Soutenance de thèse

Systèmes à composants synchronisés :

Contributions à la vérification compositionnelle du raffinement et des propriétés

Arnaud LANOIX

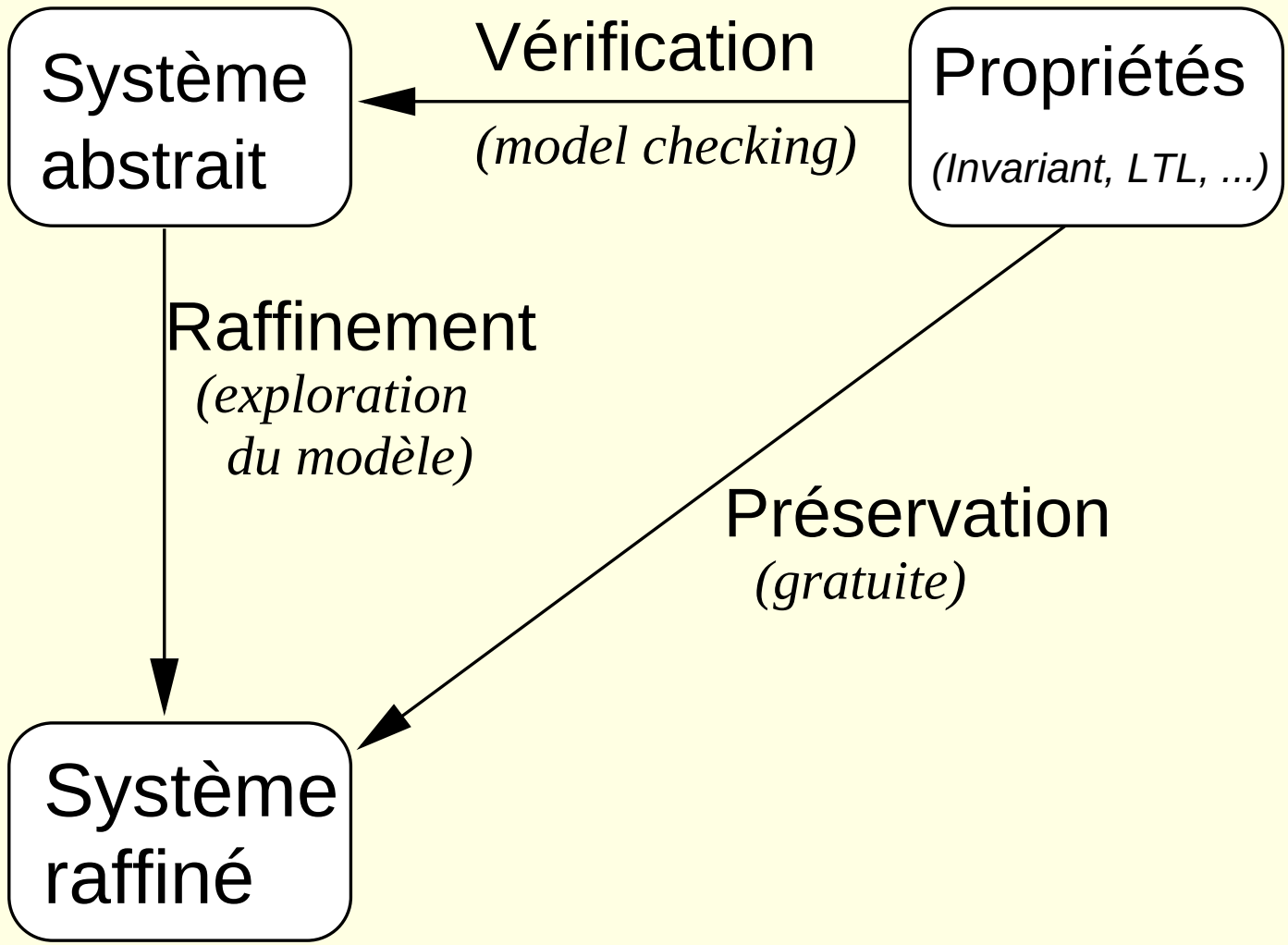
Thèse encadrée par Olga Kouchnarenko et Jacques Julliand

Problématique

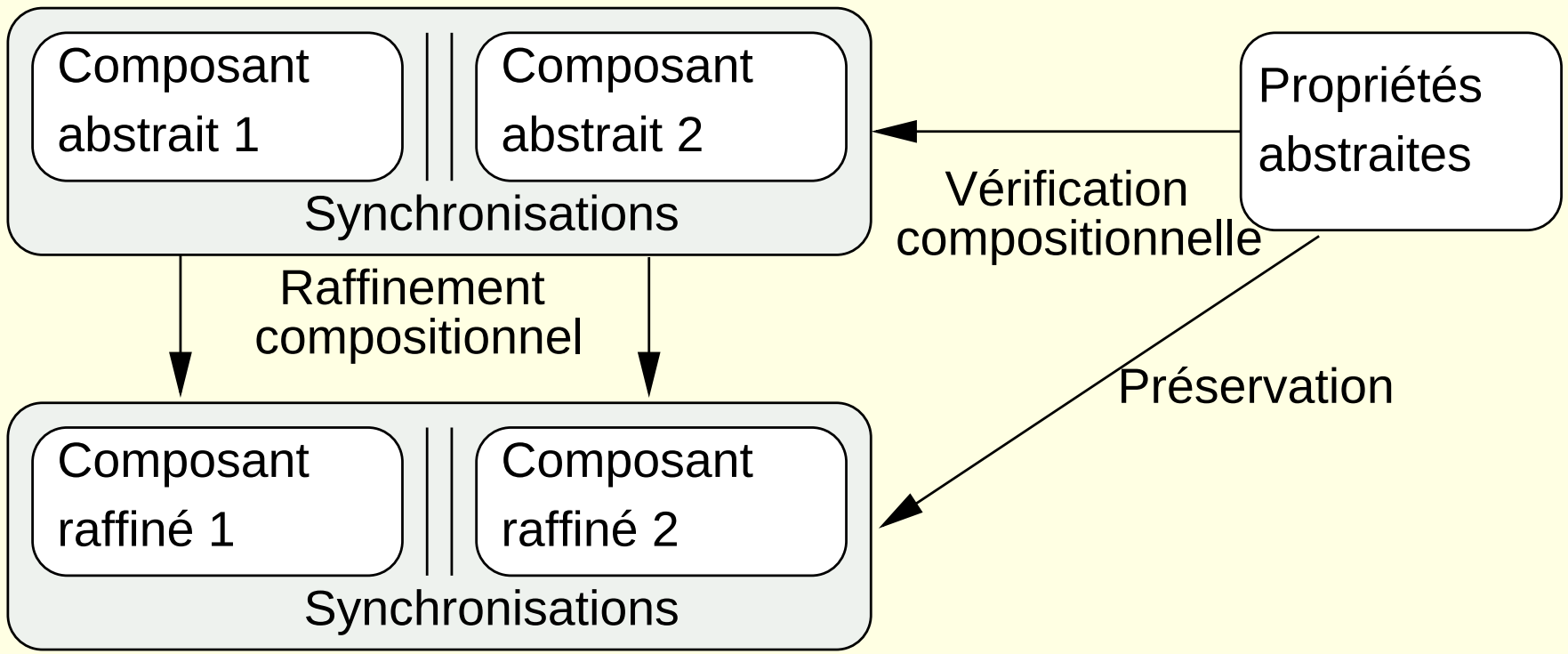
Vérification de logiciels critiques

- *Spécifier* un modèle du système
  - Composition
  - Raffinement
- *Vérifier* des propriétés sur le modèle
  - Preuve
  - Model-checking

