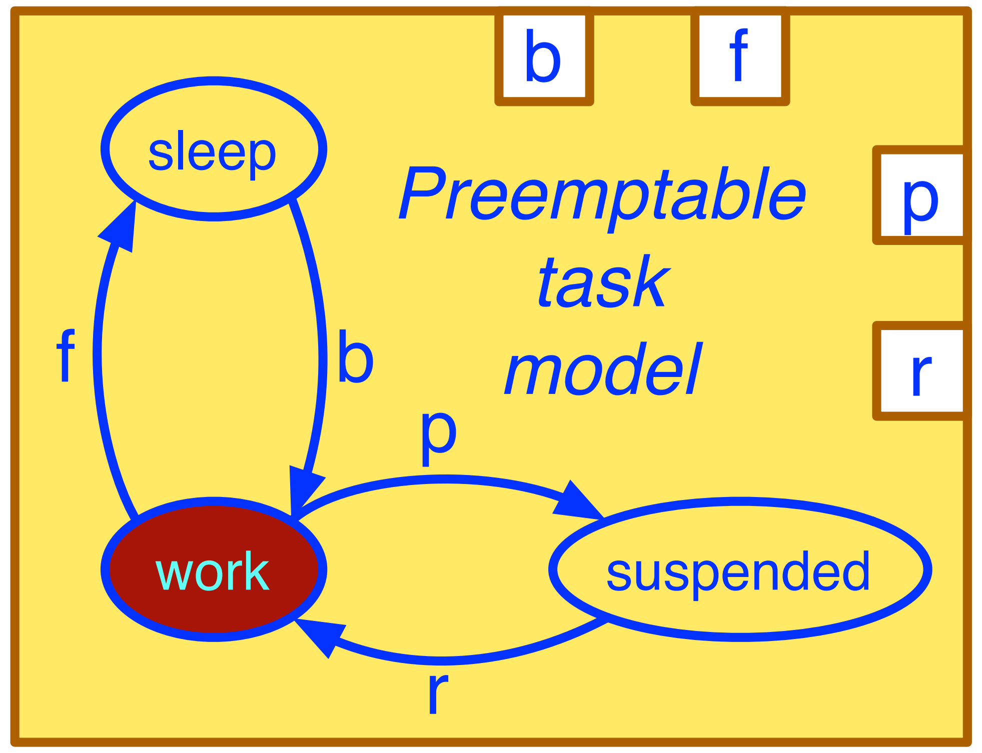
$$p_1 \Rightarrow b_2 \qquad p_2 \Rightarrow b_1$$

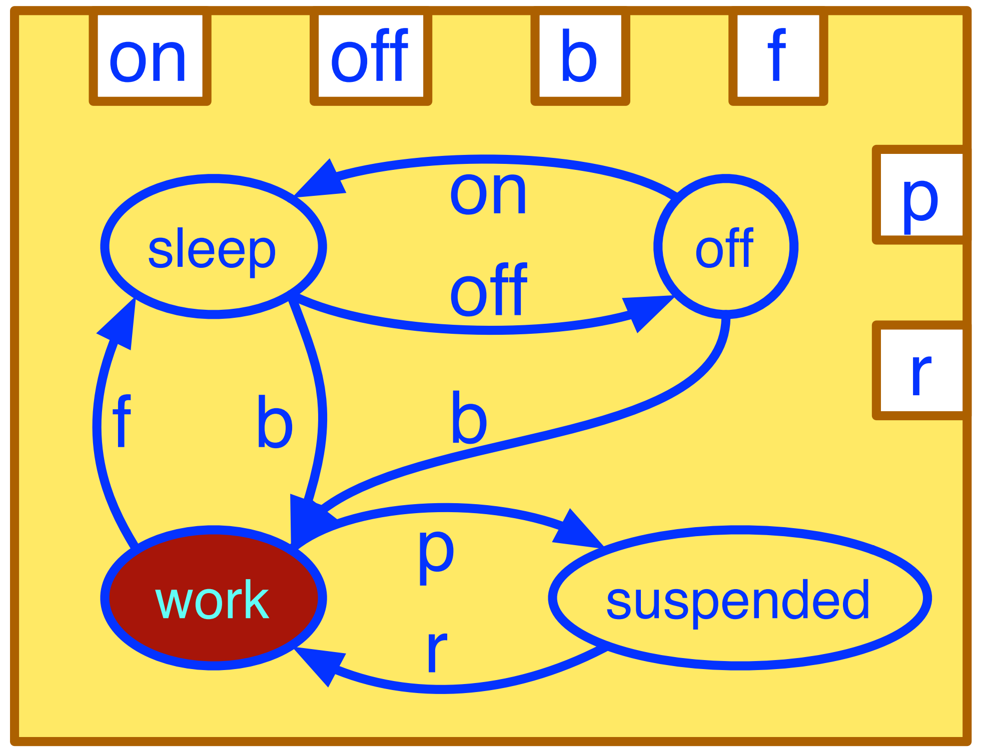
$$r_1 \Rightarrow f_2 \qquad r_2 \Rightarrow f_1$$

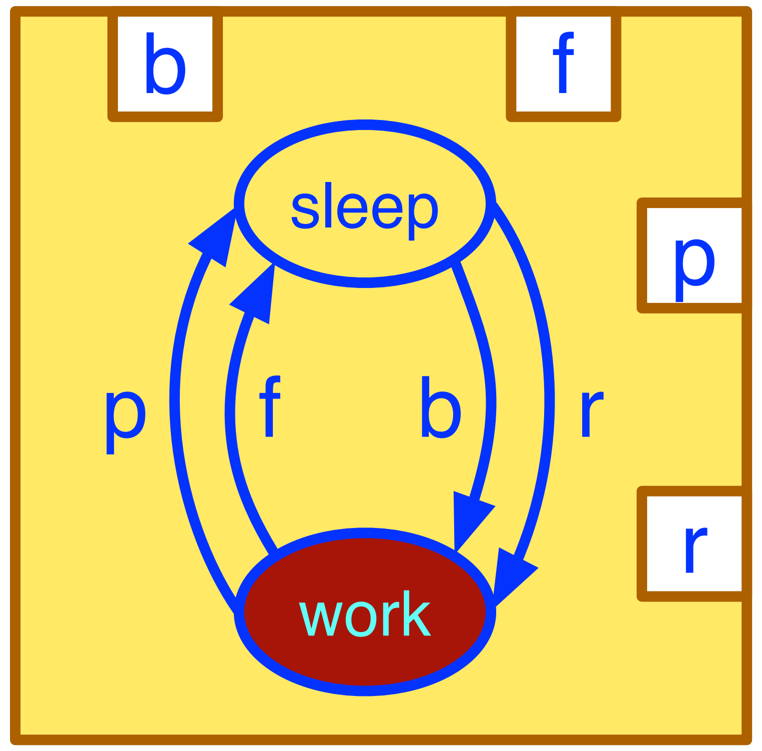
$$\begin{array}{c} b_1 \\ \downarrow \\ p_2 \end{array} \oplus \begin{array}{c} f_1 \\ \downarrow \\ r_2 \end{array} \oplus \begin{array}{c} b_2 \\ \downarrow \\ p_1 \end{array} \oplus \begin{array}{c} f_2 \\ \downarrow \\ r_1 \end{array}$$

Synthesised connectors are the weakest possible









Example: Sequential execution of 2 tasks

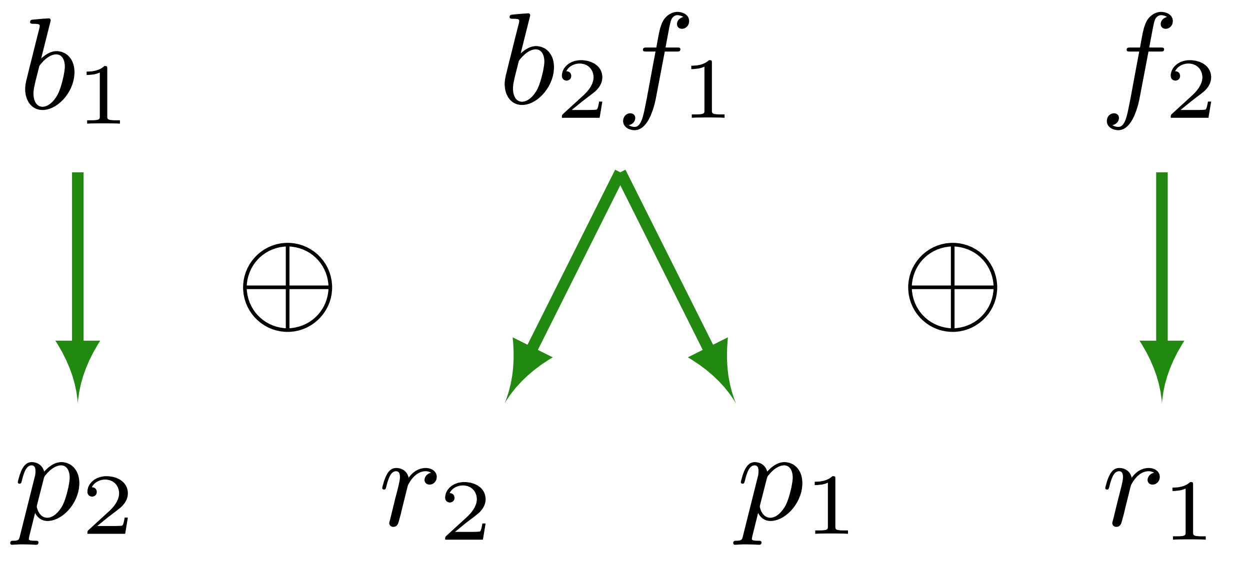
"T_1 ; T_2", i.e. $f_1 = b_2$

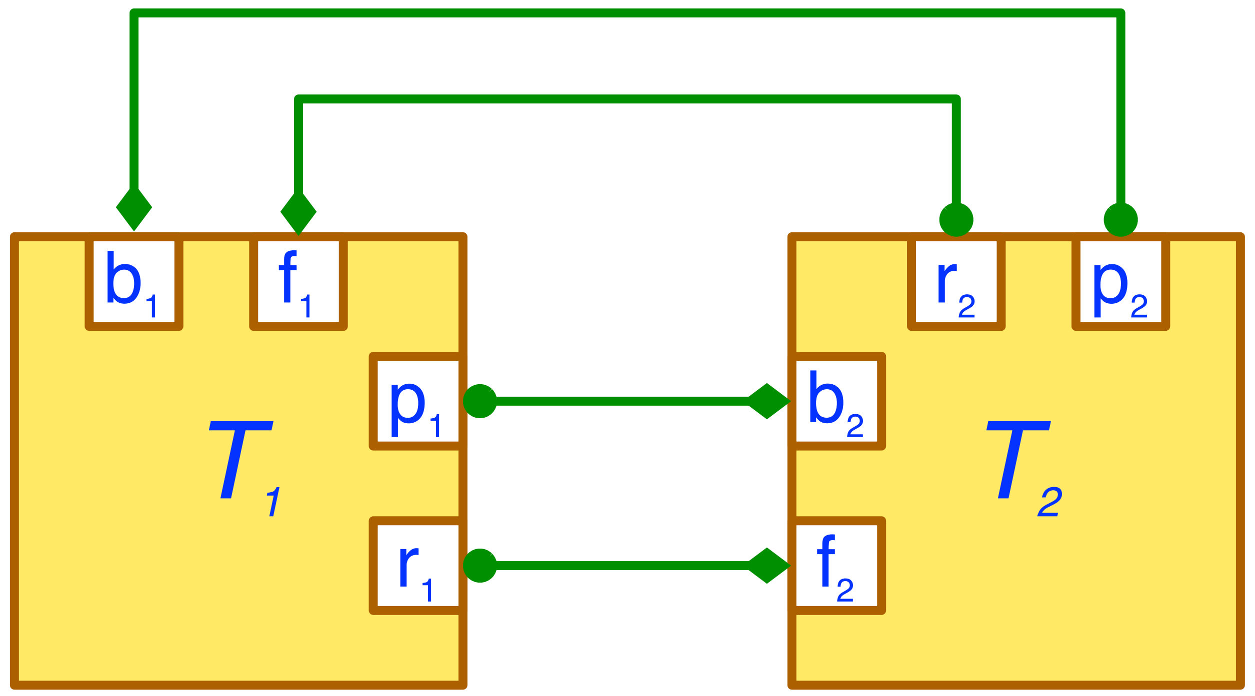
$$true \Rightarrow b_1 \vee f_1 \vee b_2 \vee f_2$$

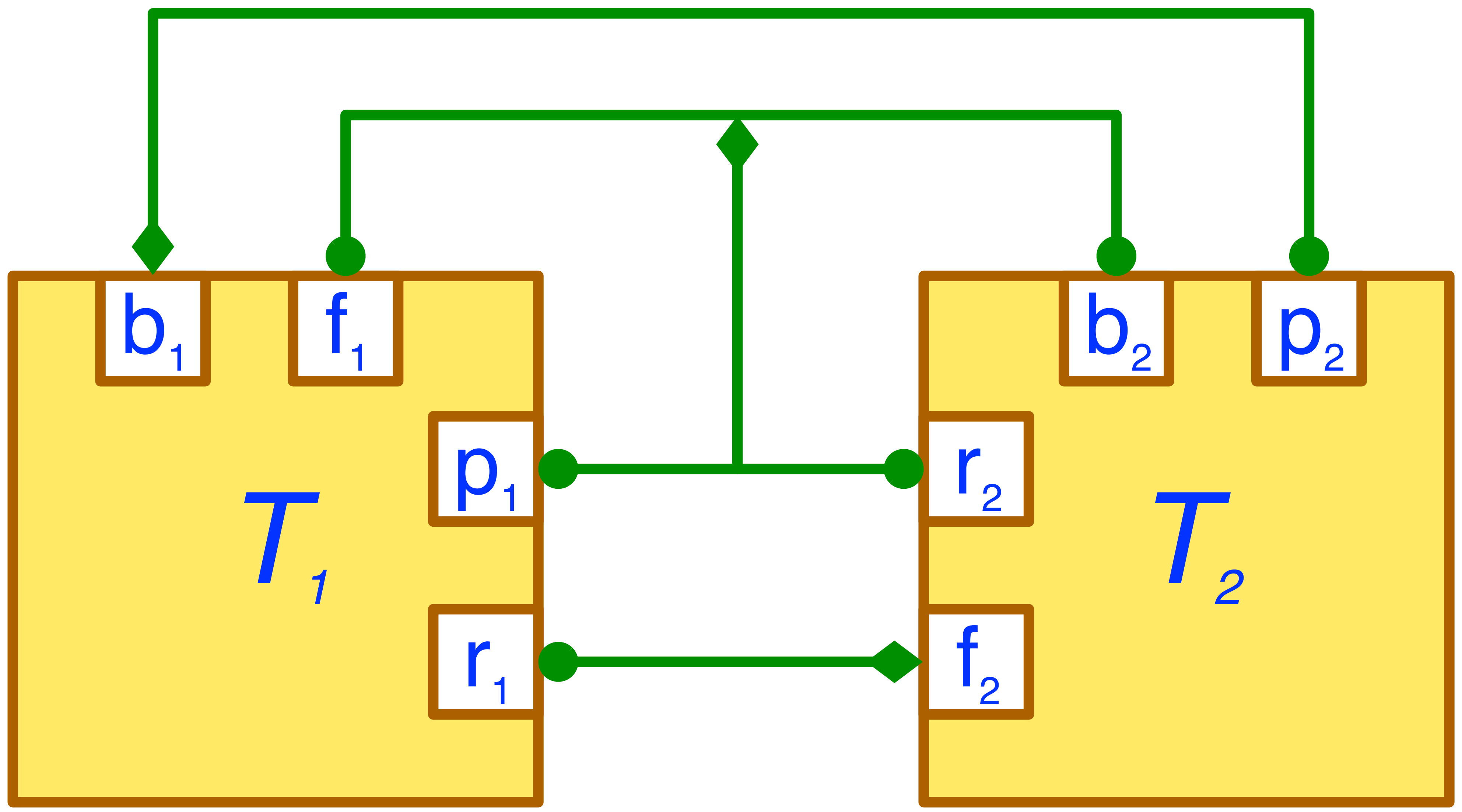
$$p_1 \Rightarrow b_2 \qquad p_2 \Rightarrow b_1$$

$$r_1 \Rightarrow f_2 \qquad r_2 \Rightarrow f_1$$

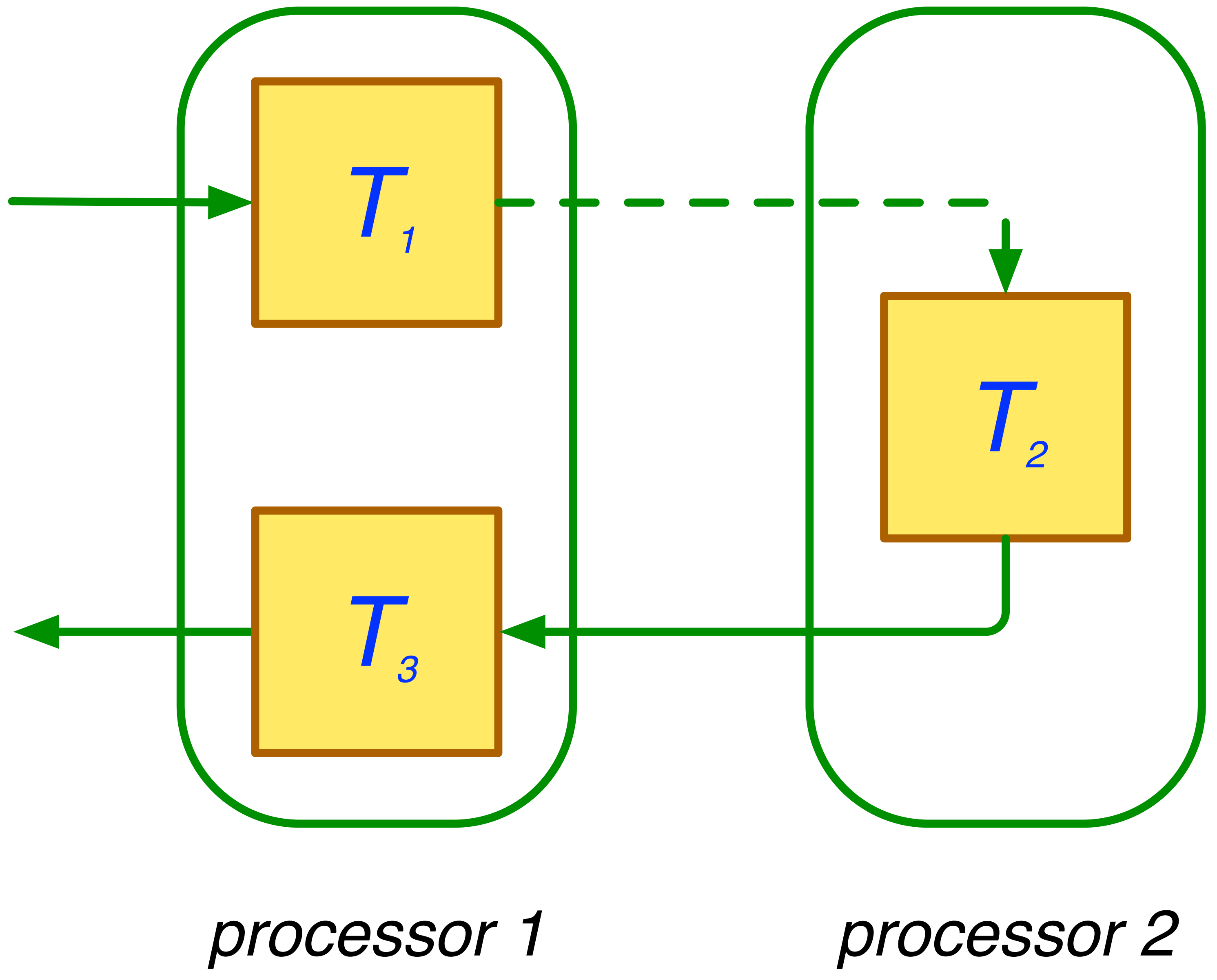
$$\mathbf{f_1} \Rightarrow \mathbf{b_2} \qquad \mathbf{b_2} \Rightarrow \mathbf{f_1}$$







Example: 3 sequential tasks on 2 processors



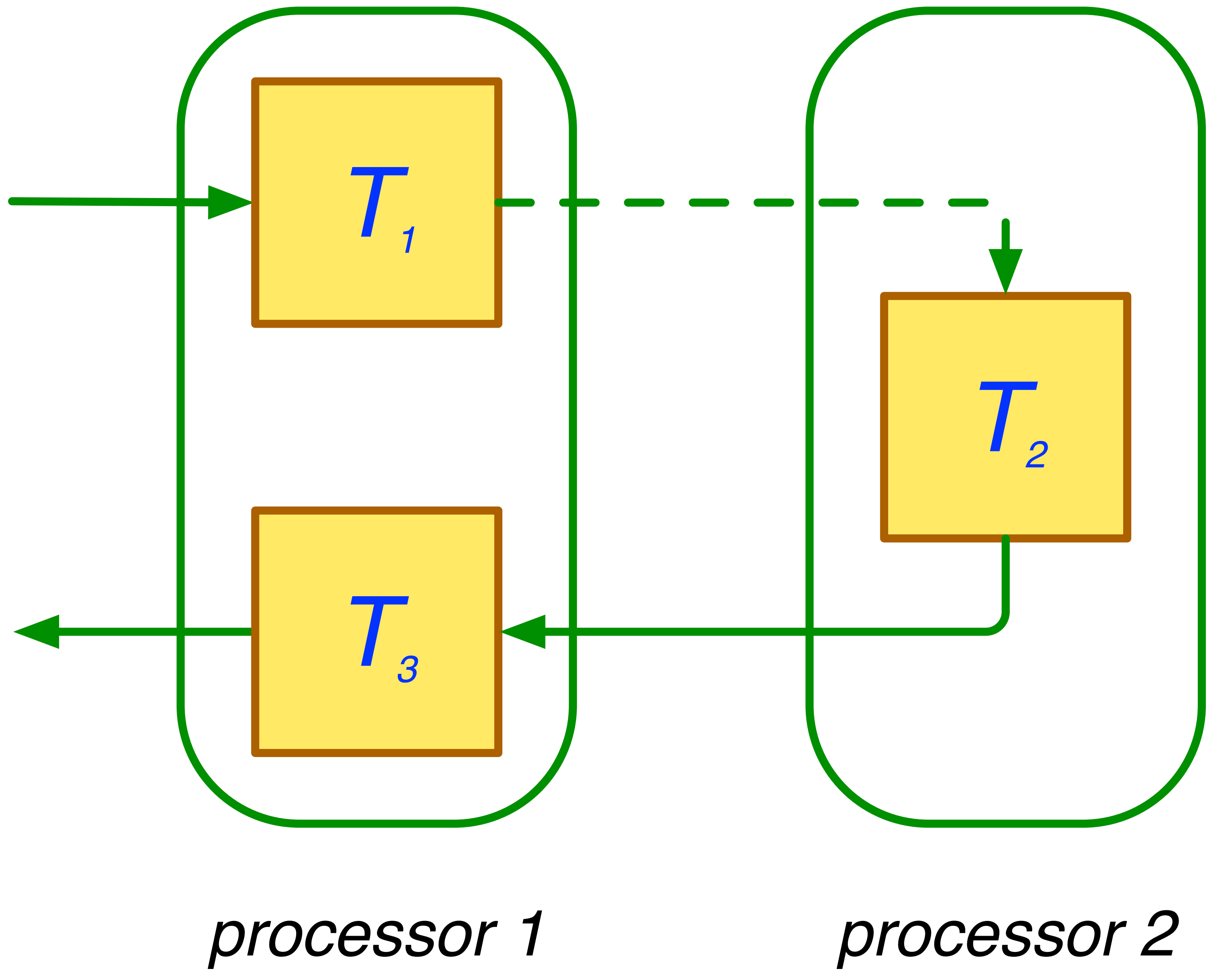
$$true \Rightarrow b_1 \vee f_1 \vee b_2 \vee f_2 \vee b_3 \vee f_3$$

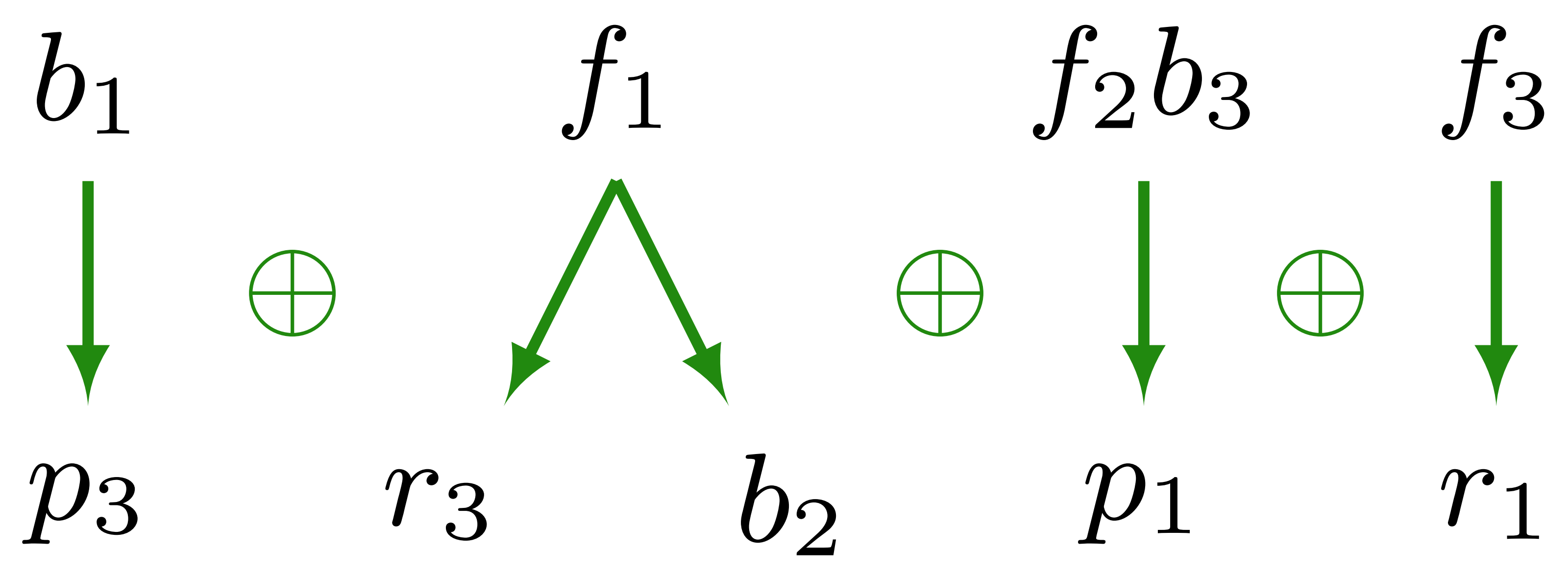
$$p_1 \Rightarrow b_3 \qquad p_3 \Rightarrow b_1$$

$$r_1 \Rightarrow f_3 \qquad r_3 \Rightarrow f_1$$

$$\mathbf{b_2} \Rightarrow \mathbf{f_1} \qquad \mathbf{f_2} = \mathbf{b_3}$$

Example: 3 sequential tasks on 2 processors



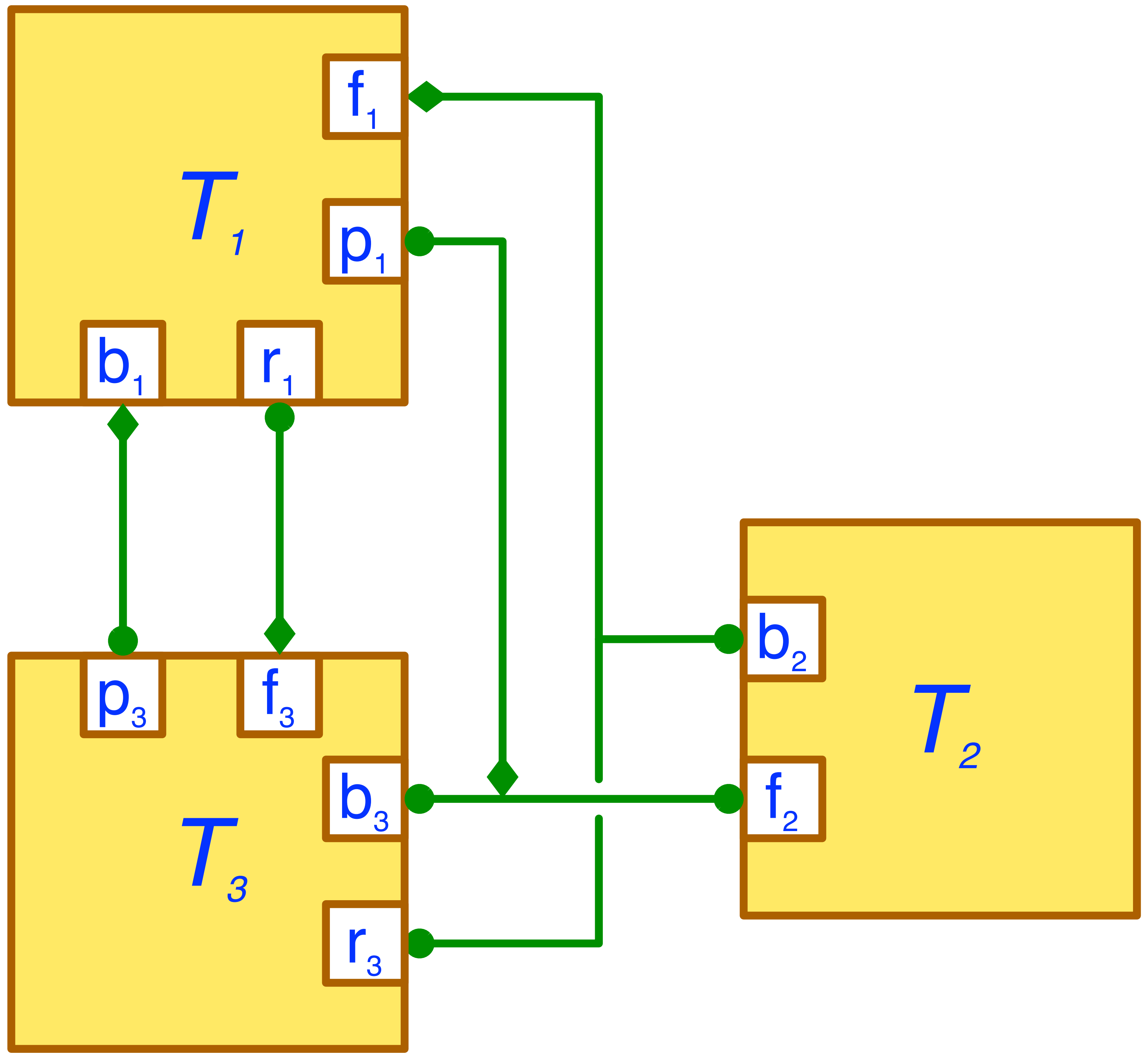


$$true \Rightarrow b_1 \vee f_1 \vee b_2 \vee f_2 \vee b_3 \vee f_3$$

$$p_1 \Rightarrow b_3 \qquad p_3 \Rightarrow b_1$$

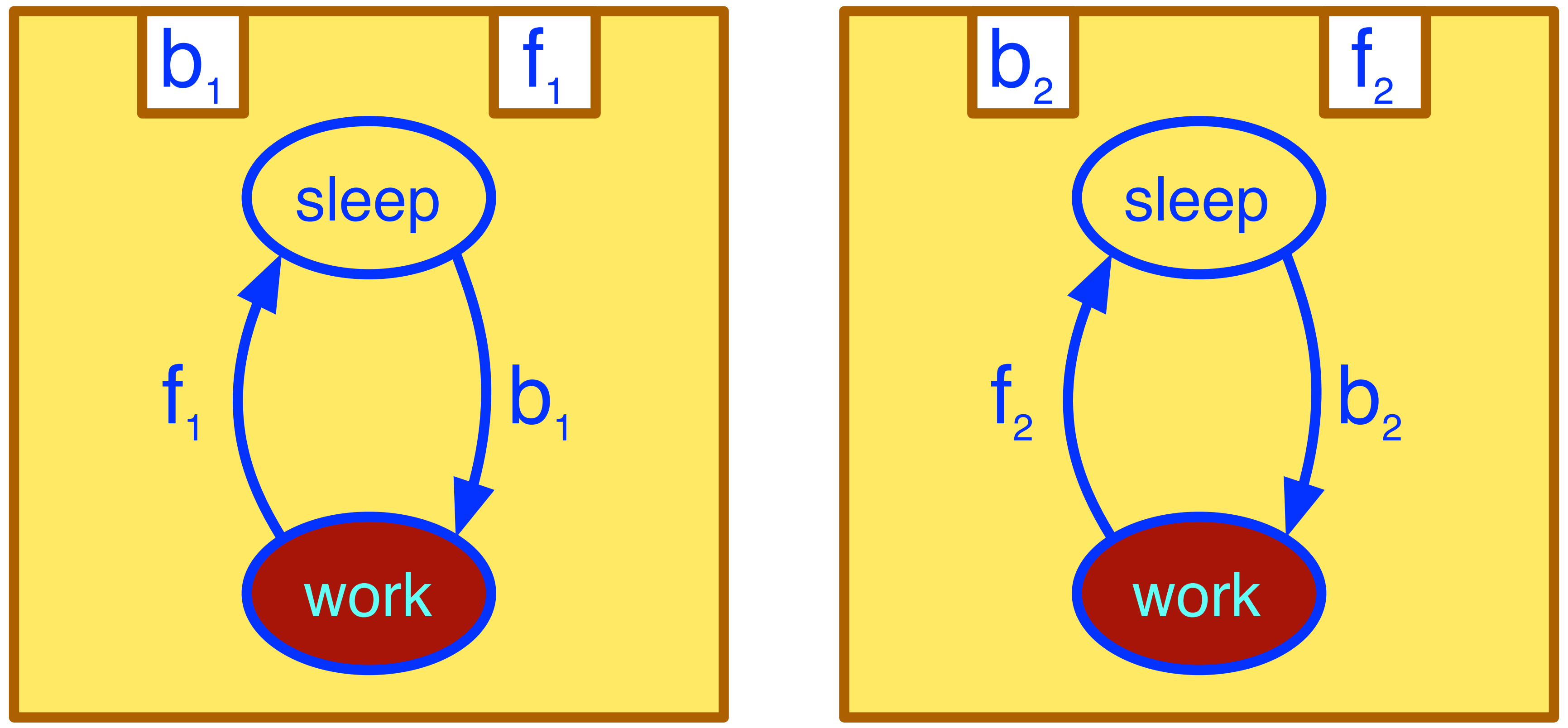
$$r_1 \Rightarrow f_3 \qquad r_3 \Rightarrow f_1$$