Approche générale



Approche compositionelle



Plan de la présentation

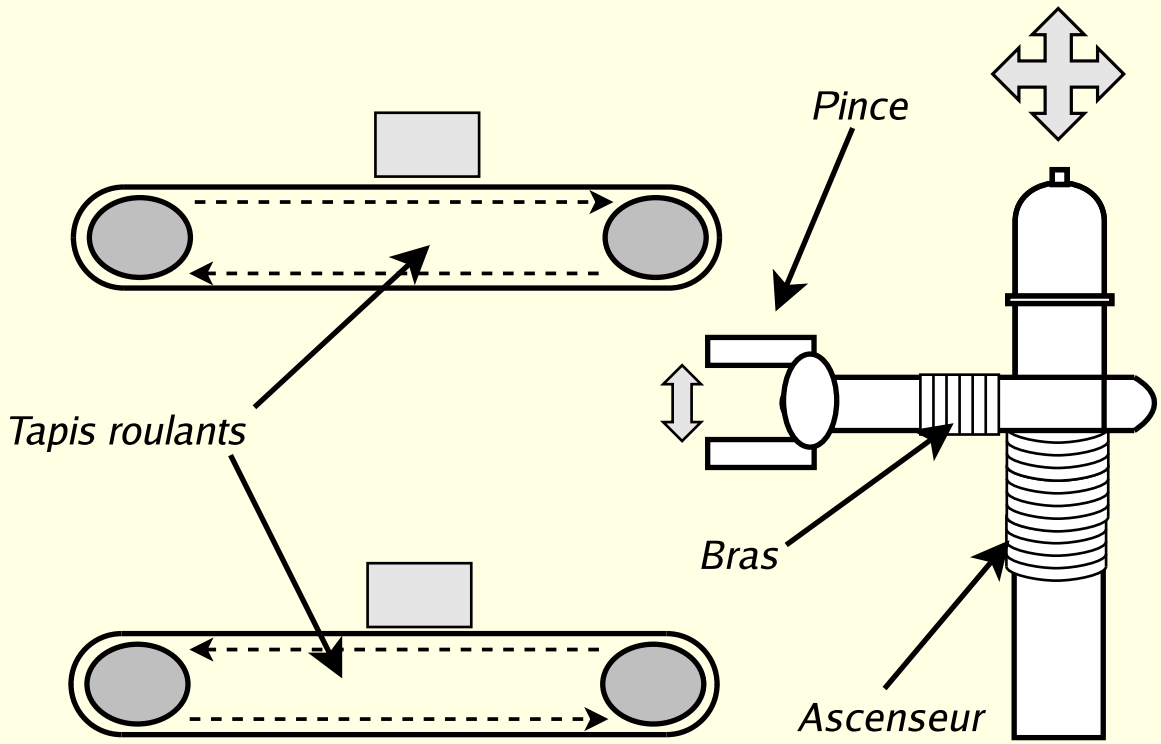
- **Préliminaires**
  - **Systèmes de transitions doublement étiquetés**
  - **Propriétés des systèmes**
  - **Raffinement des systèmes**
- Décomposition d'un système
  - Décomposition et raffinement
  - Décomposition et propriétés
- Systèmes à composants synchronisés
  - Systèmes à composants et raffinement
  - Systèmes à composants et propriétés
  - Implantation SynCo
- Conclusion et perspectives

Systèmes de transitions doublement étiquetés

Un ST2E est un six-uplet (Q, Q_0, E, T, V, l)

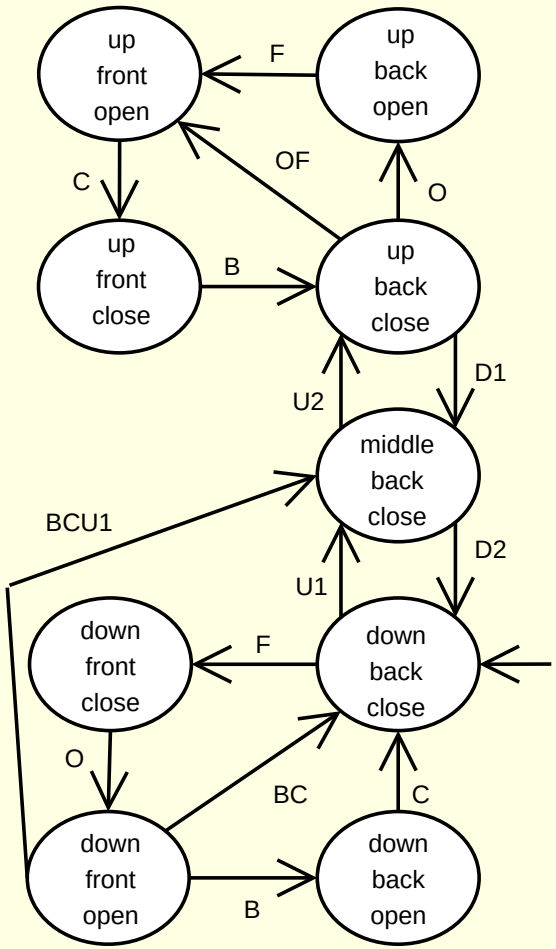
- Q, ensemble d'états
- $Q_0 \subseteq Q$, ensemble d'états initiaux
- E, ensemble de noms d'actions
- $T \subseteq Q \times E \times Q$, relation de transition étiquetée
- V, ensemble de variables
- $l : Q \to 2^{AP_V}$, fonction d'étiquetage associant à chaque état un ensemble de propositions atomiques

Systèmes de transitions : bras mobile robotisé



3 variables $\begin{cases} el \in \{up, middle, down\} \\ ar \in \{front, back\} \\ cl \in \{open, close\} \end{cases}$

11 actions : F, B, O, C, $U1$, $U2$, $D1$, $D2$, FO, BC, $BCU1$



$Robot_A$

Propriétés des systèmes

- *Propriétés d'invariance :* propriétés satisfaites dans tous les états de S
- *Propriétés temporelles :* propriétés satisfaites le long des *exécutions* de S, càd des successions d'états

  Logique Temporelle Linéaire (LTL) [Pnueli 81]

  $\bigcirc\phi,\ \phi\,\mathcal{U}\,\psi,\ \Box\phi,\ \Diamond\phi$
- Propriétés de *sûreté*, de *vivacité*, d'*atteignabilité*
- Vérification automatique par exploration du graphe d'états

  [Lichtenstein, Pnueli 85 - Vardi, Wolper 86 - Clarke, Grumberg, Peled 00]

Propriétés des systèmes : $Robot_A$

- "Si le dispositif est en position médiane alors la pince est fermée et le bras reculé"

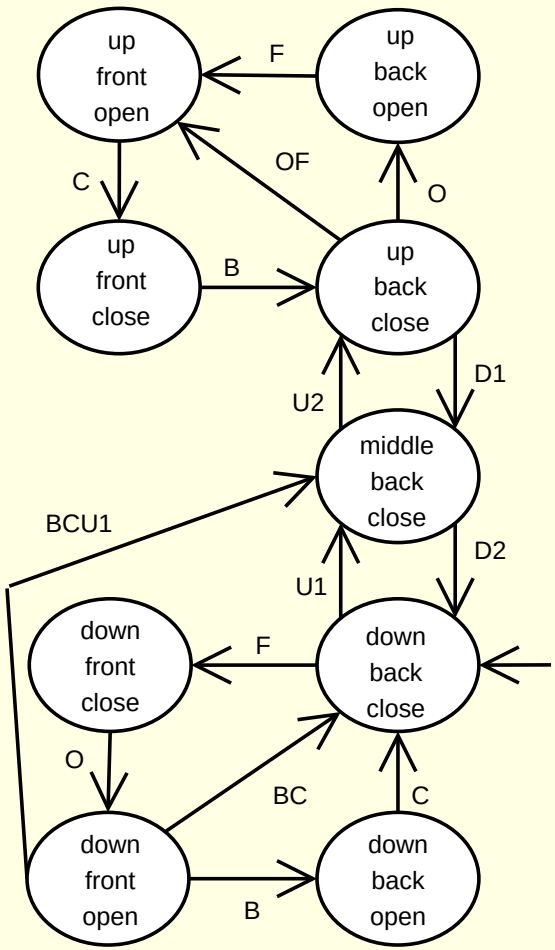
$$\Box((el = middle) \Rightarrow (ar = back \wedge cl = close))$$

- "La pince ne reste pas indéfiniment ouverte"

$$\Box((cl = open) \Rightarrow \Diamond(cl = close))$$

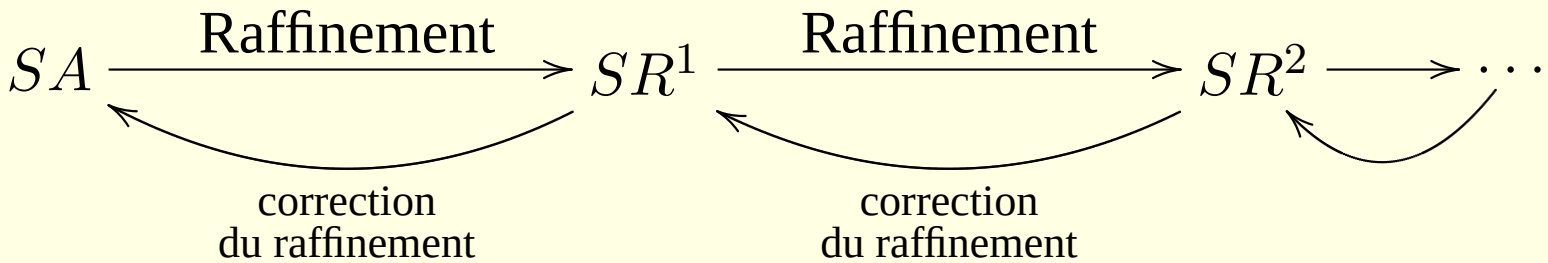
- "Quand le dispositif est en position médiane, les seules actions possibles sont la montée ou la descente"

$$\Box((el = middle) \Rightarrow \bigcirc(el \in \{up, down\}))$$



$Robot_A$

Raffinement des systèmes



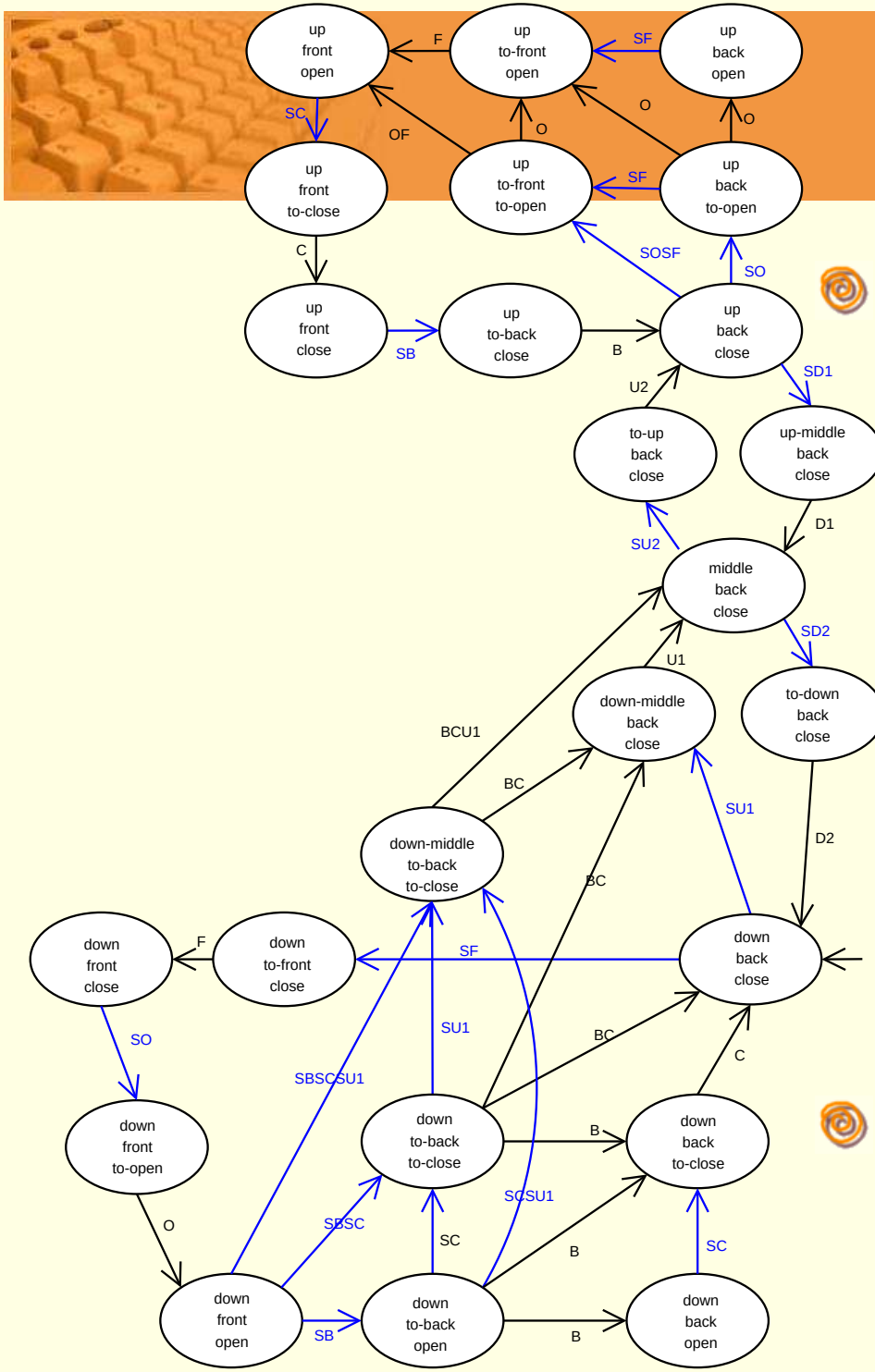
- Redéfinir les variables abstraites et ajouter de nouvelles variables

  prédicat de collage -> relation entre variables abstraites et variables raffinées

- Ajouter de nouvelles actions

raffinement de Dijkstra [Dijkstra 76], *raffinement de systèmes d'actions* [Back 88], *raffinement B* [Abrial 96], *raffinement TLA* [Lamport 96], etc.