$$\mathbf{b_2} \Rightarrow \mathbf{f_1} \qquad \mathbf{f_2} = \mathbf{b_3}$$



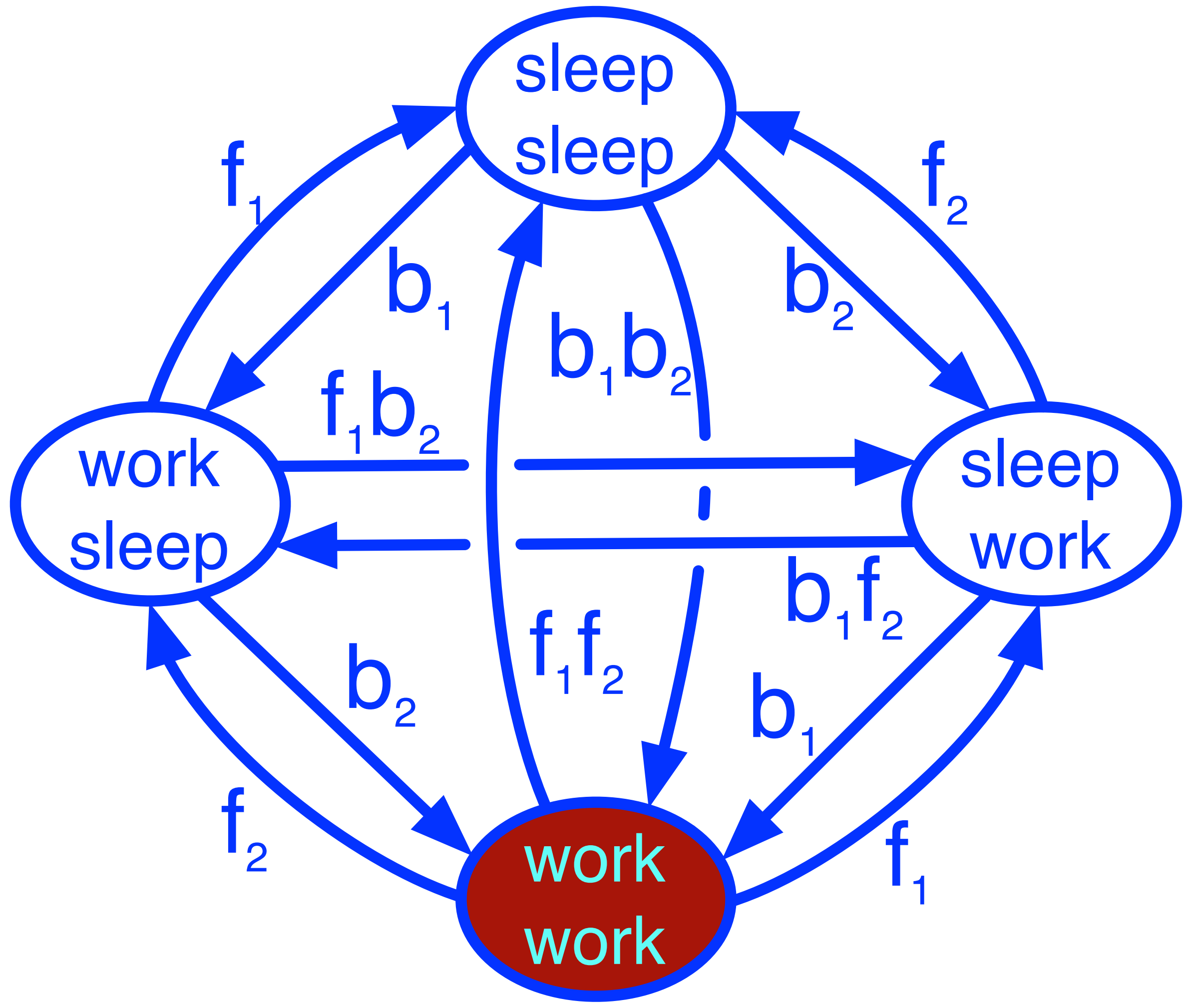
Priorities

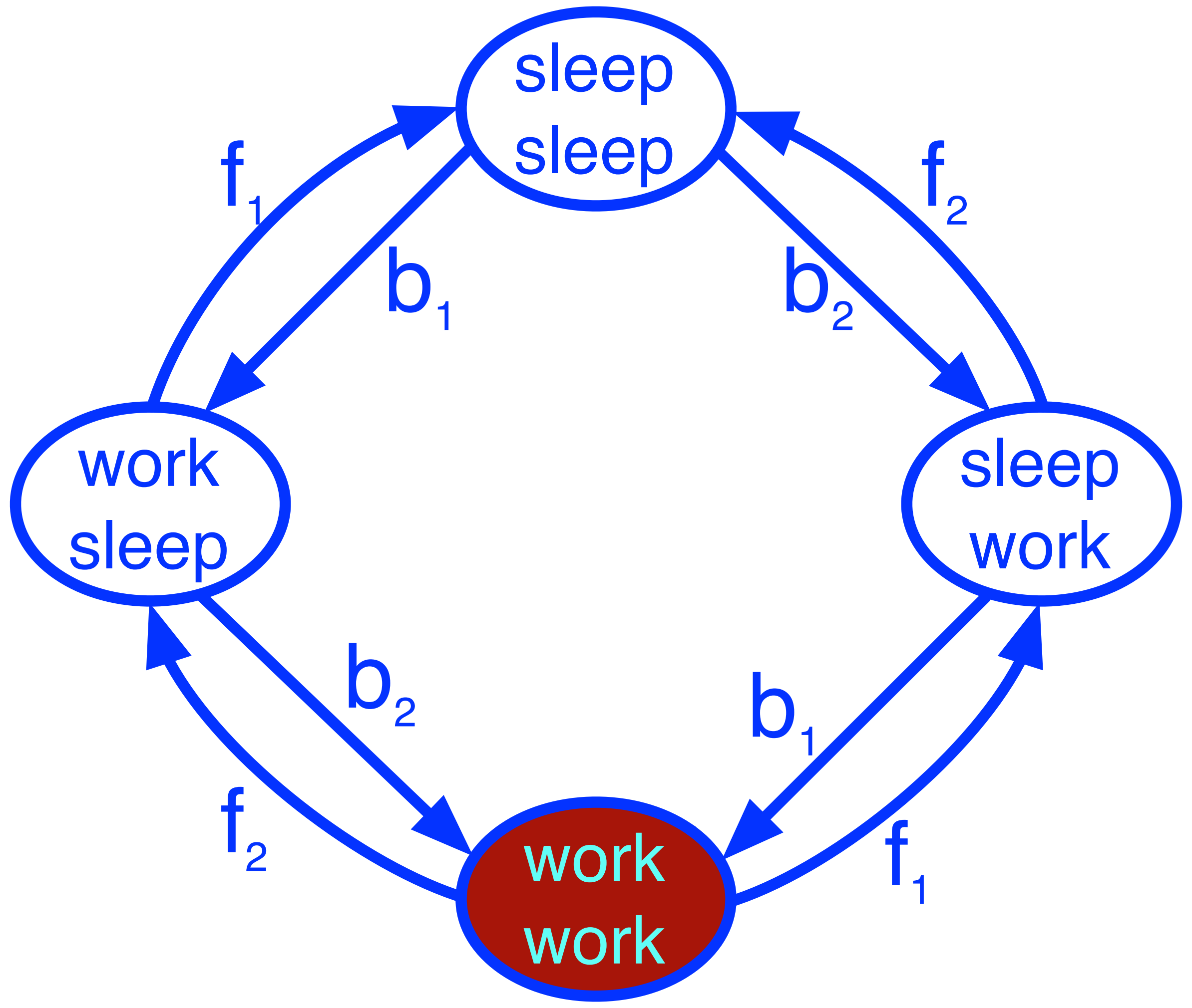
Example: Mutual exclusion

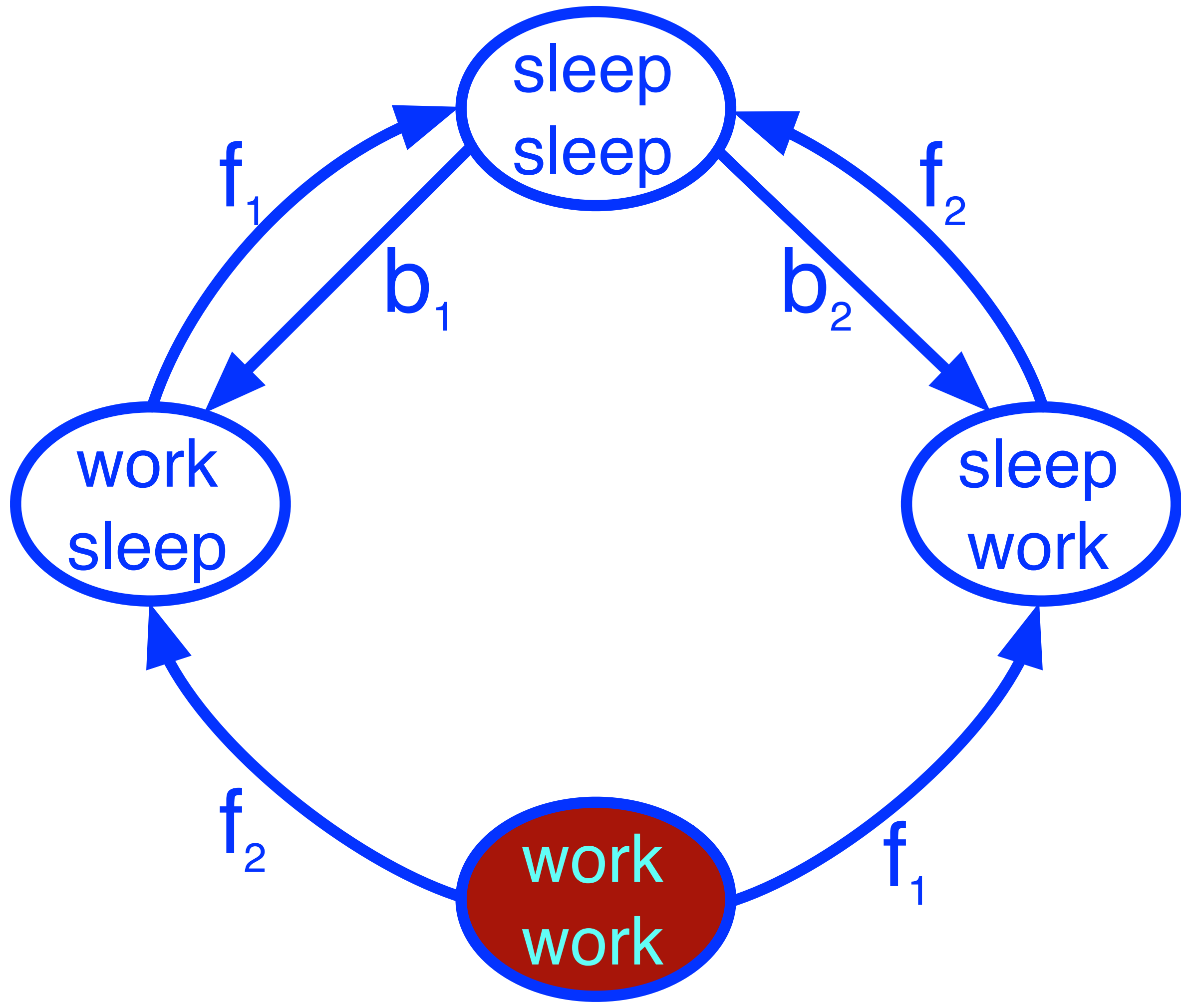


Interaction model: $\{b_1, f_1, b_2, f_2\}$

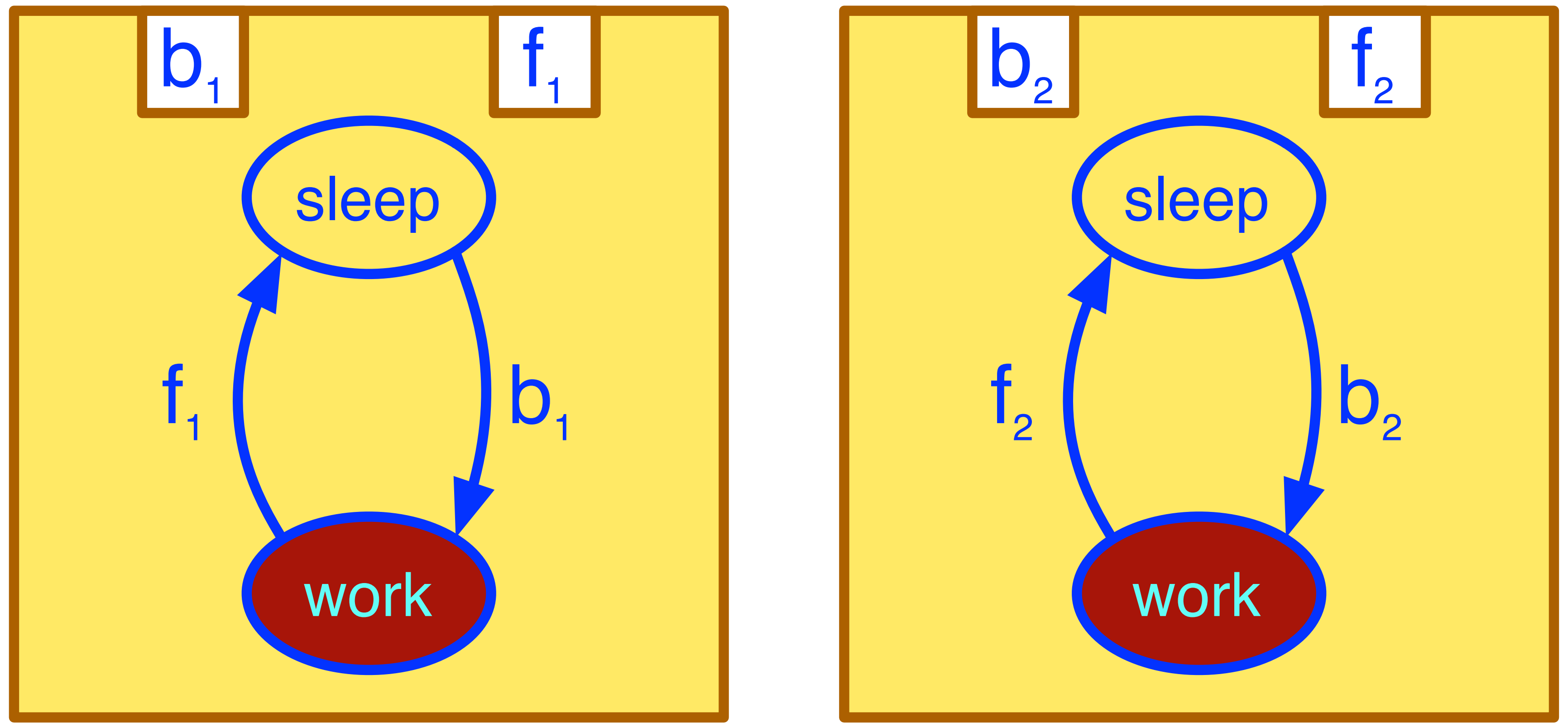
Priority model: $b_1 < f_2,\ b_2 < f_1$







Example: Mutual exclusion (2/3)



Mutual exclusion:

Task 1 can enter the critical state if the other is in the non-critical one or leaves the critical state simultaneously

$$fire(b_1) \Rightarrow \neg active(f_2) \vee fire(f_2)$$

Idem for Task 2

$$fire(b_2) \Rightarrow \neg active(f_1) \vee fire(f_1)$$

The two tasks cannot enter the critical states simultaneously

$$\neg\Big(fire(b_1) \wedge fire(b_2)\Big)$$

Example: Mutual exclusion (3/3)

For a port p in P, let p and $\dot{p}$ be boolean *activation* and *firing* variables with an additional axiom $\dot{p} \Rightarrow p$.

Example: Mutual exclusion (3/3)

For a port p in P, let p and ṗ be boolean *activation* and *firing* variables with an additional axiom ṗ ⇒ p.

Mutual exclusion: $\left(\dot{b}_1 \Rightarrow \overline{f_2} \vee \dot{f}_2\right) \wedge \left(\dot{b}_2 \Rightarrow \overline{f_1} \vee \dot{f}_1\right) \wedge \overline{\dot{b}_1 \dot{b}_2}$

Progress: $\wedge \left(\dot{b}_1 \vee \dot{f}_1 \vee \dot{b}_2 \vee \dot{f}_2\right)$

"Internality" of finish: $\wedge \overline{\dot{f}_1 \dot{f}_2} \wedge \left(\dot{f}_1 \vee \dot{f}_2 \Rightarrow \overline{\dot{b}_1}\, \overline{\dot{b}_2}\right) =$

Example: Mutual exclusion (3/3)

For a port p in P, let p and $\dot{p}$ be boolean *activation* and *firing* variables with an additional axiom $\dot{p} \Rightarrow p$.

Mutual exclusion: $\left(\dot{b}_1 \Rightarrow \overline{f_2} \vee \dot{f}_2\right) \wedge \left(\dot{b}_2 \Rightarrow \overline{f_1} \vee \dot{f}_1\right) \wedge \overline{\dot{b}_1 \dot{b}_2}$

Progress: $\wedge \left(\dot{b}_1 \vee \dot{f}_1 \vee \dot{b}_2 \vee \dot{f}_2\right)$

"Internality" of finish: $\wedge\, \overline{\dot{f}_1 \dot{f}_2} \wedge \left(\dot{f}_1 \vee \dot{f}_2 \Rightarrow \overline{\dot{b}_1}\,\overline{\dot{b}_2}\right) =$

$$= \overline{\dot{b}_1}\,\overline{\dot{b}_2}\,\dot{f}_1\,\overline{\dot{f}_2} \vee \overline{\dot{b}_1}\,\overline{\dot{b}_2}\,\overline{\dot{f}_1}\,\dot{f}_2 \vee \dot{b}_1\,\overline{\dot{b}_2}\,\overline{\dot{f}_1}\,\overline{\dot{f}_2}\,\overline{f_2} \vee \overline{\dot{b}_1}\,\dot{b}_2\,\overline{\dot{f}_1}\,\overline{\dot{f}_2}\,\overline{f_1}$$

Example: Mutual exclusion (3/3)

For a port p in P, let p and ṗ be boolean *activation* and *firing* variables with an additional axiom ṗ ⇒ p.