Raffinement : $Robot_R$



Redéfinition du domaine des variables el_R, ar_R et cl_R

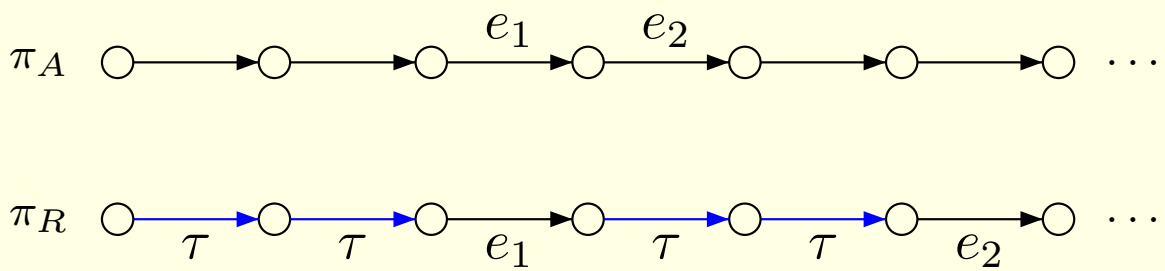
Prédicat de collage :

$el = up \Leftrightarrow el_R \in \{up, up2mid\}$
$\wedge el = middle \Leftrightarrow el_R \in \{2up, middle, 2down\}$
$\wedge el = down \Leftrightarrow el_R \in \{down, do2mid\}$
$\wedge ar = front \Leftrightarrow ar_R \in \{front, 2back\}$
$\wedge ar = back \Leftrightarrow ar_R \in \{back, 2front\}$
$\wedge cl = open \Leftrightarrow cl_R \in \{open, 2close\}$
$\wedge cl = close \Leftrightarrow cl_R \in \{close, 2open\}$

Ajout de nouvelles actions : SC, SB, SBC, SO, $SCU1$, SF, $SU1$, $SU2$ ...

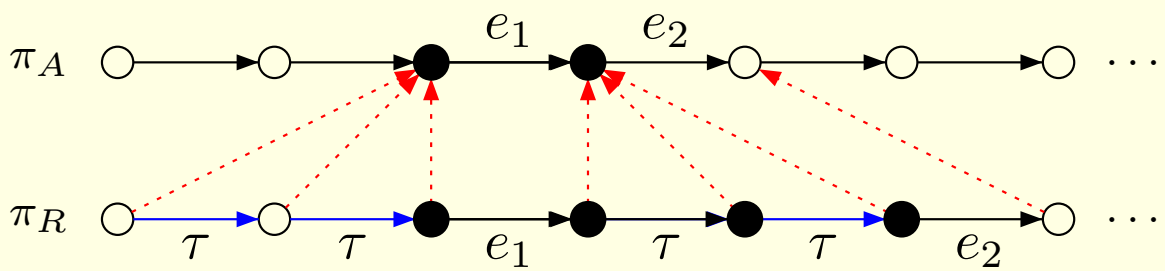
Raffinement : SR $\sqsubseteq_\eta$ SA

Relation de raffinement entre SR et SA [Bellegarde, Julliand, Kouchnarenko 00]



Raffinement : SR $\sqsubseteq_\eta$ SA

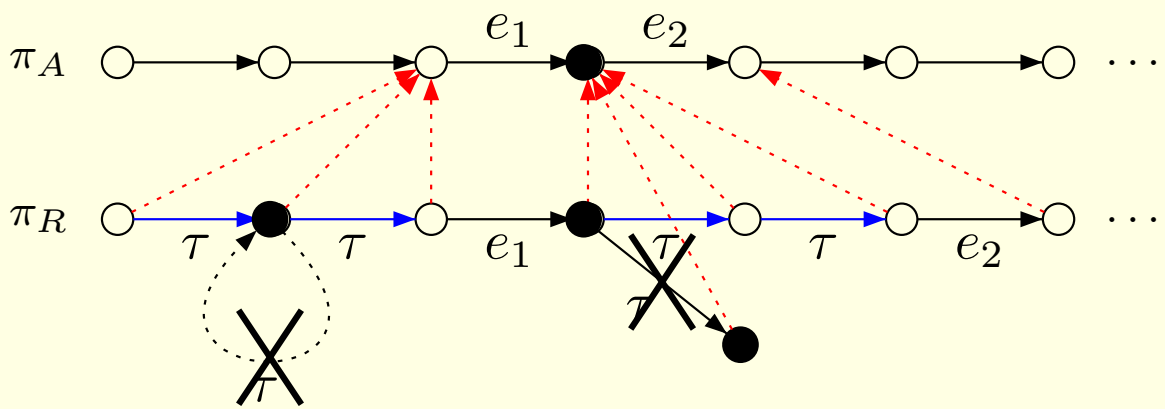
Relation de raffinement entre SR et SA [Bellegarde, Julliand, Kouchnarenko 00]



- Relation de collage
- Simulation des "anciennes" actions
- τ-simulation des "nouvelles" actions

Raffinement : SR $\sqsubseteq_\eta$ SA

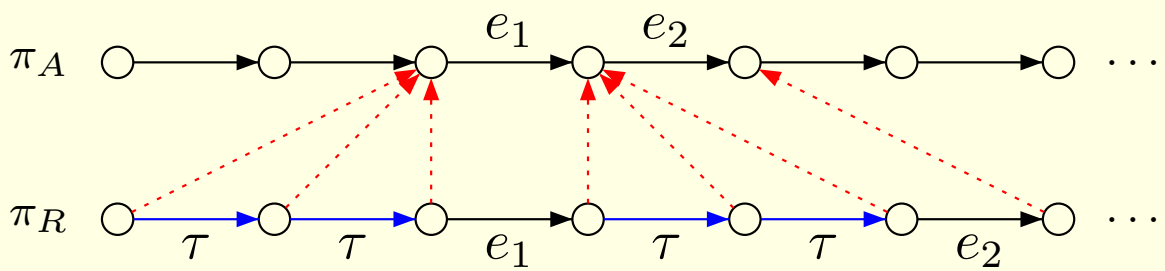
Relation de raffinement entre SR et SA [Bellegarde, Julliand, Kouchnarenko 00]



- Relation de collage
- Simulation des "anciennes" actions
- τ-simulation des "nouvelles" actions
- Absence de τ-cycles
- Absence de "nouveaux" blocages

Raffinement : SR $\sqsubseteq_\eta$ SA

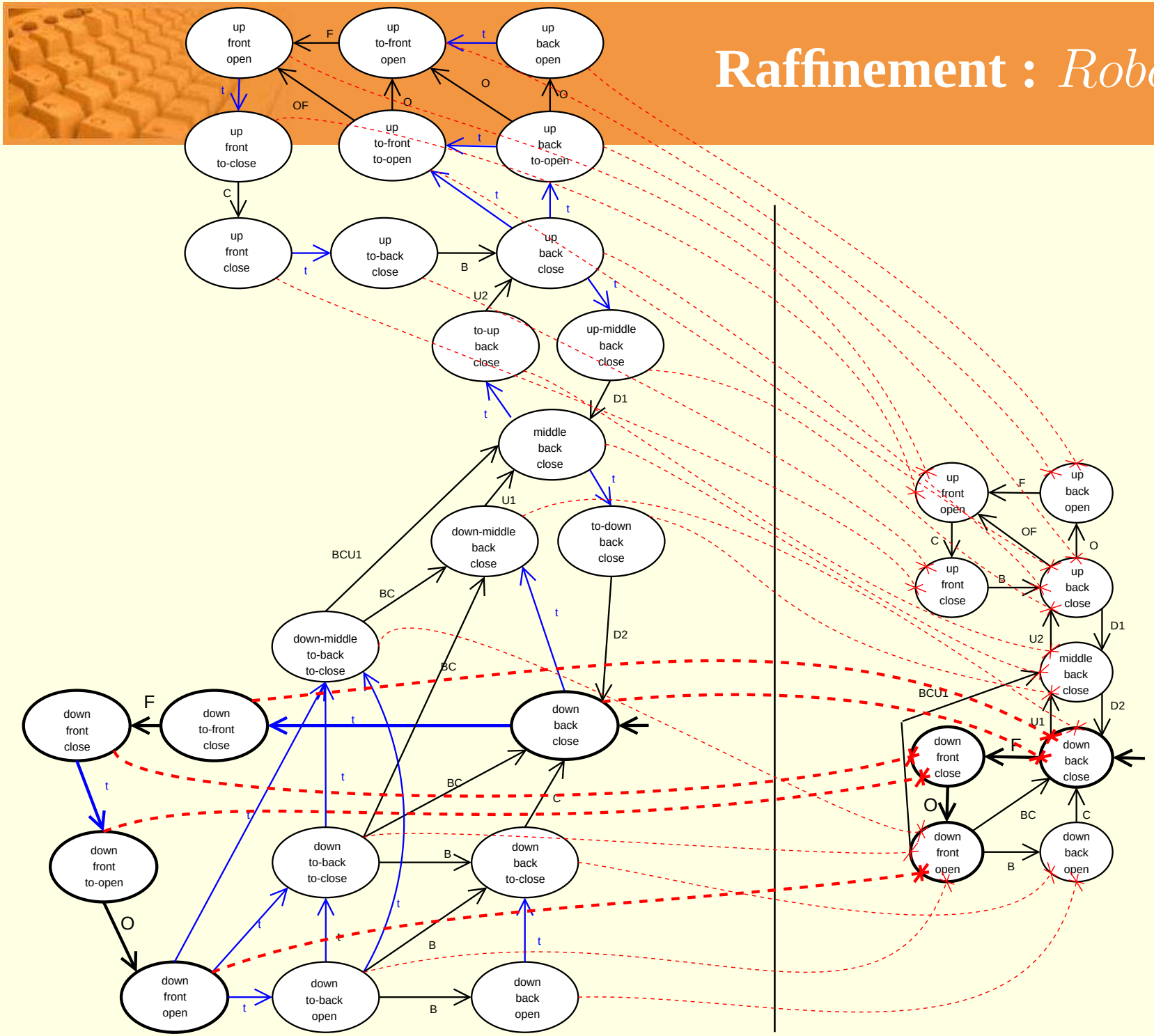
Relation de raffinement entre SR et SA [Bellegarde, Julliand, Kouchnarenko 00]



- Relation de collage
- Simulation des "anciennes" actions
- τ-simulation des "nouvelles" actions
- Absence de τ-cycles
- Absence de "nouveaux" blocages

$\Rightarrow$ Préservation des propriétés LTL [Darlot, Julliand, Kouchnarenko 03]