Mutual exclusion: $\left(\dot{b}_1 \Rightarrow \overline{f_2} \vee \dot{f}_2\right) \wedge \left(\dot{b}_2 \Rightarrow \overline{f_1} \vee \dot{f}_1\right) \wedge \overline{\dot{b}_1 \dot{b}_2}$

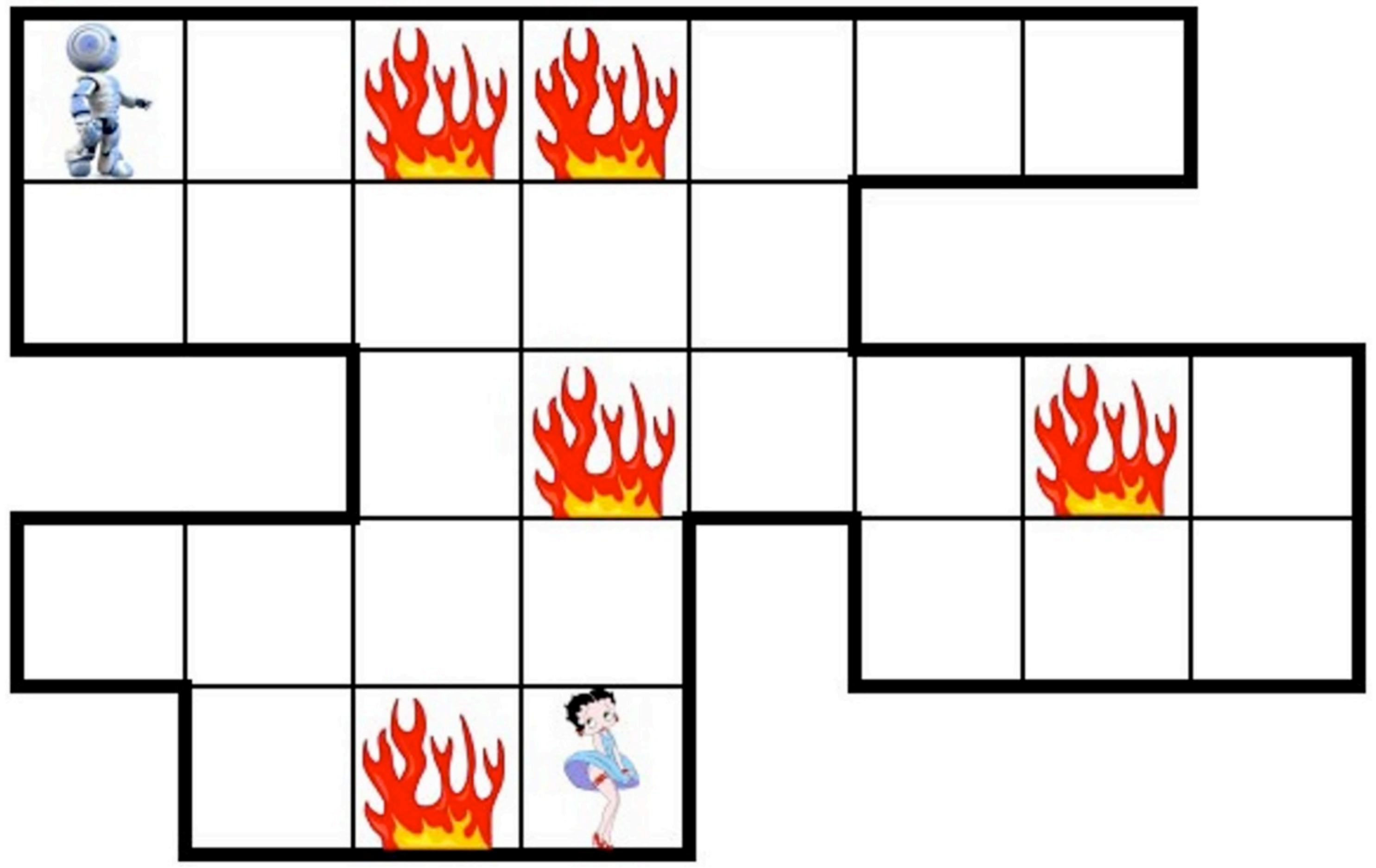
Progress: $\wedge \left(\dot{b}_1 \vee \dot{f}_1 \vee \dot{b}_2 \vee \dot{f}_2\right)$

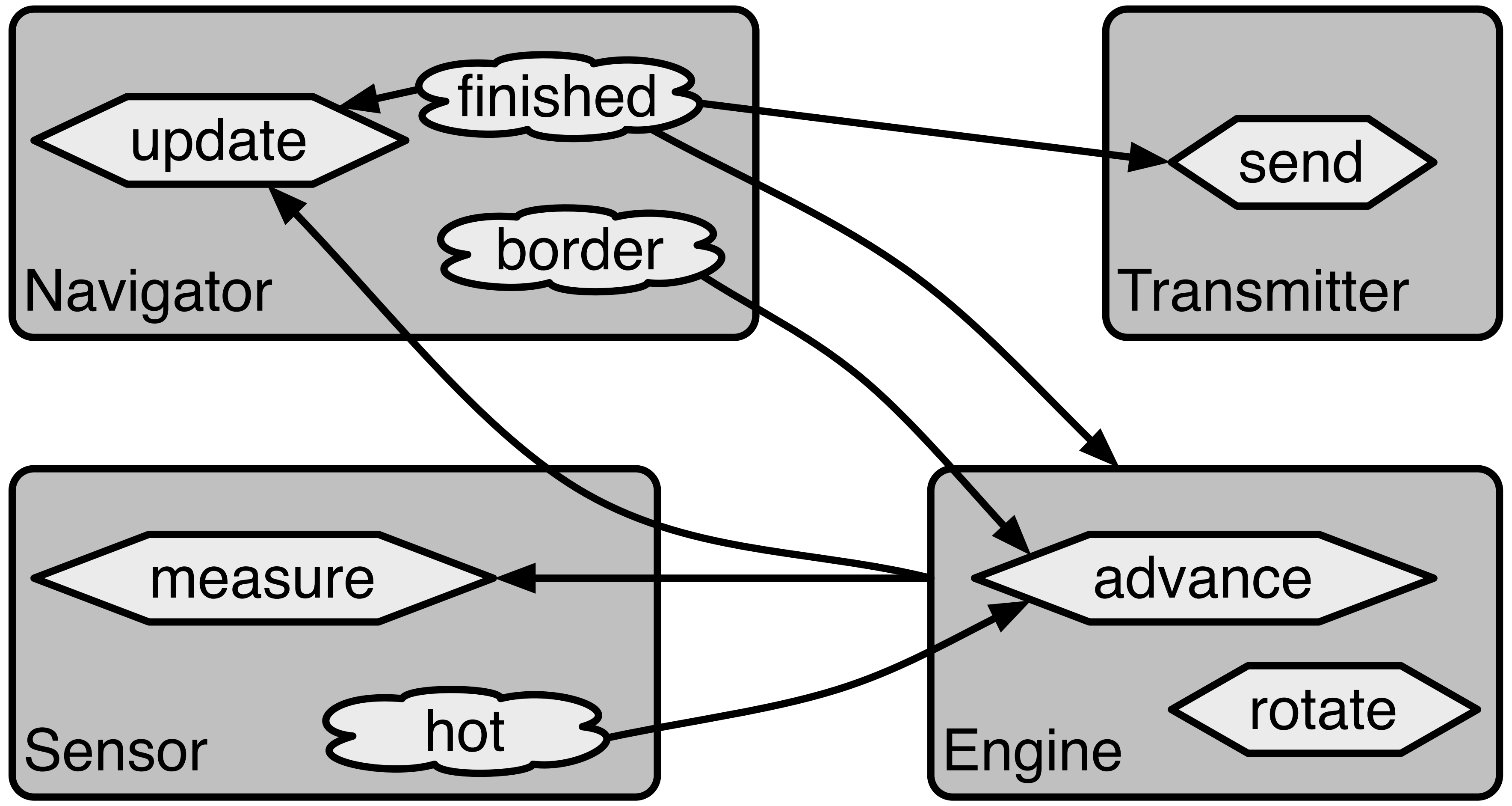
"Internality" of finish: $\wedge \overline{\dot{f}_1 \dot{f}_2} \wedge \left(\dot{f}_1 \vee \dot{f}_2 \Rightarrow \overline{\dot{b}_1}\, \overline{\dot{b}_2}\right) =$

$$= \overline{\dot{b}_1}\, \overline{\dot{b}_2}\, \dot{f}_1 \overline{\dot{f}_2} \vee \overline{\dot{b}_1}\, \overline{\dot{b}_2}\, \overline{\dot{f}_1} \dot{f}_2 \vee \dot{b}_1\, \overline{\dot{b}_2}\, \overline{\dot{f}_1}\, \overline{\dot{f}_2}\, \overline{f_2} \vee \overline{\dot{b}_1}\, \dot{b}_2\, \overline{\dot{f}_1}\, \overline{\dot{f}_2}\, \overline{f_1}$$

$$\frac{q_1 \xrightarrow{f_1} q_1'}{q_1 q_2 \xrightarrow{f_1} q_1' q_2}, \quad \frac{q_2 \xrightarrow{f_2} q_2'}{q_1 q_2 \xrightarrow{f_2} q_1 q_2'}, \quad \underbrace{\frac{q_1 \xrightarrow{b_1} q_1' \quad q_2 \not\xrightarrow{f_2}}{q_1 q_2 \xrightarrow{b_1} q_1' q_2}, \quad \frac{q_1 \not\xrightarrow{f_1} \quad q_2 \xrightarrow{b_2} q_2'}{q_1 q_2 \xrightarrow{b_2} q_1 q_2'}}_{\text{Priorities: } b_1 \prec f_2,\ b_2 \prec f_1}$$

Rescue robot





Safety constraints

Shall not advance and rotate at the same time

Shall not leave the region

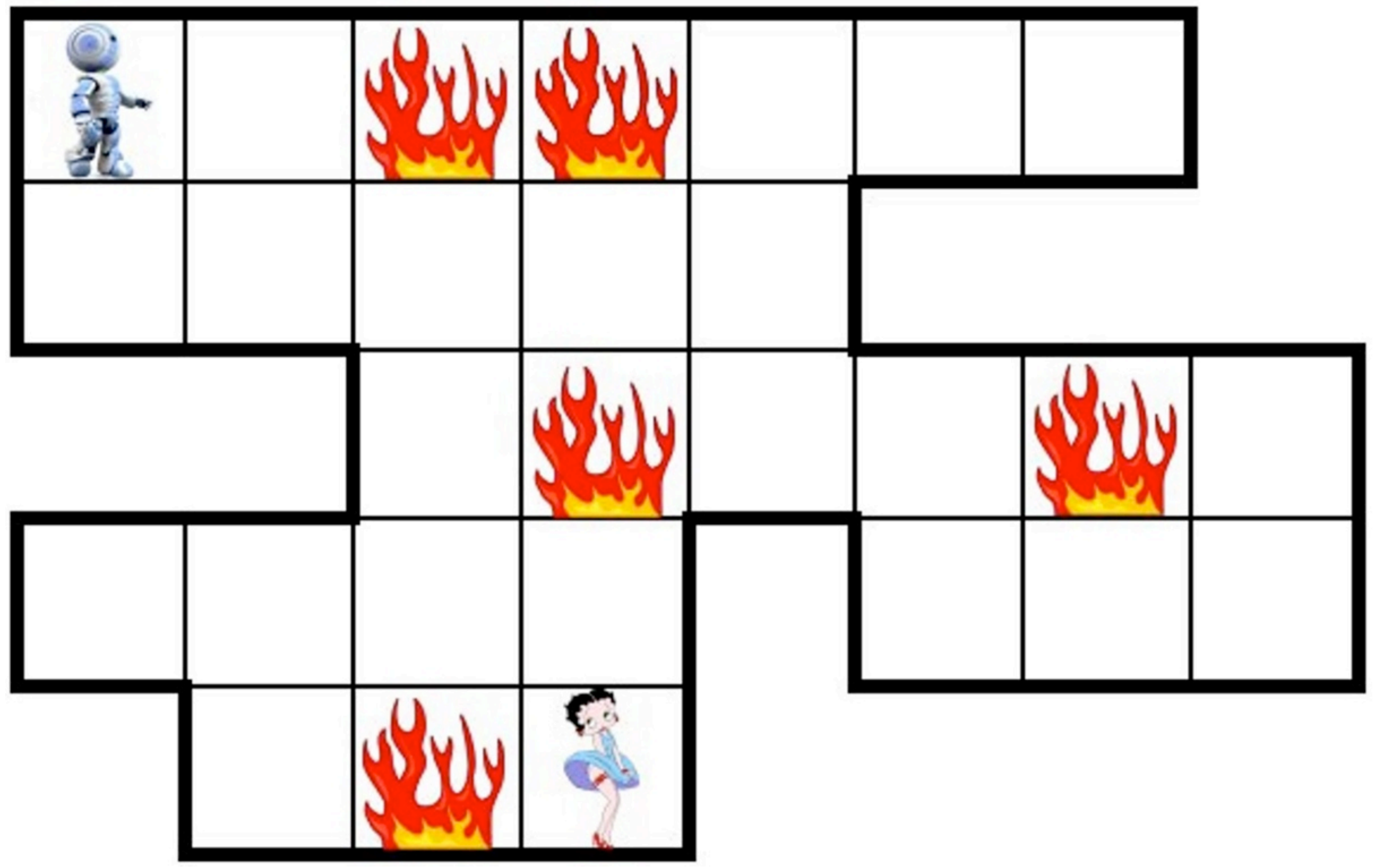
Shall not drive into hot areas

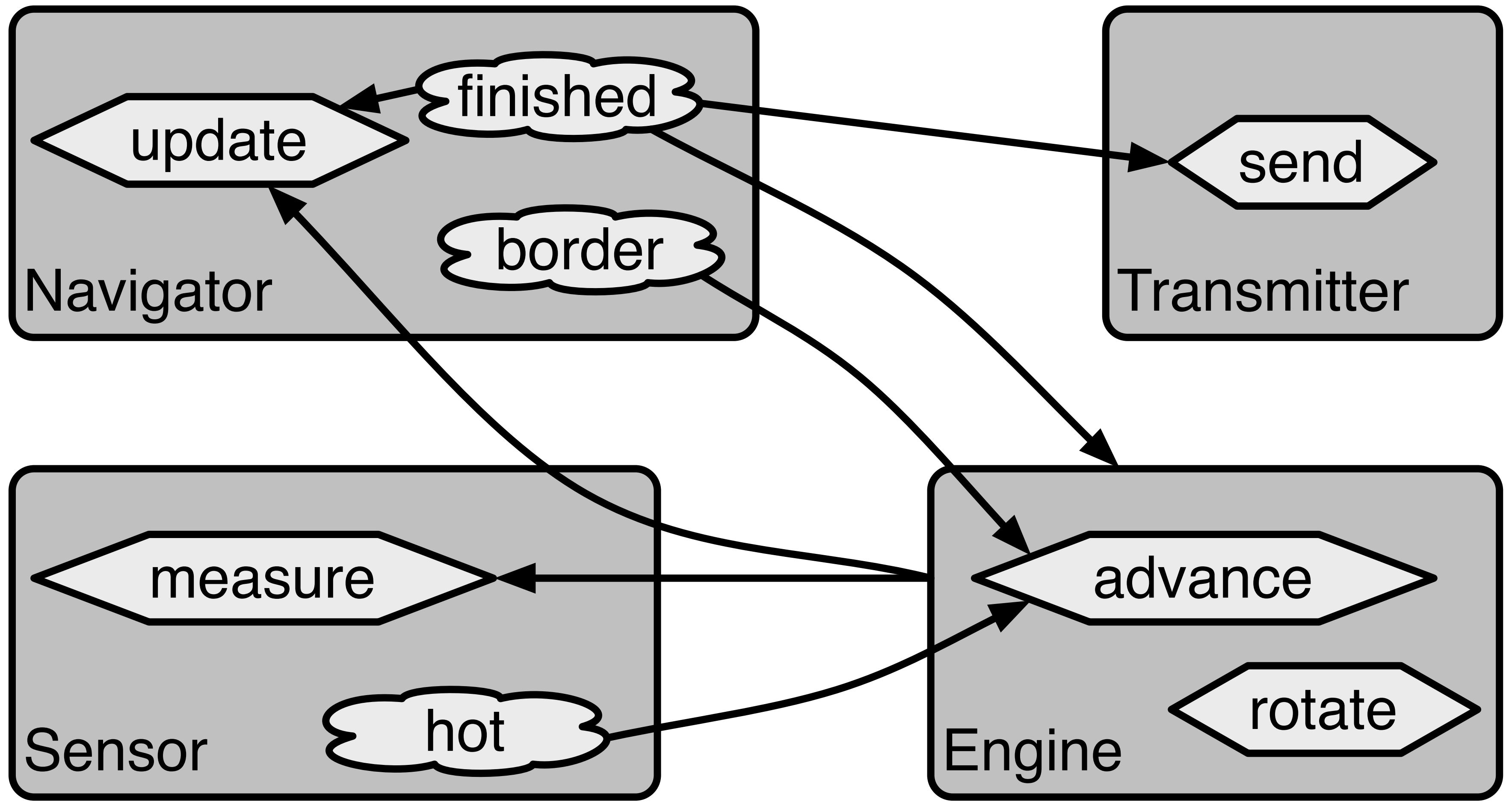
Shall update navigation and sensor data at each move

Shall objective is found, must stop and transmit it's coordinates

Shall transmit coordinates only when objective is reached

Rescue robot





Safety constraints

Shall not advance and rotate at the same time	$\overline{\dot{a}\,\dot{r}}$
Shall not leave the region	$b \Rightarrow \overline{\dot{a}}$
Shall not drive into hot areas	$h \Rightarrow \overline{\dot{a}}$
Shall update navigation and sensor data at each move	$\dot{a} \vee \dot{r} \Rightarrow \dot{u}\,\dot{m}$
Shall objective is found, must stop and transmit it's coordinates	$f \Rightarrow \overline{\dot{a}}\,\overline{\dot{r}}\,\overline{\dot{u}}\,\overline{\dot{m}}\,\dot{s}$
Shall transmit coordinates only when objective is reached	$\dot{s} \Rightarrow f$

Rescue robot

$$\overline{\dot{a}\,\dot{r}} \wedge (b \Rightarrow \overline{\dot{a}}) \wedge (h \Rightarrow \overline{\dot{a}}) \wedge (f \Rightarrow \overline{\dot{a}}\,\overline{\dot{r}}\,\dot{u}\,\dot{m}\,\dot{s}) \wedge (\dot{a} \vee \dot{r} \Rightarrow \dot{u}\,\dot{m})$$ ⟵ Safety

$$\wedge\, (\dot{a} \vee \dot{r} \vee \dot{u} \vee \dot{m} \vee \dot{s}) \wedge \overline{\dot{h}}\,\overline{\dot{b}}\,\overline{\dot{f}}$$ ⟵ Progress

Safety constraints

Shall not advance and rotate at the same time	$\overline{\dot{a}\,\dot{r}}$
Shall not leave the region	$b \Rightarrow \overline{\dot{a}}$
Shall not drive into hot areas	$h \Rightarrow \overline{\dot{a}}$
Shall update navigation and sensor data at each move	$\dot{a} \vee \dot{r} \Rightarrow \dot{u}\,\dot{m}$
Shall objective is found, must stop and transmit it's coordinates	$f \Rightarrow \overline{\dot{a}}\,\overline{\dot{r}}\,\overline{\dot{u}}\,\overline{\dot{m}}\,\dot{s}$
Shall transmit coordinates only when objective is reached	$\dot{s} \Rightarrow f$

Rescue robot

$$\overline{\dot a\,\dot r} \wedge (b \Rightarrow \overline{\dot a}) \wedge (h \Rightarrow \overline{\dot a}) \wedge (f \Rightarrow \overline{\dot a}\,\overline{\dot r}\,\dot u\,\dot m\,\dot s) \wedge (\dot a \vee \dot r \Rightarrow \dot u\,\dot m) \longleftarrow \text{Safety}$$

$$\wedge\, (\dot a \vee \dot r \vee \dot u \vee \dot m \vee \dot s) \wedge \overline{\dot h}\,\overline{\dot b}\,\overline{\dot f} \longleftarrow \text{Progress}$$

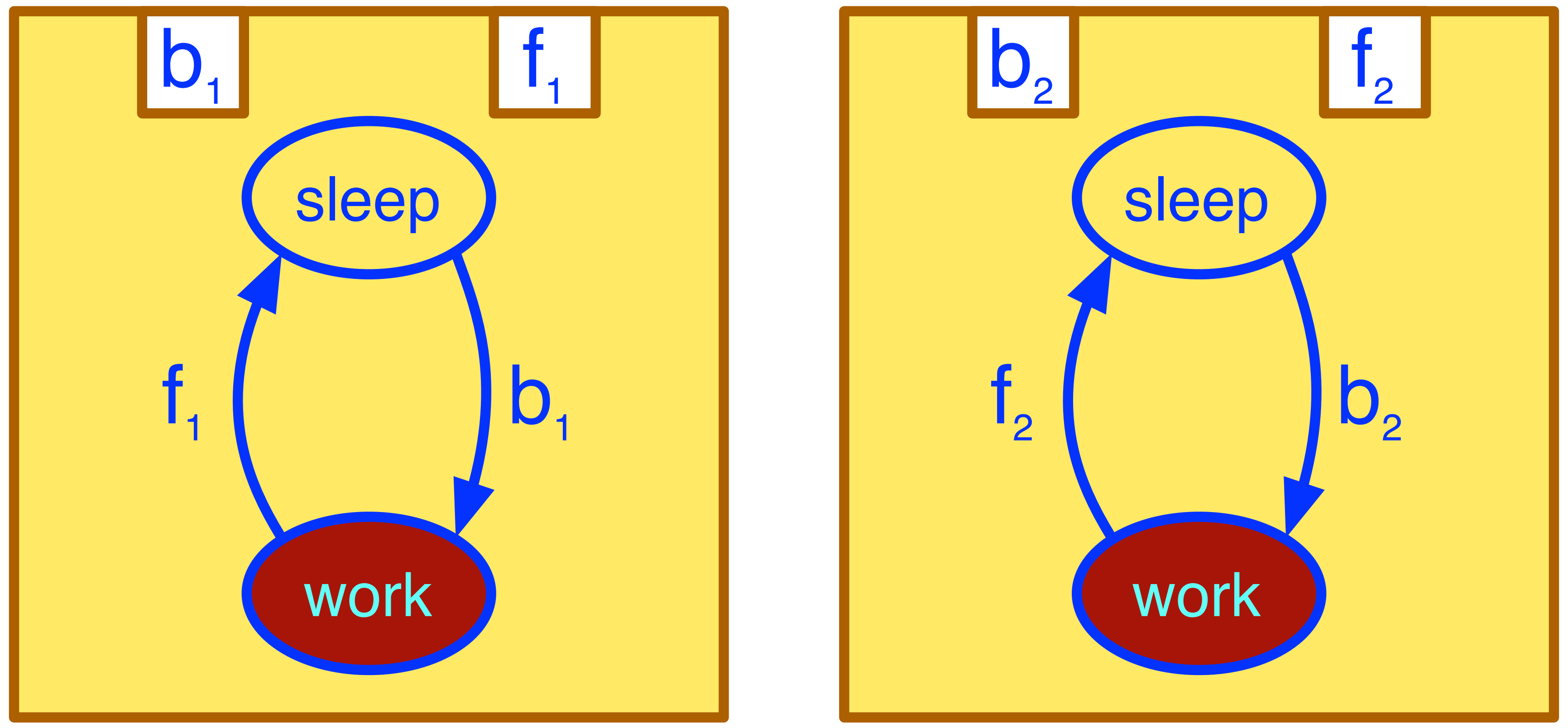
$$= \Big(\overline{\dot a}\,\overline{\dot r}\,\overline{\dot u}\,\overline{\dot m}\,\dot s\, f \vee \overline{f}\,\overline{\dot s}\,\overline{\dot a}\,\overline{\dot r}\,\dot u\,\overline{\dot m} \vee \overline{f}\,\overline{\dot s}\,\overline{\dot a}\,\overline{\dot r}\,\dot u\,\dot m \vee \overline{f}\,\overline{\dot s}\,\overline{\dot a}\,\overline{\dot r}\,\overline{\dot u}\,\dot m$$

$$\vee\, \overline{f}\,\overline{\dot s}\,\overline{\dot a}\,\dot r\,\dot u\,\dot m \vee \overline{b}\,\overline{h}\,\overline{f}\,\overline{\dot s}\,\dot a\,\overline{\dot r}\,\dot u\,\dot m\Big) \wedge \overline{\dot h}\,\overline{\dot b}\,\overline{\dot f}$$

Safety constraints

Shall not advance and rotate at the same time	$\overline{\dot a\,\dot r}$
Shall not leave the region	$b \Rightarrow \overline{\dot a}$
Shall not drive into hot areas	$h \Rightarrow \overline{\dot a}$
Shall update navigation and sensor data at each move	$\dot a \vee \dot r \Rightarrow \dot u\,\dot m$
Shall objective is found, must stop and transmit it's coordinates	$f \Rightarrow \overline{\dot a}\,\overline{\dot r}\,\overline{\dot u}\,\overline{\dot m}\,\dot s$
Shall transmit coordinates only when objective is reached	$\dot s \Rightarrow f$

Revisiting mutual exclusion (1/4)



Mutual exclusion:

One task can enter the critical state if the other is in the non-critical one or leaves the critical state simultaneously

The two tasks cannot enter the critical states simultaneously

$$\left(\dot{b}_1 \Rightarrow \overline{f_2} \vee \dot{f}_2\right)\left(\dot{b}_2 \Rightarrow \overline{f_1} \vee \dot{f}_1\right)\left(\overline{\dot{b}_1 \dot{b}_2}\right)\left(\overline{\dot{b}_1} \vee \overline{\dot{f}_1}\right)\left(\overline{\dot{b}_2} \vee \overline{\dot{f}_2}\right)$$

$$= \left(\overline{\dot{b}_1} \vee \overline{f_2} \vee \dot{f}_2\right)\left(\overline{\dot{b}_2} \vee \overline{f_1} \vee \dot{f}_1\right)\left(\overline{\dot{b}_1} \vee \overline{\dot{b}_2}\right)(\dots)(\dots)$$

$$= \overline{\dot{b}_1}\left(\overline{\dot{b}_2} \vee \overline{f_1} \vee \dot{f}_1\right)\left(\overline{\dot{b}_2} \vee \overline{\dot{f}_2}\right) \vee \overline{\dot{b}_2}\left(\overline{\dot{b}_1} \vee \overline{f_2} \vee \dot{f}_2\right)\left(\overline{\dot{b}_1} \vee \overline{\dot{f}_1}\right)$$

$$= \overline{\dot{b}_1}\,\overline{\dot{f}_2}\left(\overline{f_1} \vee \dot{f}_1\right) \vee \overline{\dot{b}_2}\,\overline{\dot{f}_2}\left(\overline{f_2} \vee \dot{f}_2\right) \vee \overline{\dot{b}_1}\,\overline{\dot{b}_2}$$

Revisiting mutual exclusion

$$\left(\dot b_1 \Rightarrow \overline{f_2} \vee \dot f_2\right)\left(\dot b_2 \Rightarrow \overline{f_1} \vee \dot f_1\right)\left(\overline{\dot b_1 \dot b_2}\right)\color{red}{\left(\overline{\dot b_1} \vee \overline{\dot f_1}\right)\left(\overline{\dot b_2} \vee \overline{\dot f_2}\right)}$$

$$= \left(\overline{\dot b_1} \vee \overline{f_2} \vee \dot f_2\right)\left(\overline{\dot b_2} \vee \overline{f_1} \vee \dot f_1\right)\left(\overline{\dot b_1} \vee \overline{\dot b_2}\right)\color{red}{(\dots)(\dots)}$$

$$= \overline{\dot b_1}\left(\overline{\dot b_2} \vee \overline{f_1} \vee \dot f_1\right)\left(\overline{\dot b_2} \vee \overline{\dot f_2}\right) \vee \overline{\dot b_2}\left(\overline{\dot b_1} \vee \overline{f_2} \vee \dot f_2\right)\left(\overline{\dot b_1} \vee \overline{\dot f_1}\right)$$

$$= \overline{\dot b_1}\,\overline{\dot f_2}\left(\overline{f_1} \vee \dot f_1\right) \vee \overline{\dot b_2}\,\overline{\dot f_2}\left(\overline{f_2} \vee \dot f_2\right) \vee \overline{\dot b_1}\,\overline{\dot b_2}$$

Revisiting mutual exclusion

$$\left(\dot b_1 \Rightarrow \overline{f_2} \vee \dot f_2\right) \left(\dot b_2 \Rightarrow \overline{f_1} \vee \dot f_1\right) \left(\overline{\dot b_1 \dot b_2}\right) \color{red}{\left(\overline{\dot b_1} \vee \overline{\dot f_1}\right) \left(\overline{\dot b_2} \vee \overline{\dot f_2}\right)}$$

$$= \left(\overline{\dot b_1} \vee \overline{f_2} \vee \dot f_2\right) \left(\overline{\dot b_2} \vee \overline{f_1} \vee \dot f_1\right) \left(\overline{\dot b_1} \vee \overline{\dot b_2}\right) \color{red}{(\ldots)(\ldots)}$$

$$= \overline{\dot b_1} \left(\overline{\dot b_2} \vee \overline{f_1} \vee \dot f_1\right) \left(\overline{\dot b_2} \vee \overline{\dot f_2}\right) \vee \overline{\dot b_2} \left(\overline{\dot b_1} \vee \overline{f_2} \vee \dot f_2\right) \left(\overline{\dot b_1} \vee \overline{\dot f_1}\right)$$

$$= \boxed{\overline{\dot b_1}\, \overline{\dot f_2} \left(\overline{f_1} \vee \dot f_1\right)} \vee \overline{\dot b_2}\, \overline{\dot f_2} \left(\overline{f_2} \vee \dot f_2\right) \vee \overline{\dot b_1}\, \overline{\dot b_2}$$

Revisiting mutual exclusion

$$\left(\dot{b}_1 \Rightarrow \overline{f_2} \vee \dot{f}_2\right)\left(\dot{b}_2 \Rightarrow \overline{f_1} \vee \dot{f}_1\right)\left(\overline{\dot{b}_1 \dot{b}_2}\right)\left(\overline{\dot{b}_1} \vee \overline{\dot{f}_1}\right)\left(\overline{\dot{b}_2} \vee \overline{\dot{f}_2}\right)$$

$$= \left(\overline{\dot{b}_1} \vee \overline{f_2} \vee \dot{f}_2\right)\left(\overline{\dot{b}_2} \vee \overline{f_1} \vee \dot{f}_1\right)\left(\overline{\dot{b}_1} \vee \overline{\dot{b}_2}\right)(\dots)(\dots)$$

$$= \overline{\dot{b}_1}\left(\overline{\dot{b}_2} \vee \overline{f_1} \vee \dot{f}_1\right)\left(\overline{\dot{b}_2} \vee \overline{\dot{f}_2}\right) \vee \overline{\dot{b}_2}\left(\overline{\dot{b}_1} \vee \overline{f_2} \vee \dot{f}_2\right)\left(\overline{\dot{b}_1} \vee \overline{\dot{f}_1}\right)$$

$$= \boxed{\overline{\dot{b}_1}\,\overline{\dot{f}_2}\left(\overline{f_1} \vee \dot{f}_1\right)} \vee \overline{\dot{b}_2}\,\overline{\dot{f}_2}\left(\overline{f_2} \vee \dot{f}_2\right) \vee \overline{\dot{b}_1}\,\overline{\dot{b}_2}$$

$$true \Rightarrow \overline{f_1} + \dot{f}_1\,,$$
$$\dot{b}_1 \Rightarrow false\,,$$
$$\dot{b}_2 \Rightarrow true\,,$$
$$\dot{f}_1 \Rightarrow true\,,$$
$$\dot{f}_2 \Rightarrow false$$

Revisiting mutual exclusion

$$\left(\dot b_1 \Rightarrow \overline{f_2} \vee \dot f_2\right)\left(\dot b_2 \Rightarrow \overline{f_1} \vee \dot f_1\right)\left(\overline{\dot b_1 \dot b_2}\right)\color{red}{\left(\overline{\dot b_1} \vee \overline{\dot f_1}\right)\left(\overline{\dot b_2} \vee \overline{\dot f_2}\right)}$$

$$= \left(\overline{\dot b_1} \vee \overline{f_2} \vee \dot f_2\right)\left(\overline{\dot b_2} \vee \overline{f_1} \vee \dot f_1\right)\left(\overline{\dot b_1} \vee \overline{\dot b_2}\right)\color{red}{(\dots)(\dots)}$$

$$= \overline{\dot b_1}\left(\overline{\dot b_2} \vee \overline{f_1} \vee \dot f_1\right)\left(\overline{\dot b_2} \vee \overline{\dot f_2}\right) \vee \overline{\dot b_2}\left(\overline{\dot b_1} \vee \overline{f_2} \vee \dot f_2\right)\left(\overline{\dot b_1} \vee \overline{\dot f_1}\right)$$

$$= \boxed{\overline{\dot b_1}\,\overline{\dot f_2}\left(\overline{f_1} \vee \dot f_1\right)} \vee \overline{\dot b_2}\,\overline{\dot f_2}\left(\overline{f_2} \vee \dot f_2\right) \vee \overline{\dot b_1}\,\overline{\dot b_2}$$

$$\begin{array}{ll}
true \Rightarrow \overline{f_1} + \dot f_1\,, & true \Rightarrow \overline{f_1} + \dot f_1\,, \\
\dot b_1 \Rightarrow false\,, & \dot b_1 \Rightarrow false\,, \\
\dot b_2 \Rightarrow true\,, & \dot b_2 \Rightarrow \overline{f_1} + \dot f_1\,, \\
\dot f_1 \Rightarrow true\,, & \dot f_1 \Rightarrow true\,, \\
\dot f_2 \Rightarrow false & \dot f_2 \Rightarrow false
\end{array}$$

Revisiting mutual exclusion

$$\left(\dot{b}_1 \Rightarrow \overline{f_2} \vee \dot{f}_2\right)\left(\dot{b}_2 \Rightarrow \overline{f_1} \vee \dot{f}_1\right)\left(\overline{\dot{b}_1 \dot{b}_2}\right)\color{red}{\left(\overline{\dot{b}_1} \vee \overline{\dot{f}_1}\right)\left(\overline{\dot{b}_2} \vee \overline{\dot{f}_2}\right)}$$

$$= \left(\overline{\dot{b}_1} \vee \overline{f_2} \vee \dot{f}_2\right)\left(\overline{\dot{b}_2} \vee \overline{f_1} \vee \dot{f}_1\right)\left(\overline{\dot{b}_1} \vee \overline{\dot{b}_2}\right)\color{red}{(\dots)(\dots)}$$

$$= \overline{\dot{b}_1}\left(\overline{\dot{b}_2} \vee \overline{f_1} \vee \dot{f}_1\right)\left(\overline{\dot{b}_2} \vee \overline{\dot{f}_2}\right) \vee \overline{\dot{b}_2}\left(\overline{\dot{b}_1} \vee \overline{f_2} \vee \dot{f}_2\right)\left(\overline{\dot{b}_1} \vee \overline{\dot{f}_1}\right)$$

$$= \boxed{\overline{\dot{b}_1}\,\overline{\dot{f}_2}\left(\overline{f_1} \vee \dot{f}_1\right)} \vee \overline{\dot{b}_2}\,\overline{\dot{f}_2}\left(\overline{f_2} \vee \dot{f}_2\right) \vee \overline{\dot{b}_1}\,\overline{\dot{b}_2}$$

$true \Rightarrow \overline{f_1} + \dot{f}_1\,,$	$true \Rightarrow \overline{f_1} + \dot{f}_1\,,$	$\overline{f_1}, \dot{f}_1,$
$\dot{b}_1 \Rightarrow false\,,$	$\dot{b}_1 \Rightarrow false\,,$	$/$
$\dot{b}_2 \Rightarrow true\,,$	$\dot{b}_2 \Rightarrow \overline{f_1} + \dot{f}_1\,,$	$\dot{b}_2\,\overline{f_1}, \dot{b}_2\,\dot{f}_1,$
$\dot{f}_1 \Rightarrow true\,,$	$\dot{f}_1 \Rightarrow true\,,$	$\dot{f}_1,$
$\dot{f}_2 \Rightarrow false$	$\dot{f}_2 \Rightarrow false$	$/$

Revisiting mutual exclusion

$$\left(\dot b_1 \Rightarrow \overline{f_2} \vee \dot f_2\right)\left(\dot b_2 \Rightarrow \overline{f_1} \vee \dot f_1\right)\left(\overline{\dot b_1 \dot b_2}\right)\left(\overline{\dot b_1} \vee \overline{\dot f_1}\right)\left(\overline{\dot b_2} \vee \overline{\dot f_2}\right)$$

$$= \left(\overline{\dot b_1} \vee \overline{f_2} \vee \dot f_2\right)\left(\overline{\dot b_2} \vee \overline{f_1} \vee \dot f_1\right)\left(\overline{\dot b_1} \vee \overline{\dot b_2}\right)(\dots)(\dots)$$

$$= \overline{\dot b_1}\left(\overline{\dot b_2} \vee \overline{f_1} \vee \dot f_1\right)\left(\overline{\dot b_2} \vee \overline{\dot f_2}\right) \vee \overline{\dot b_2}\left(\overline{\dot b_1} \vee \overline{f_2} \vee \dot f_2\right)\left(\overline{\dot b_1} \vee \overline{\dot f_1}\right)$$

$$= \boxed{\overline{\dot b_1}\,\overline{\dot f_2}\left(\overline{f_1} \vee \dot f_1\right)} \vee \overline{\dot b_2}\,\overline{\dot f_2}\left(\overline{f_2} \vee \dot f_2\right) \vee \overline{\dot b_1}\,\overline{\dot b_2}$$

$true \Rightarrow \overline{f_1} + \dot f_1\,,$	$true \Rightarrow \overline{f_1} + \dot f_1\,,$	$\overline{f_1}, \dot f_1,$
$\dot b_1 \Rightarrow false\,,$	$\dot b_1 \Rightarrow false\,,$	$/$
$\dot b_2 \Rightarrow true\,,$	$\dot b_2 \Rightarrow \overline{f_1} + \dot f_1\,,$	$\dot b_2\,\overline{f_1}, \dot b_2\,\dot f_1,$
$\dot f_1 \Rightarrow true\,,$	$\dot f_1 \Rightarrow true\,,$	$\dot f_1,$
$\dot f_2 \Rightarrow false$	$\dot f_2 \Rightarrow false$	$/$

$$\begin{matrix}\overline{f_1} & & \dot f_1 \\ \downarrow & \oplus & \downarrow \\ \dot b_2 & & \dot b_2\end{matrix}$$