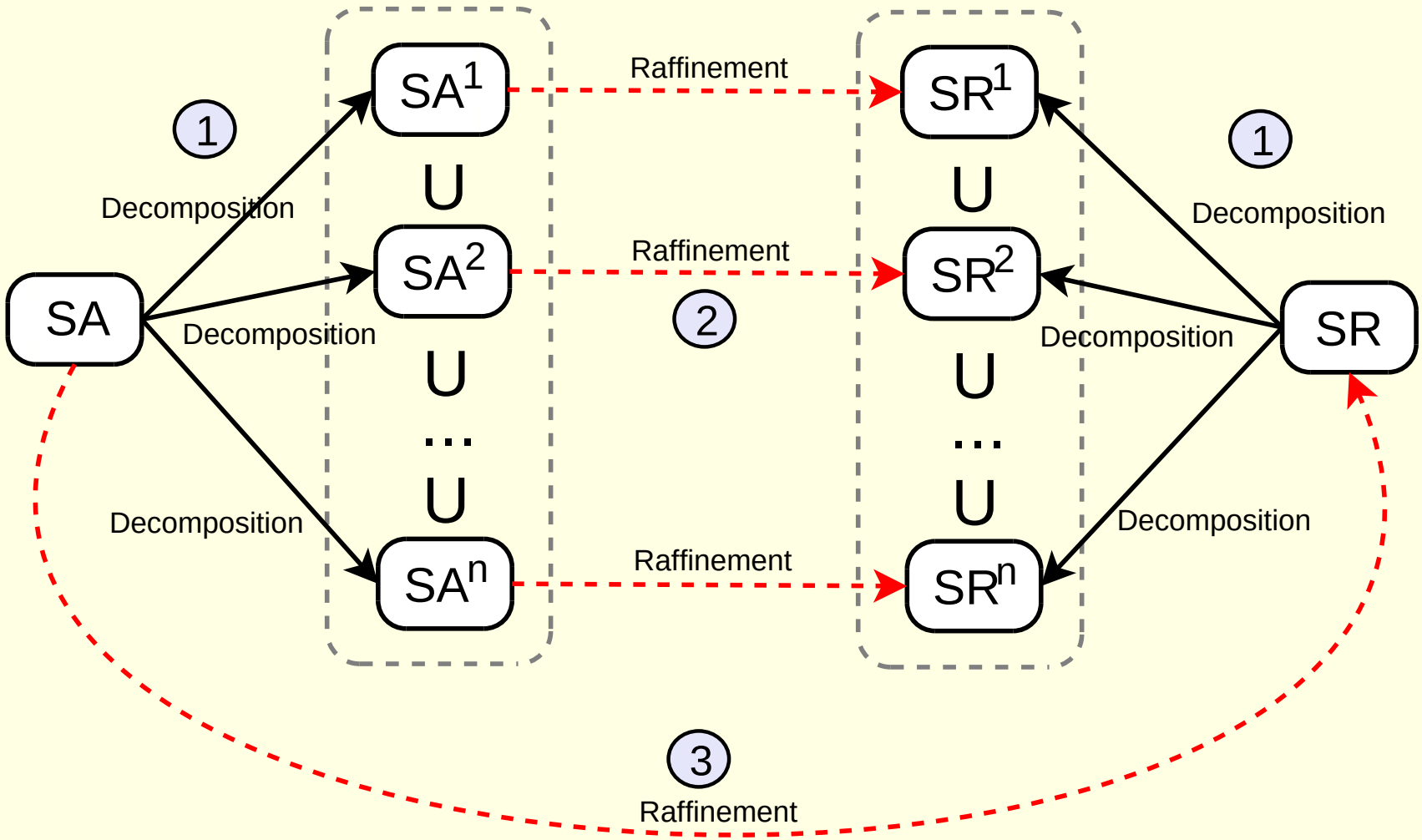
Raffinement : $Robot_R$



Plan de la présentation

- Préliminaires
  - Systèmes de transitions doublement étiquetés
  - Propriétés des systèmes
  - Raffinement des systèmes
- **Décomposition d'un système**
  - **Décomposition et raffinement**
  - **Décomposition et propriétés**
- Systèmes à composants synchronisés
  - Systèmes à composants et raffinement
  - Systèmes à composants et propriétés
  - Implantation SynCo
- Conclusion et perspectives

Décomposition



Décomposition : sous-systèmes

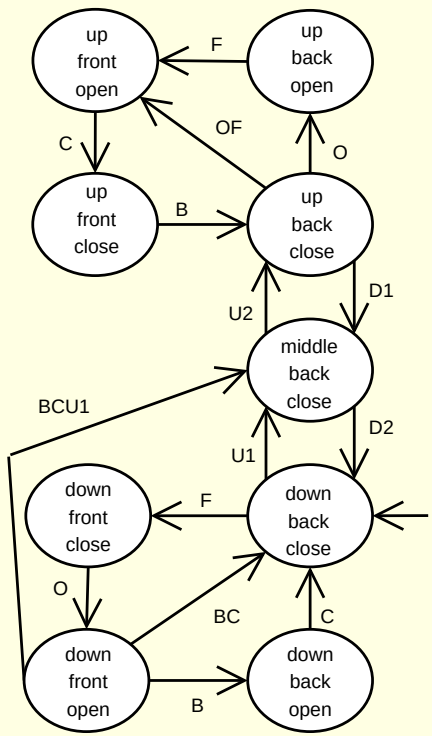
S^1 et S^2 sont des *sous-systèmes* de $S = S^1 \cup S^2$ si

- $Q = Q^1 \cup Q^2$
- $E = E^1 \cup E^2$
- $Q_0 = Q_0^1 \cup Q_0^2$
- $T = T^1 \cup T^2$
- $\forall q \in Q,\ l(q) = \begin{cases} l^1(q) \text{ si } q \in Q^1 \setminus Q^2 \\ l^2(q) \text{ si } q \in Q^2 \setminus Q^1 \\ l^1(q) = l^2(q) \text{ si } q \in Q^1 \cap Q^2 \end{cases}$

La décomposition se généralise par associativité :

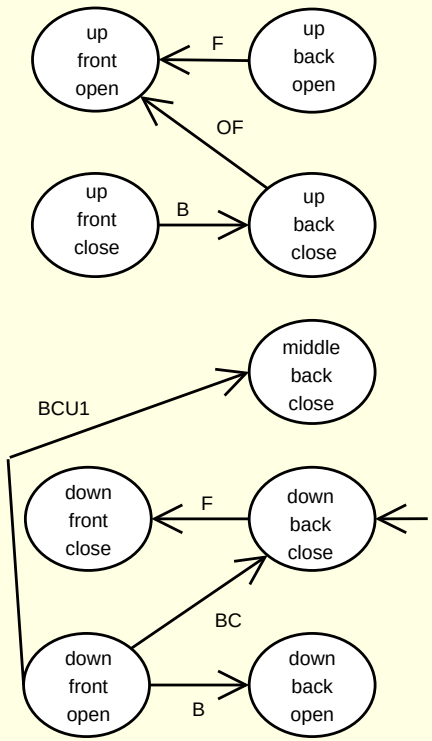
$(S^1 \cup S^2) \cup S^3 = S^1 \cup (S^2 \cup S^3)$