Revisiting mutual exclusion

$$\left(\dot{b}_1 \Rightarrow \overline{f_2} \vee \dot{f}_2\right)\left(\dot{b}_2 \Rightarrow \overline{f_1} \vee \dot{f}_1\right)\left(\overline{\dot{b}_1 \dot{b}_2}\right)\left(\overline{\dot{b}_1} \vee \overline{\dot{f}_1}\right)\left(\overline{\dot{b}_2} \vee \overline{\dot{f}_2}\right)$$

$$= \left(\overline{\dot{b}_1} \vee \overline{f_2} \vee \dot{f}_2\right)\left(\overline{\dot{b}_2} \vee \overline{f_1} \vee \dot{f}_1\right)\left(\overline{\dot{b}_1} \vee \overline{\dot{b}_2}\right)(\ldots)(\ldots)$$

$$= \overline{\dot{b}_1}\left(\overline{\dot{b}_2} \vee \overline{f_1} \vee \dot{f}_1\right)\left(\overline{\dot{b}_2} \vee \overline{\dot{f}_2}\right) \vee \overline{\dot{b}_2}\left(\overline{\dot{b}_1} \vee \overline{f_2} \vee \dot{f}_2\right)\left(\overline{\dot{b}_1} \vee \overline{\dot{f}_1}\right)$$

$$= \boxed{\overline{\dot{b}_1}\,\overline{\dot{f}_2}\left(\overline{f_1} \vee \dot{f}_1\right)} \vee \overline{\dot{b}_2}\,\overline{\dot{f}_2}\left(\overline{f_2} \vee \dot{f}_2\right) \vee \overline{\dot{b}_1}\,\overline{\dot{b}_2}$$

$$\begin{array}{lll}
true \Rightarrow \overline{f_1} + \dot{f}_1\,, & true \Rightarrow \overline{f_1} + \dot{f}_1\,, & \overline{f_1}, \dot{f}_1, \\
\dot{b}_1 \Rightarrow false\,, & \dot{b}_1 \Rightarrow false\,, & / \\
\dot{b}_2 \Rightarrow true\,, & \dot{b}_2 \Rightarrow \overline{f_1} + \dot{f}_1\,, & \dot{b}_2\,\overline{f_1}, \dot{b}_2\,\dot{f}_1, \\
\dot{f}_1 \Rightarrow true\,, & \dot{f}_1 \Rightarrow true\,, & \dot{f}_1, \\
\dot{f}_2 \Rightarrow false & \dot{f}_2 \Rightarrow false & /
\end{array}$$

$$\begin{array}{c} \overline{f_1} \\ \downarrow \\ \dot{b}_2 \end{array} \oplus \begin{array}{c} \dot{f}_1 \\ \downarrow \\ \dot{b}_2 \end{array}$$

$$\dot{b}_2\,\overline{f_1} \oplus \begin{array}{c} \dot{f}_1 \\ \downarrow \\ \dot{b}_2 \end{array}$$

Revisiting mutual exclusion (3/4)

$$\left(\dot{b}_1 \Rightarrow \overline{f_2} \vee \dot{f}_2\right)\left(\dot{b}_2 \Rightarrow \overline{f_1} \vee \dot{f}_1\right)\left(\overline{\dot{b}_1 \dot{b}_2}\right)\color{red}{\left(\overline{\dot{b}_1} \vee \overline{\dot{f}_1}\right)\left(\overline{\dot{b}_2} \vee \overline{\dot{f}_2}\right)}$$

$$= \left(\overline{\dot{b}_1} \vee \overline{f_2} \vee \dot{f}_2\right)\left(\overline{\dot{b}_2} \vee \overline{f_1} \vee \dot{f}_1\right)\left(\overline{\dot{b}_1} \vee \overline{\dot{b}_2}\right)\color{red}{(\dots)(\dots)}$$

$$= \overline{\dot{b}_1}\left(\overline{\dot{b}_2} \vee \overline{f_1} \vee \dot{f}_1\right)\left(\overline{\dot{b}_2} \vee \overline{\dot{f}_2}\right) \vee \overline{\dot{b}_2}\left(\overline{\dot{b}_1} \vee \overline{f_2} \vee \dot{f}_2\right)\left(\overline{\dot{b}_1} \vee \overline{\dot{f}_1}\right)$$

$$= \overline{\dot{b}_1}\,\overline{\dot{f}_2}\left(\overline{f_1} \vee \dot{f}_1\right) \vee \overline{\dot{b}_2}\,\overline{\dot{f}_2}\left(\overline{f_2} \vee \dot{f}_2\right) \vee \boxed{\overline{\dot{b}_1}\,\overline{\dot{b}_2}}$$

Revisiting mutual exclusion (3/4)

$$\left(\dot{b}_1 \Rightarrow \overline{f_2} \vee \dot{f}_2\right)\left(\dot{b}_2 \Rightarrow \overline{f_1} \vee \dot{f}_1\right)\left(\overline{\dot{b}_1 \dot{b}_2}\right) {\color{red}\left(\overline{\dot{b}_1} \vee \overline{\dot{f}_1}\right)\left(\overline{\dot{b}_2} \vee \overline{\dot{f}_2}\right)}$$

$$= \left(\overline{\dot{b}_1} \vee \overline{f_2} \vee \dot{f}_2\right)\left(\overline{\dot{b}_2} \vee \overline{f_1} \vee \dot{f}_1\right)\left(\overline{\dot{b}_1} \vee \overline{\dot{b}_2}\right) {\color{red}(\dots)(\dots)}$$

$$= \overline{\dot{b}_1}\left(\overline{\dot{b}_2} \vee \overline{f_1} \vee \dot{f}_1\right)\left(\overline{\dot{b}_2} \vee \overline{\dot{f}_2}\right) \vee \overline{\dot{b}_2}\left(\overline{\dot{b}_1} \vee \overline{f_2} \vee \dot{f}_2\right)\left(\overline{\dot{b}_1} \vee \overline{\dot{f}_1}\right)$$

$$= \overline{\dot{b}_1}\,\overline{\dot{f}_2}\left(\overline{f_1} \vee \dot{f}_1\right) \vee \overline{\dot{b}_2}\,\overline{\dot{f}_2}\left(\overline{f_2} \vee \dot{f}_2\right) \vee \boxed{\overline{\dot{b}_1}\,\overline{\dot{b}_2}}$$

$$true \Rightarrow true\,,$$

$$\dot{b}_1 \Rightarrow false\,,$$

$$\dot{b}_2 \Rightarrow false\,,$$

$$\dot{f}_1 \Rightarrow true\,,$$

$$\dot{f}_2 \Rightarrow true$$

Revisiting mutual exclusion (3/4)

$$\left(\dot b_1 \Rightarrow \overline{f_2} \vee \dot f_2\right)\left(\dot b_2 \Rightarrow \overline{f_1} \vee \dot f_1\right)\left(\overline{\dot b_1 \dot b_2}\right)\color{red}{\left(\overline{\dot b_1} \vee \overline{\dot f_1}\right)\left(\overline{\dot b_2} \vee \overline{\dot f_2}\right)}$$

$$= \left(\overline{\dot b_1} \vee \overline{f_2} \vee \dot f_2\right)\left(\overline{\dot b_2} \vee \overline{f_1} \vee \dot f_1\right)\left(\overline{\dot b_1} \vee \overline{\dot b_2}\right)\color{red}{(\ldots)(\ldots)}$$

$$= \overline{\dot b_1}\left(\overline{\dot b_2} \vee \overline{f_1} \vee \dot f_1\right)\left(\overline{\dot b_2} \vee \overline{\dot f_2}\right) \vee \overline{\dot b_2}\left(\overline{\dot b_1} \vee \overline{f_2} \vee \dot f_2\right)\left(\overline{\dot b_1} \vee \overline{\dot f_1}\right)$$

$$= \overline{\dot b_1}\,\overline{\dot f_2}\left(\overline{f_1} \vee \dot f_1\right) \vee \overline{\dot b_2}\,\overline{\dot f_2}\left(\overline{f_2} \vee \dot f_2\right) \vee \boxed{\overline{\dot b_1}\,\overline{\dot b_2}}$$

$$\begin{array}{rcll} true & \Rightarrow & true\,, & / \\ \dot b_1 & \Rightarrow & false\,, & / \\ \dot b_2 & \Rightarrow & false\,, & / \\ \dot f_1 & \Rightarrow & true\,, & \dot f_1\,, \\ \dot f_2 & \Rightarrow & true & \dot f_2 \end{array}$$

Revisiting mutual exclusion (3/4)

$$\left(\dot{b}_1 \Rightarrow \overline{f_2} \vee \dot{f}_2\right)\left(\dot{b}_2 \Rightarrow \overline{f_1} \vee \dot{f}_1\right)\left(\overline{\dot{b}_1 \dot{b}_2}\right)\left(\overline{\dot{b}_1} \vee \overline{\dot{f}_1}\right)\left(\overline{\dot{b}_2} \vee \overline{\dot{f}_2}\right)$$

$$= \left(\overline{\dot{b}_1} \vee \overline{f_2} \vee \dot{f}_2\right)\left(\overline{\dot{b}_2} \vee \overline{f_1} \vee \dot{f}_1\right)\left(\overline{\dot{b}_1} \vee \overline{\dot{b}_2}\right)(\dots)(\dots)$$

$$= \overline{\dot{b}_1}\left(\overline{\dot{b}_2} \vee \overline{f_1} \vee \dot{f}_1\right)\left(\overline{\dot{b}_2} \vee \overline{\dot{f}_2}\right) \vee \overline{\dot{b}_2}\left(\overline{\dot{b}_1} \vee \overline{f_2} \vee \dot{f}_2\right)\left(\overline{\dot{b}_1} \vee \overline{\dot{f}_1}\right)$$

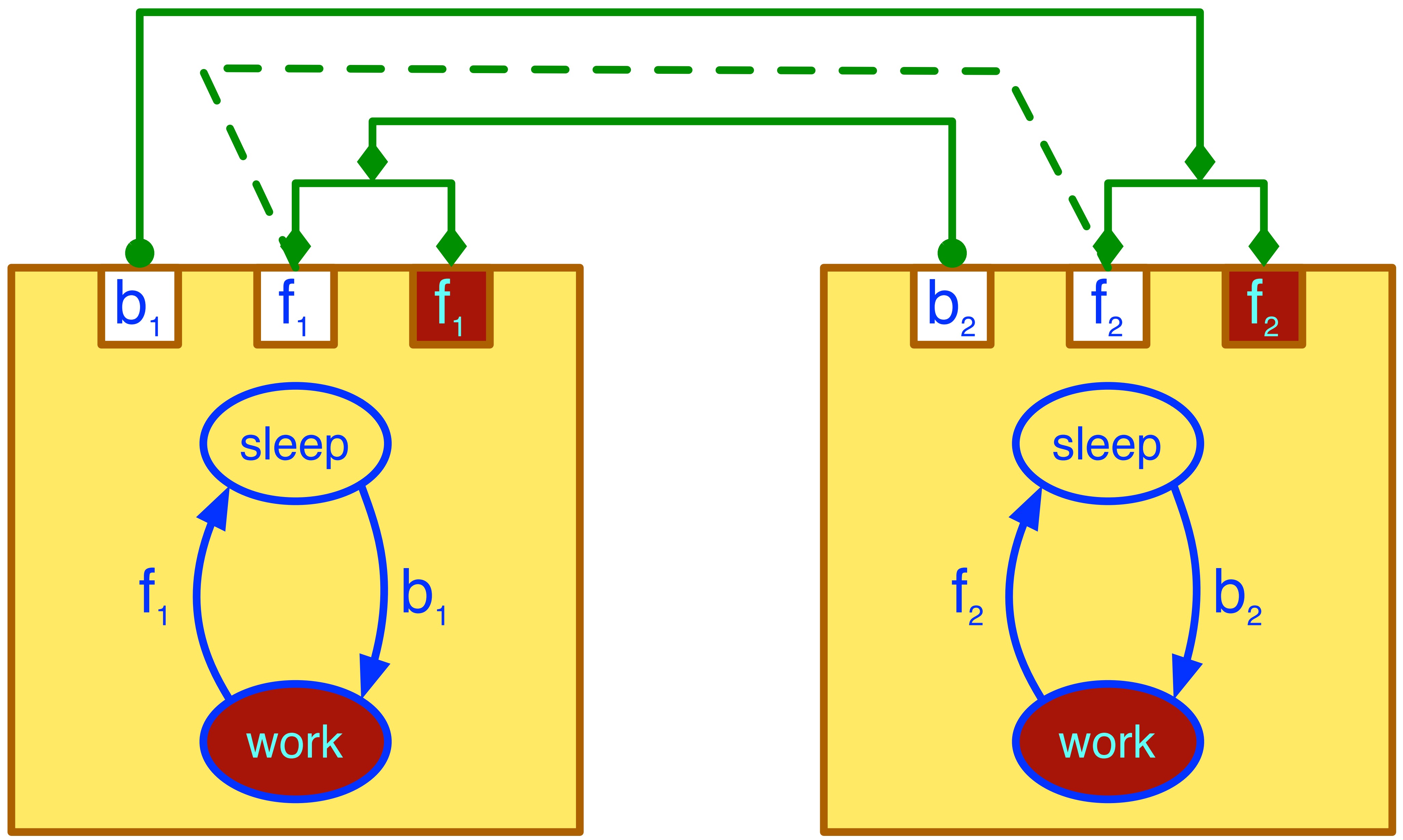
$$= \overline{\dot{b}_1}\,\overline{\dot{f}_2}\left(\overline{f_1} \vee \dot{f}_1\right) \vee \overline{\dot{b}_2}\,\overline{\dot{f}_2}\left(\overline{f_2} \vee \dot{f}_2\right) \vee \boxed{\overline{\dot{b}_1}\,\overline{\dot{b}_2}}$$

$true \Rightarrow true\,,$	$/$	
$\dot{b}_1 \Rightarrow false\,,$	$/$	
$\dot{b}_2 \Rightarrow false\,,$	$/$	$\dot{f}_1 \oplus \dot{f}_2$
$\dot{f}_1 \Rightarrow true\,,$	$\dot{f}_1\,,$	
$\dot{f}_2 \Rightarrow true$	$\dot{f}_2$	

Revisiting mutual exclusion (4/4)

$$\dot{f}_1 \oplus \dot{f}_2 \qquad \dot{b}_2\,\overline{f_1} \oplus \begin{array}{c}\dot{f}_1\\ \downarrow\\ \dot{b}_2\end{array} \qquad \dot{b}_1\,\overline{f_2} \oplus \begin{array}{c}\dot{f}_2\\ \downarrow\\ \dot{b}_1\end{array}$$

$$\dot{f}_1{}'\,\dot{f}_2{}' + \left[\dot{b}_2\,\overline{f_1}\right]'\left[\dot{f}_1{}'\,\dot{b}_2\right]' + \left[\dot{b}_1\,\overline{f_2}\right]'\left[\dot{f}_2{}'\,\dot{b}_1\right]' \simeq \dot{f}_1{}'\,\dot{f}_2{}' + \dot{b}_2\left[\overline{f_1}'\,\dot{f}_1{}'\right] + \dot{b}_1\left[\overline{f_2}'\,\dot{f}_2{}'\right]$$



Expressiveness of BIP

What is this?

Expressiveness of BIP

Component-based frameworks

$$C ::= B \mid f(C_1, \ldots, C_n)\,, \qquad \text{with } B \in \mathcal{B}, f \in \mathcal{G}$$

Behaviour   Glue

$\mathcal{A}$ — the set of all components

$\sigma : \mathcal{A} \to \mathcal{B}$ — a semantic mapping

$\simeq\ \subseteq \mathcal{A} \times \mathcal{A}$ — an equivalence relation

$$\sigma(B) = B \qquad \sigma(C_1) = \sigma(C_2) \implies C_1 \simeq C_2$$

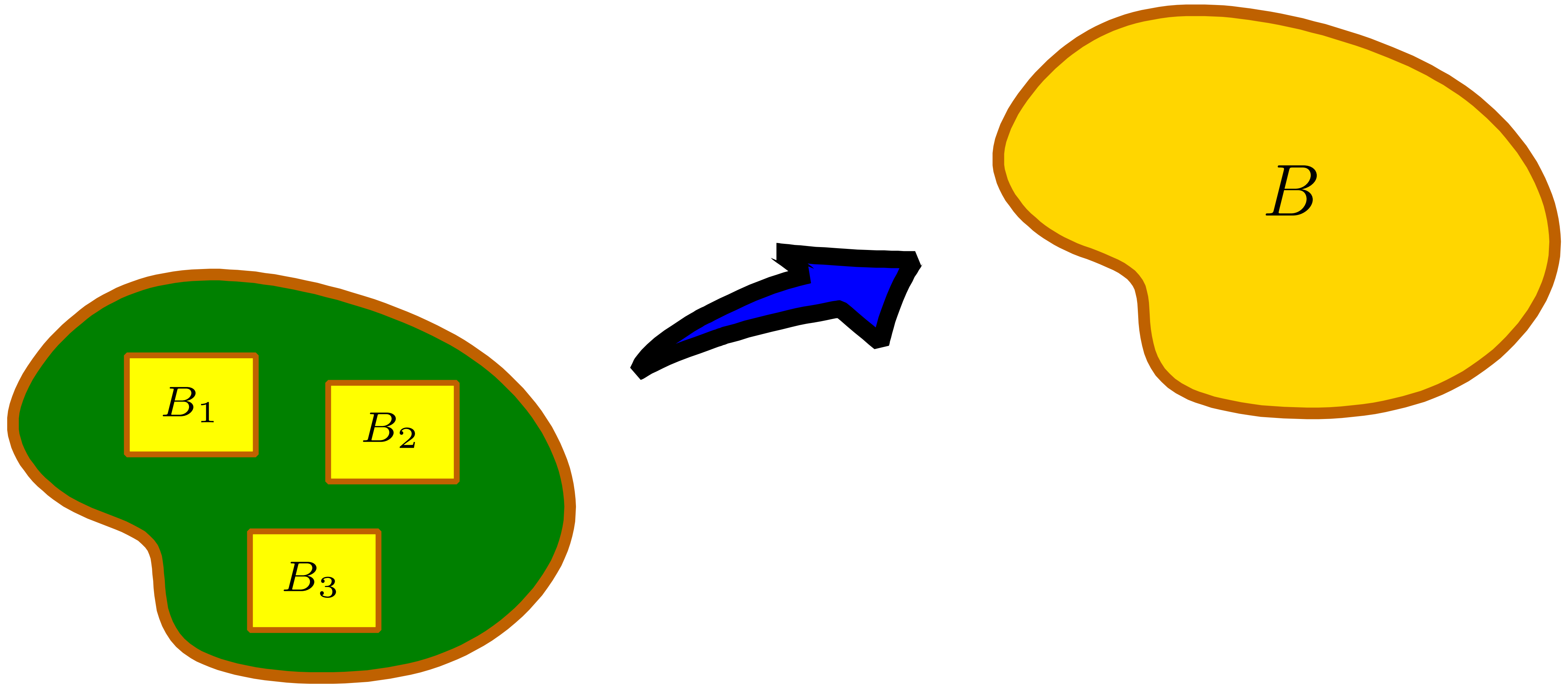
Expressiveness

Absolute:

What behaviours can be obtained?