Décomposition : $Robot_A$

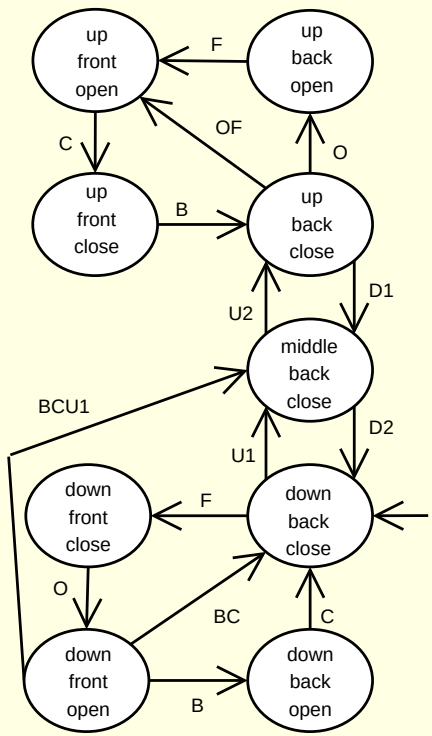


$Robot_A$

Décomposition : $Robot_A$

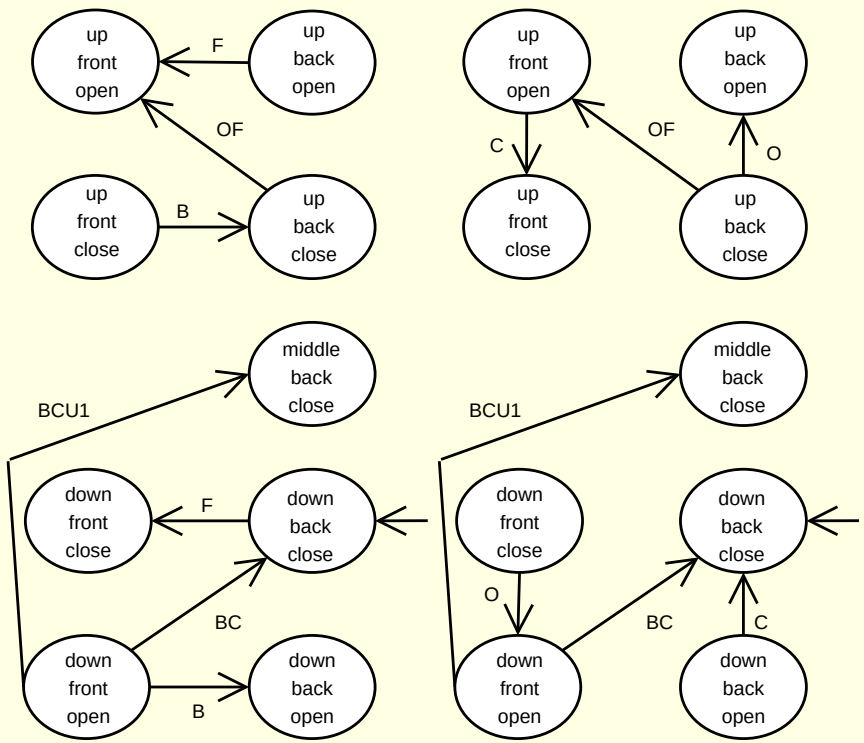


$Robot_A^1$

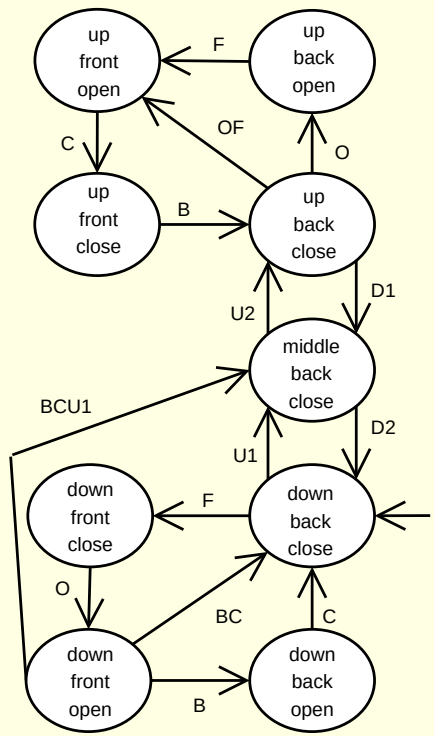


$Robot_A$

Décomposition : $Robot_A$

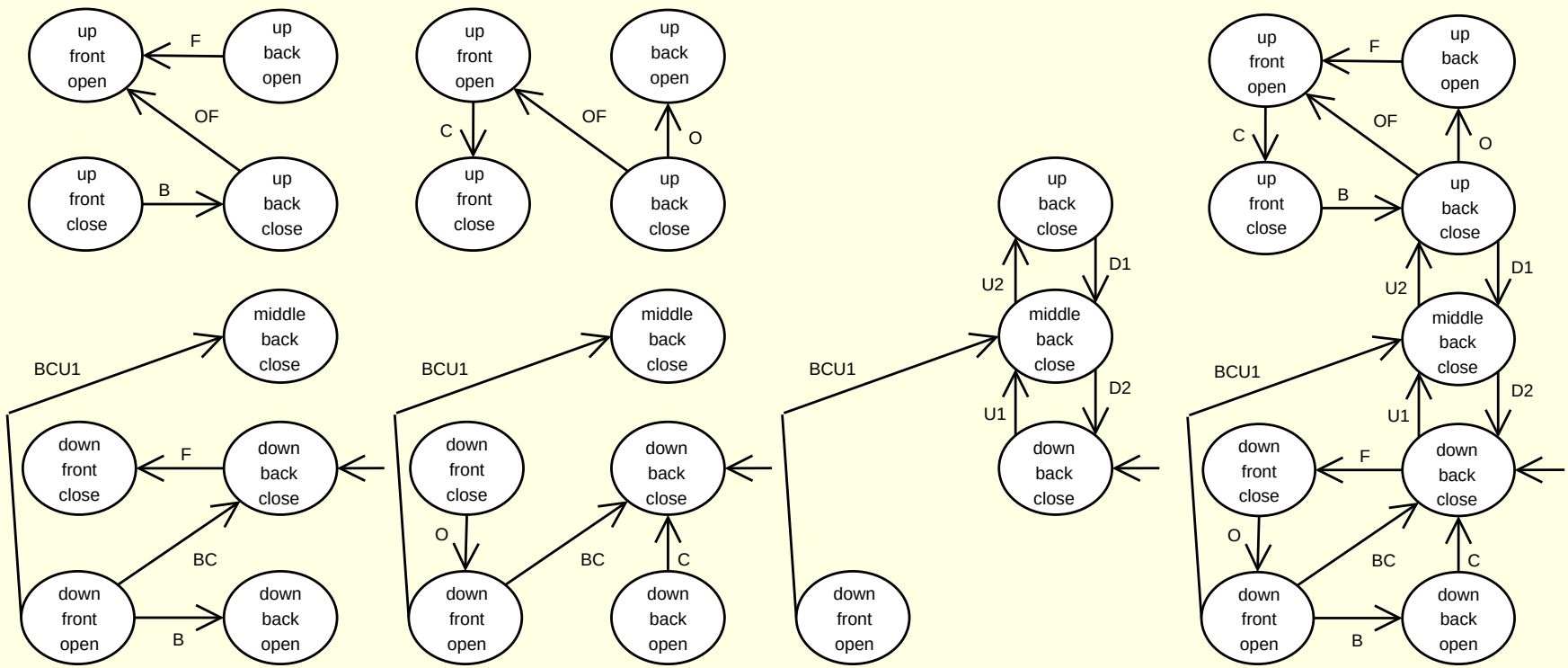


$Robot_A^1 \cup Robot_A^2$



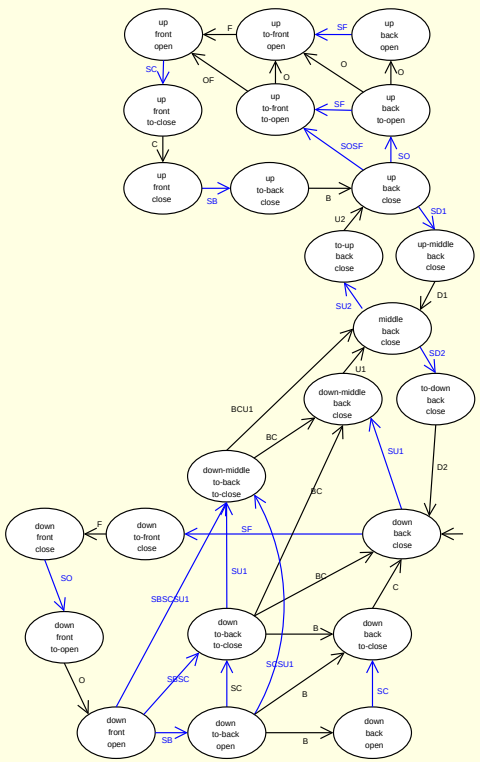
$Robot_A$

Décomposition : $Robot_A$