Let $id \in \mathcal{G}\,, \qquad \sigma(\mathcal{A}) = \mathcal{B}$:

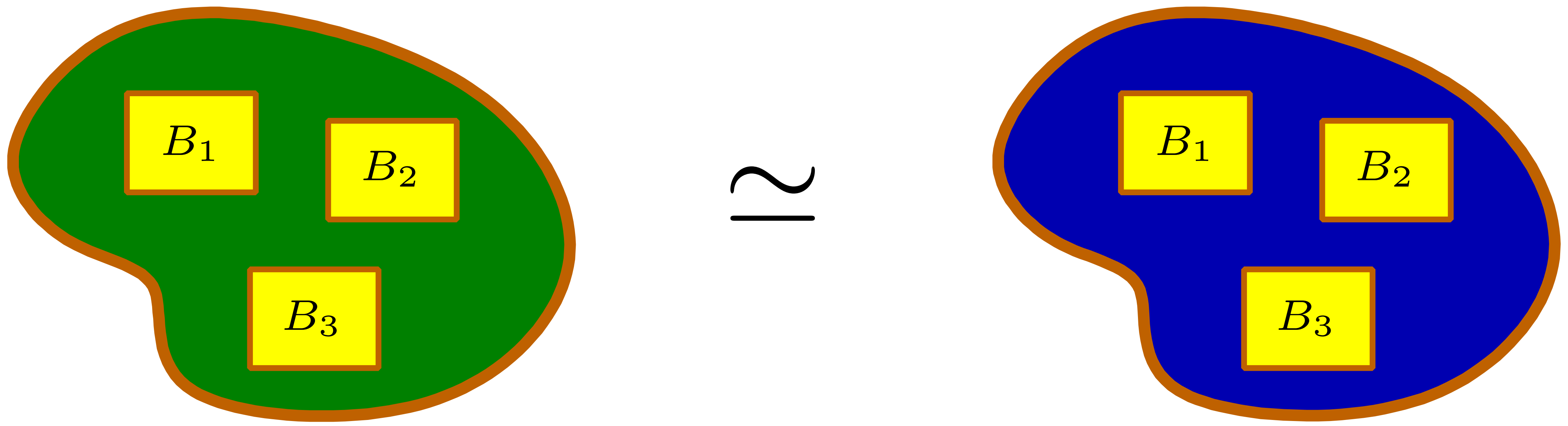
$$\sigma(\mathcal{A}) \subseteq \mathcal{B} = id(\mathcal{B}) \subseteq \sigma(\mathcal{B}) \subseteq \sigma(\mathcal{A})$$



Relative:

Are there “good” language encodings?

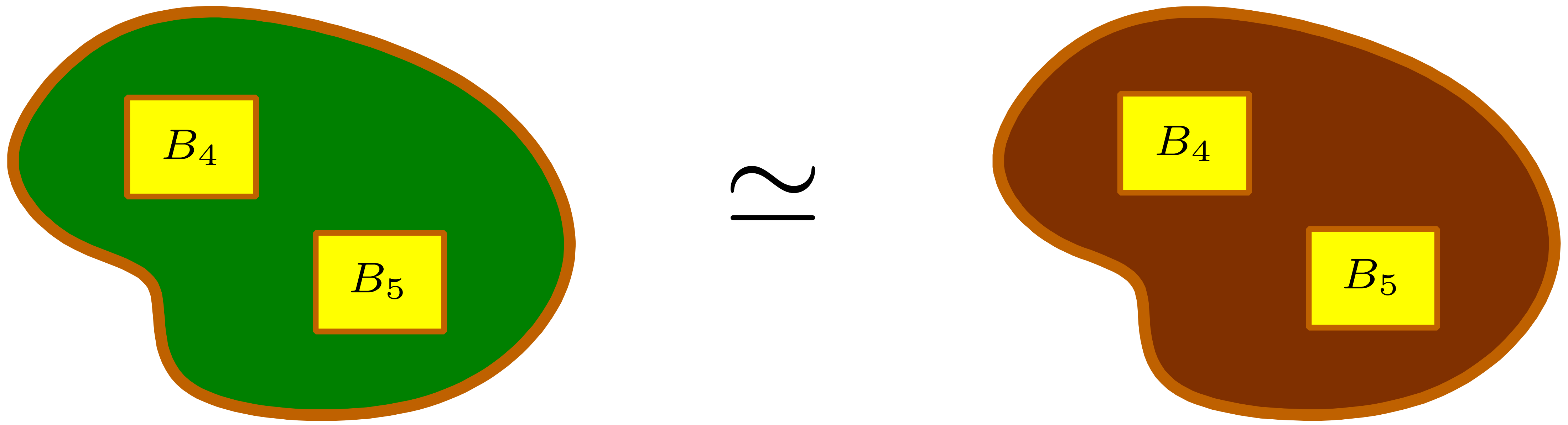
Felleisen [’90], Gorla [’08, ’10]



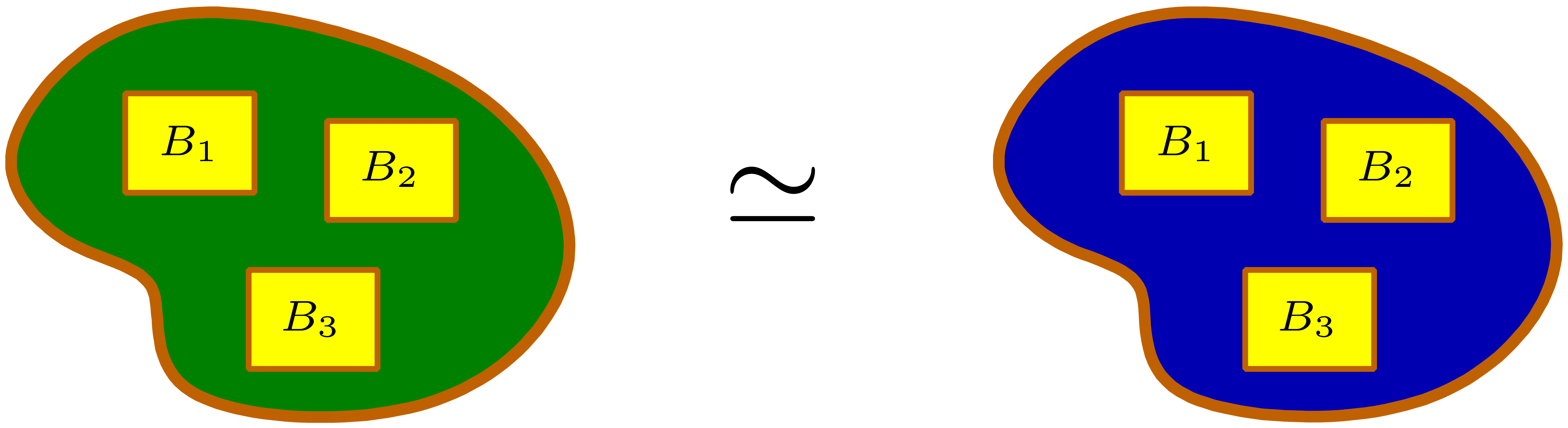
Coordination:

Relative approach *with fixed atomic components.*

This work and [CONCUR’08]



Strong full expressiveness

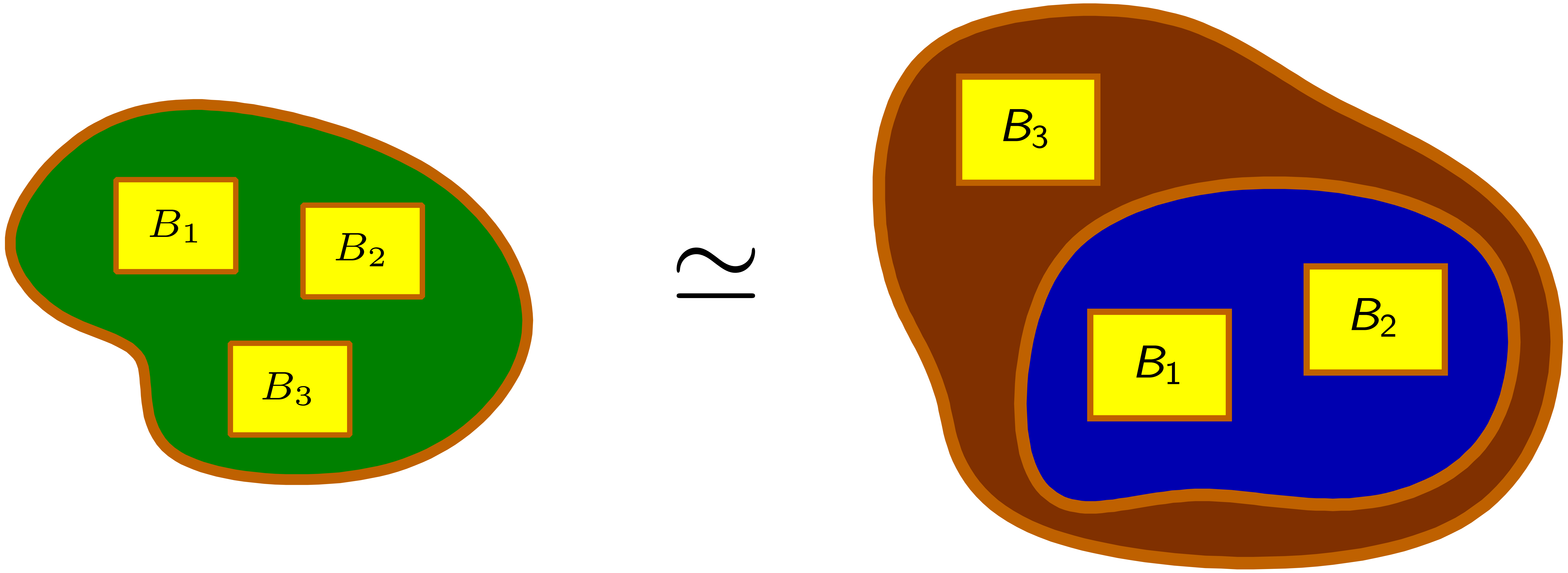


$$\mathcal{O} \subseteq \bigcup_{n=0}^{\infty} (\mathcal{B}^n \to \mathcal{B})$$

$$\forall o \in \mathcal{O}^n,\ \exists \tilde{o} \in \mathcal{G} :\ \forall B_1, \dots, B_n \in \mathcal{B},$$

$$\sigma\big(\tilde{o}(B_1, \dots, B_n)\big) = o(B_1, \dots, B_n)$$

Weak full expressiveness



$$\mathcal{O} \subseteq \bigcup_{n=0}^{\infty} (\mathcal{B}^n \to \mathcal{B})$$

$$\forall o \in \mathcal{O}^n,\ \exists \tilde{o} \in \mathcal{G}[Z_1, \dots, Z_n] :\ \forall B_1, \dots, B_n \in \mathcal{B},$$
$$\sigma\big(\tilde{o}[B_1/Z_1, \dots, B_n/Z_n]\big) = o(B_1, \dots, B_n)$$

Expressiveness of BIP

Semantics

$$B_i = (Q_i, P_i, \to_i), \qquad \to_i \subseteq Q_i \times 2^{P_i} \times Q_i, \qquad P = \dot{\bigcup_i} P_i$$

Interaction model: $\gamma \subseteq 2^P$ — a set of allowed interactions

$$\frac{q_i \xrightarrow{a \cap P_i} q_i' \ (\text{if } a \cap P_i \neq \emptyset) \quad q_i = q_i' \ (\text{if } a \cap P_i = \emptyset)}{q_1 \dots q_n \xrightarrow{a} q_1' \dots q_n'}$$

for each $a \in \gamma$.

Priority model: $\prec \subseteq \gamma \times \gamma$ — strict partial order

$$\frac{q \xrightarrow{a} q' \qquad \forall a \prec a',\ q \not\xrightarrow{a'}}{q \xrightarrow{a}_{\prec} q'}$$

for each $a \in 2^P$.

The question

Does BIP glue…

- interactions
- priorities

…have full expressiveness w.r.t. BIP-like SOS operators?

$$\frac{\left\{q_i \xrightarrow{a\cap P_i} q_i' \,\middle|\, i \in I\right\} \quad \left\{q_i = q_i' \,\middle|\, i \notin I\right\} \quad \left\{q_j \stackrel{b_j^k}{\not\longrightarrow} \,\middle|\, j \in J, k \in K_j\right\}}{q_1 \dots q_n \xrightarrow{a} q_1' \dots q_n'}$$

Restrictions on priority models

Only interactions in the interaction model can be used

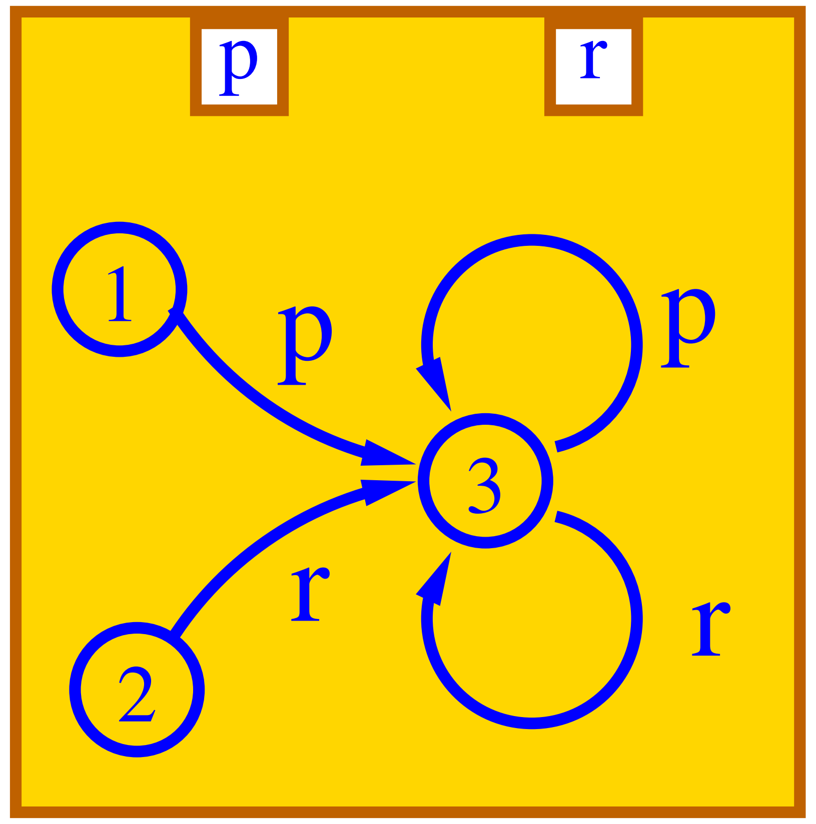
$$\prec \subseteq \gamma \times \gamma$$

Priority is a strict partial order on interactions

- transitive
- irreflexive
- (hence also) antisymmetric

Corollary (Sifakis, Gößler, 2003): BIP priorities cannot introduce deadlocks

Blocking with BIP-like SOS rules



$$\frac{q_1 \xrightarrow{p} q_1' \qquad q_1 \stackrel{r}{\not\longrightarrow}}{q_1 \xrightarrow{p} q_1'} \qquad\qquad \frac{q_1 \xrightarrow{r} q_1' \qquad q_1 \stackrel{p}{\not\longrightarrow}}{q_1 \xrightarrow{r} q_1'}$$

Relaxing the priority model

Strict partial order $\prec \subseteq 2^P \times 2^P$

Arbitrary relation $\prec \subseteq \gamma \times \gamma$

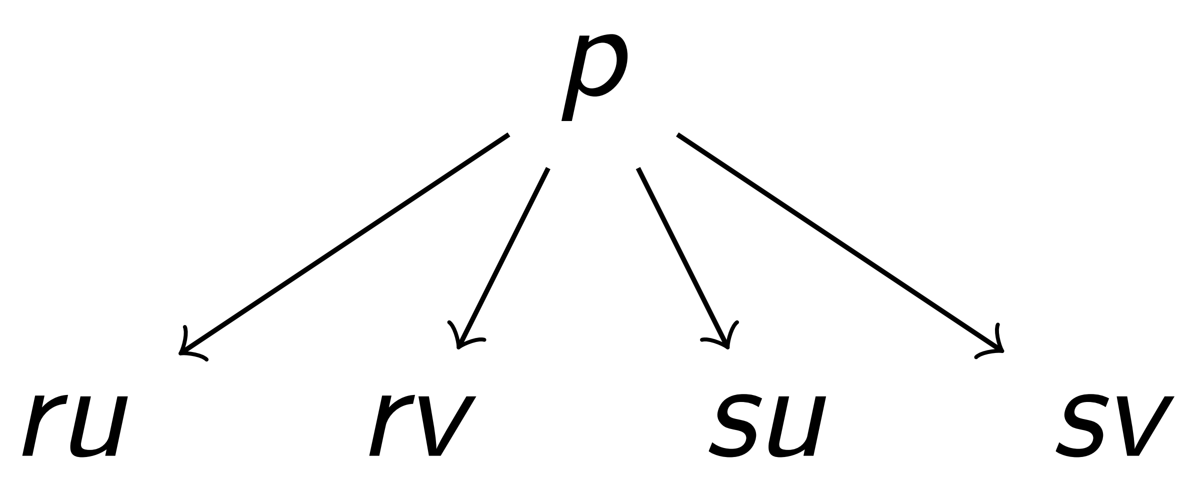
Arbitrary relation $\prec \subseteq 2^P \times 2^P$

Alternatively, restrict the set of reference operators

Inhibiting relation

$$\frac{q_1 \xrightarrow{p} q_1' \quad q_2 \not\xrightarrow{r} \quad q_3 \not\xrightarrow{s}}{q_1 q_2 q_3 \xrightarrow{p} q_1' q_2 q_3} \qquad \frac{q_1 \xrightarrow{p} q_1' \quad q_2 \not\xrightarrow{u} \quad q_3 \not\xrightarrow{v}}{q_1 q_2 q_3 \xrightarrow{p} q_1' q_2 q_3}$$

$$\begin{aligned} p \wedge (\overline{r}\,\overline{s} \vee \overline{u}\,\overline{v}) &\equiv p \wedge \overline{(r \vee s) \wedge (u \vee v)} \\ &\equiv p \wedge \overline{(ru \wedge rv \wedge su \wedge sv)} \end{aligned}$$

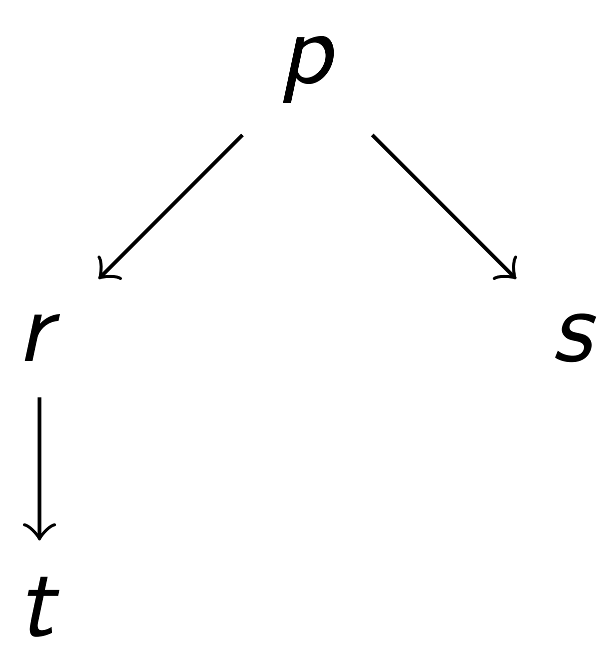


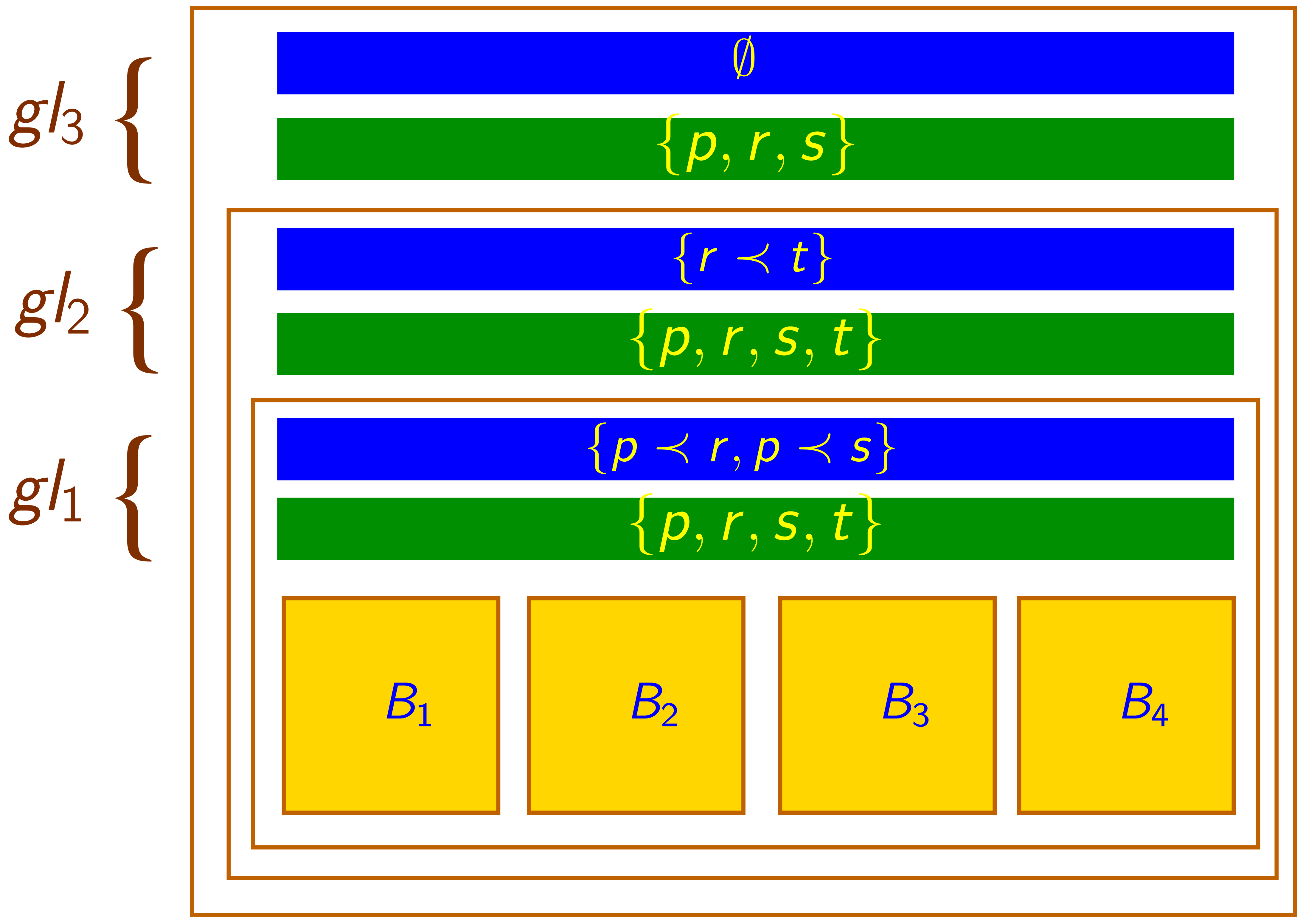
A relation on the set of all interactions

may not be a strict partial order; may involve interactions not in the model

Example: DAG inhibiting relation

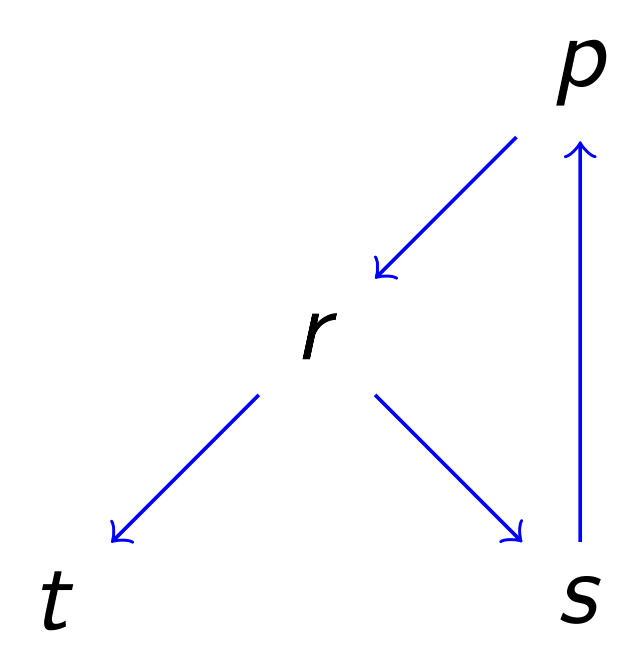
$$\frac{q_1 \xrightarrow{p} q_1' \qquad q_2 \not\xrightarrow{r} \qquad q_3 \not\xrightarrow{s}}{q_1q_2q_3q_4 \xrightarrow{p} q_1'q_2q_3q_4} \qquad \frac{q_2 \xrightarrow{r} q_2' \qquad q_4 \not\xrightarrow{t}}{q_1q_2q_3q_4 \xrightarrow{r} q_1q_2'q_3q_4} \qquad \frac{q_3 \xrightarrow{s} q_3'}{q_1q_2q_3q_4 \xrightarrow{s} q_1q_2q_3'q_4}$$

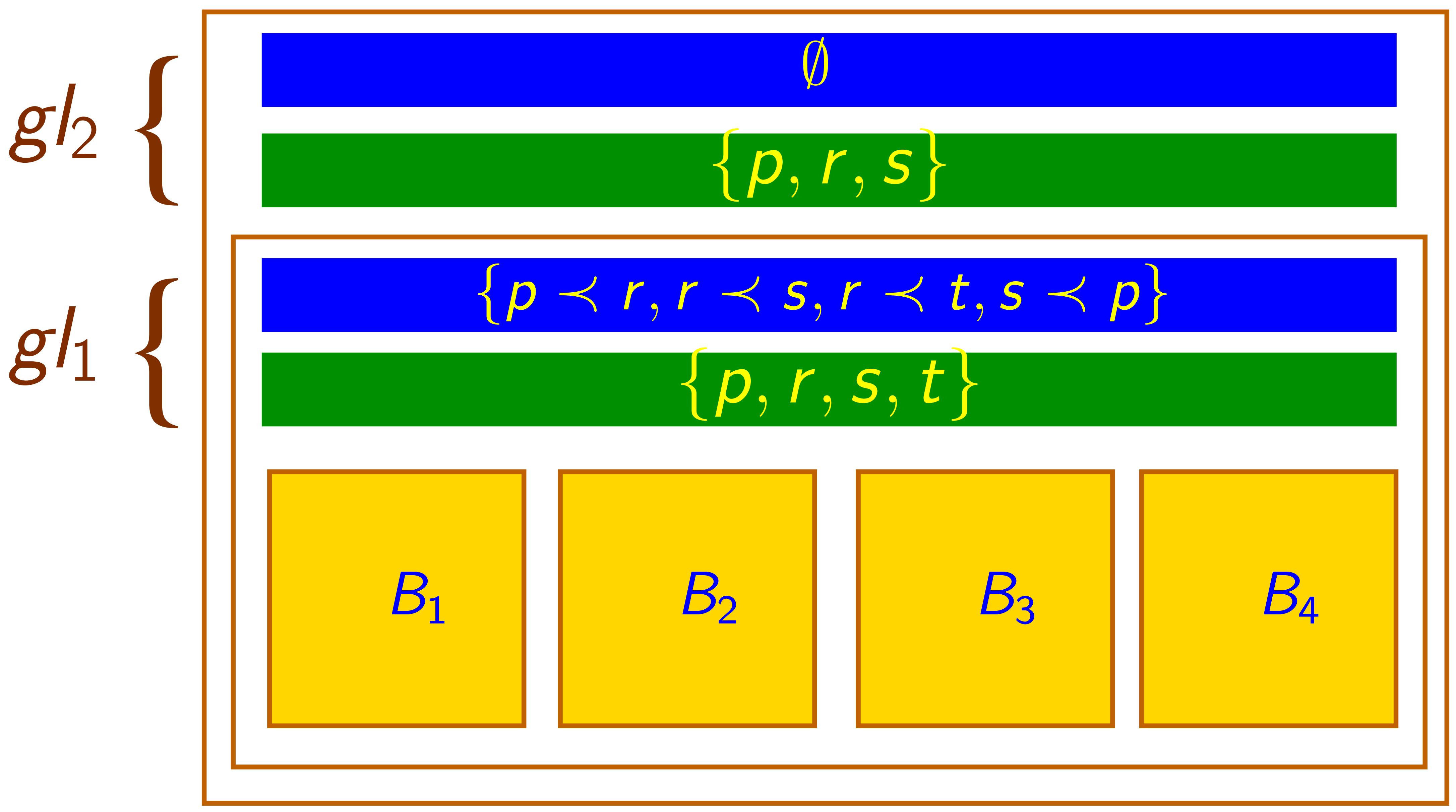




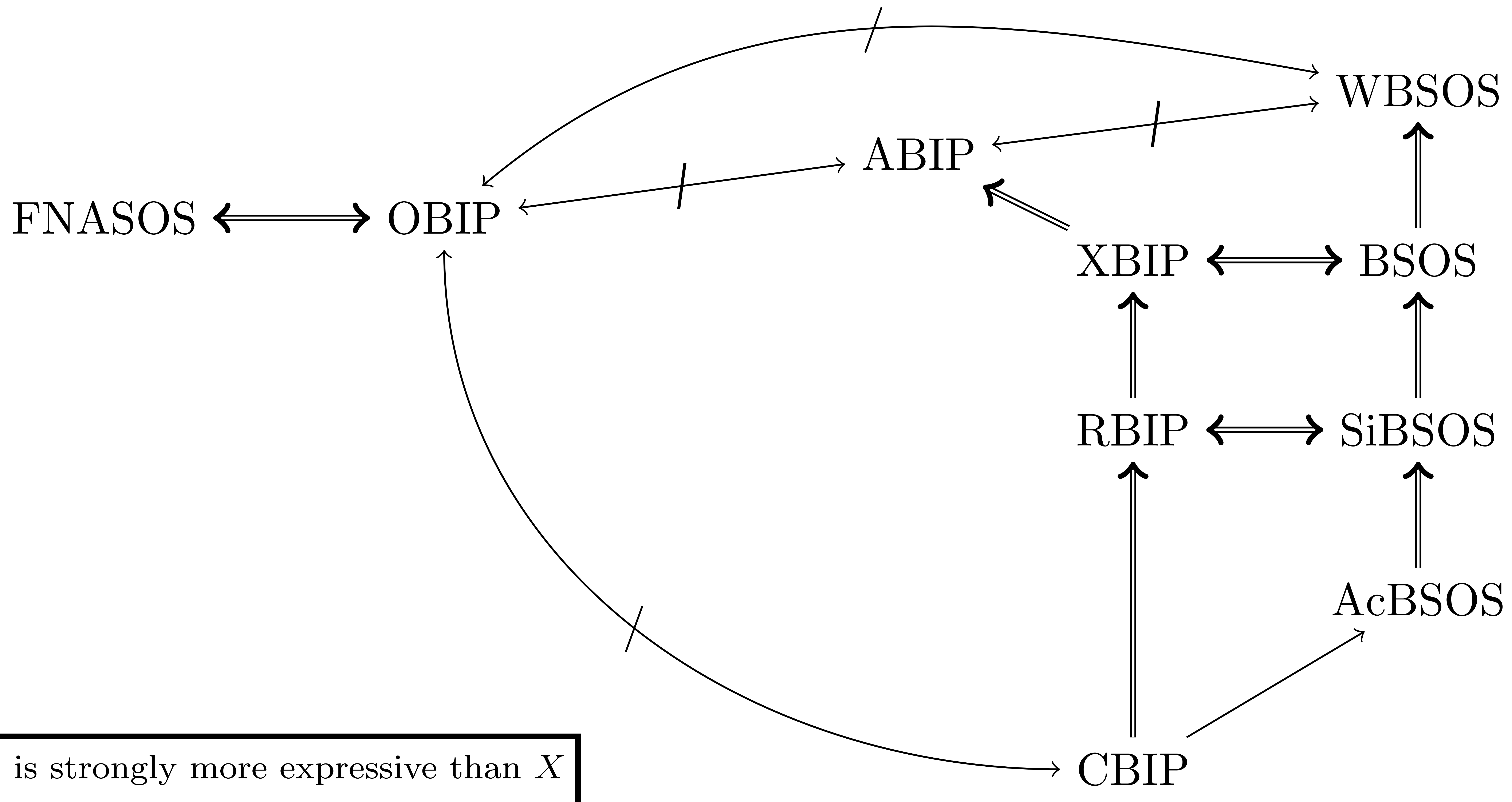
Example: arbitrary relation on γ

$$\frac{q_2 \xrightarrow{r} q_2' \qquad q_3 \not\xrightarrow{s} \qquad q_4 \not\xrightarrow{t}}{q_1q_2q_3q_4 \xrightarrow{r} q_1q_2'q_3q_4} \qquad \frac{q_1 \xrightarrow{p} q_1' \qquad q_2 \not\xrightarrow{r}}{q_1q_2q_3q_4 \xrightarrow{r} q_1'q_2q_3q_4} \qquad \frac{q_3 \xrightarrow{s} q_3' \qquad q_1 \not\xrightarrow{p}}{q_1q_2q_3q_4 \xrightarrow{s} q_1q_2q_3'q_4}$$



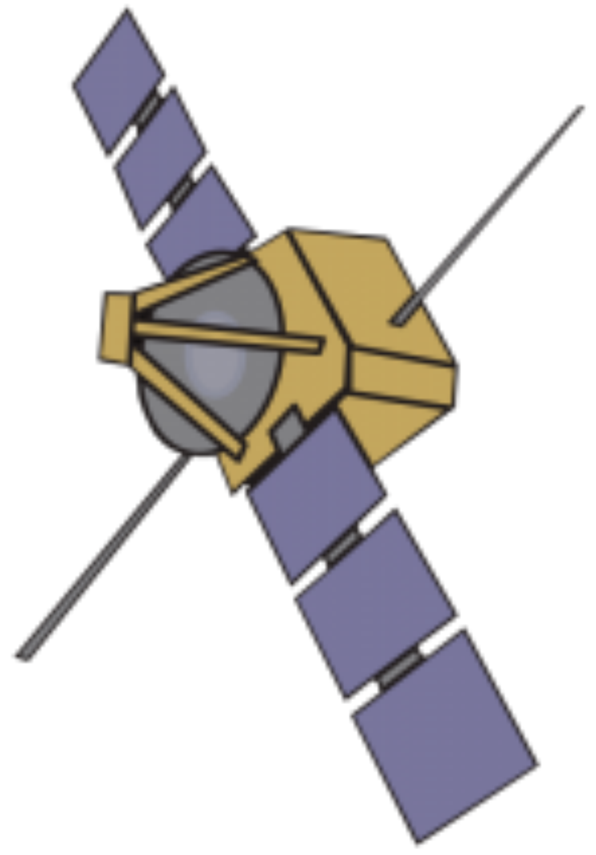


Expressiveness hierarchy



$X \Longrightarrow Y$	Y is strongly more expressive than X
$X \longrightarrow Y$	Y is weakly more expressive than X
$X \Longleftrightarrow Y$	X and Y are strongly equivalent
$X \longleftrightarrow\!\!\!\!\!\!/\;\; Y$	X and Y are incomparable

Conclusion



Powerful theoretical tools to build systems that are correct by construction

Going from theory to practice requires a lot of effort and cross-domain collaborations

Bigger challenge yet: taking these methods to less constrained application domains

Thanks!