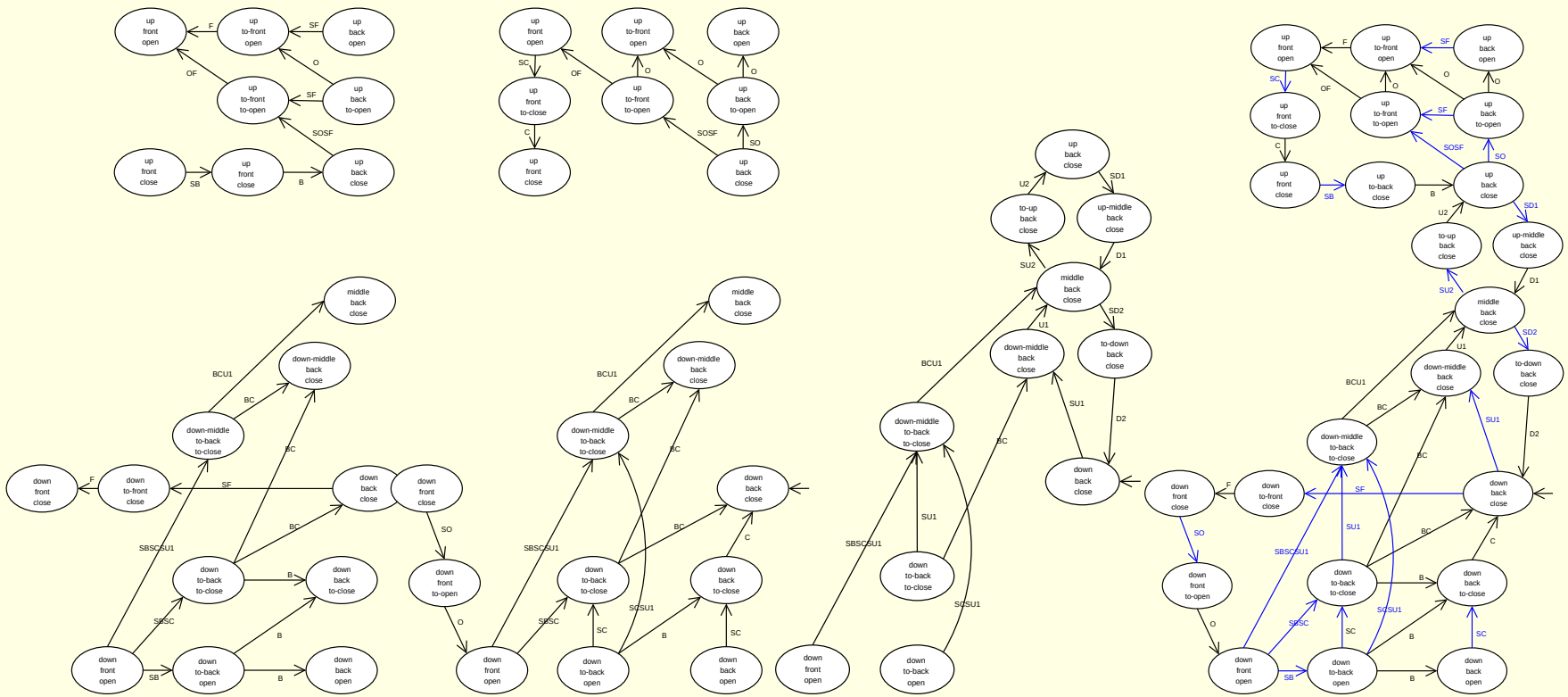
$$Robot_A^1 \cup Robot_A^2 \cup Robot_A^3 = Robot_A$$

Décomposition et raffinement : $Robot_R$



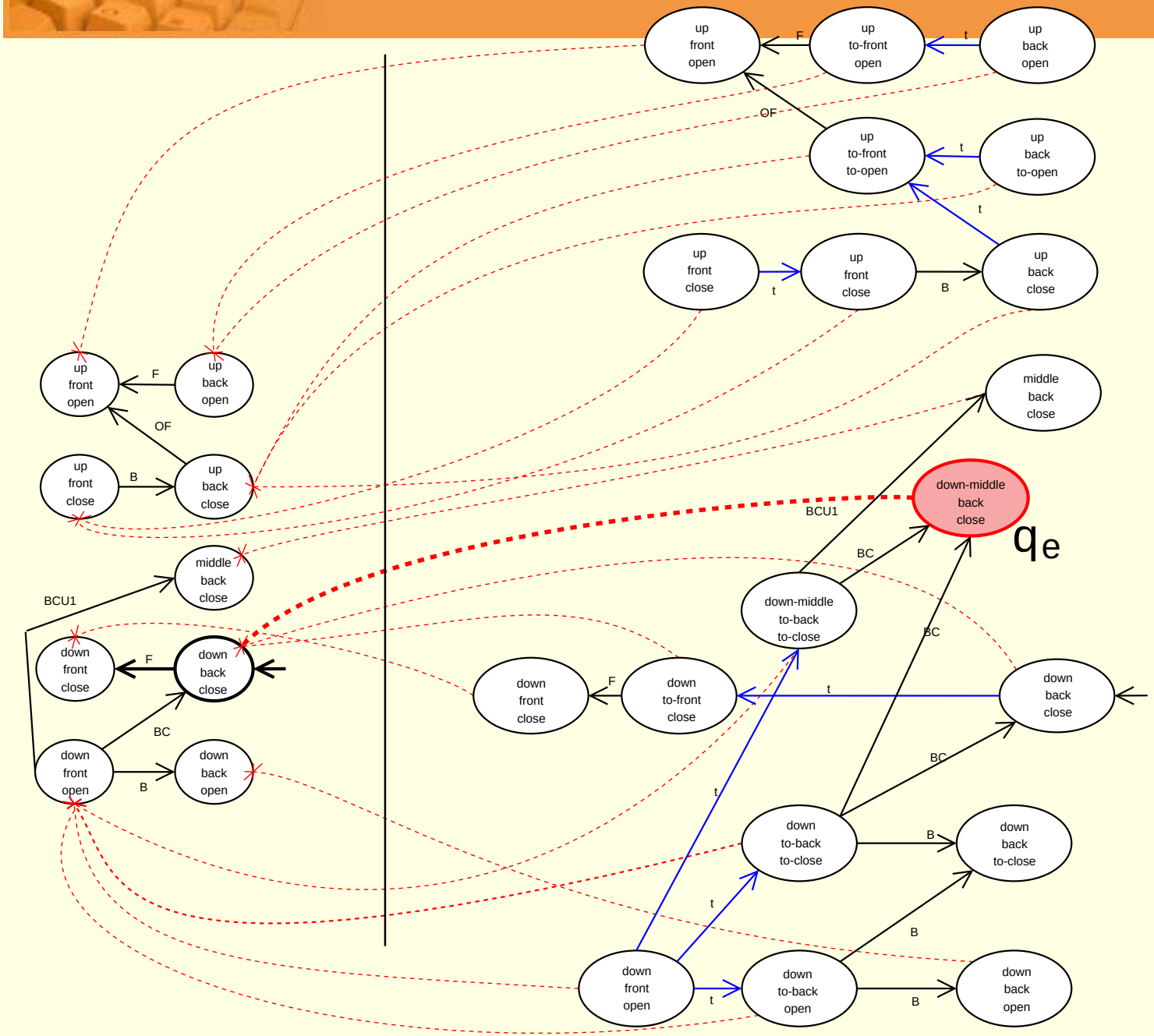
$Robot_R$

Décomposition et raffinement : $Robot_R$



$$Robot_R^1 \cup Robot_R^2 \cup Robot_R^3 = Robot_R$$

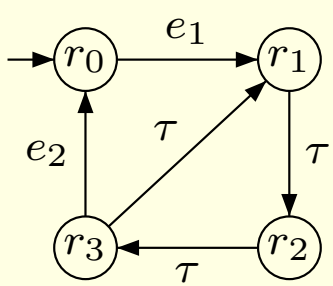
Décomposition et raffinement : $Robot^1_R \sqsubseteq_\eta Robot^1_A$



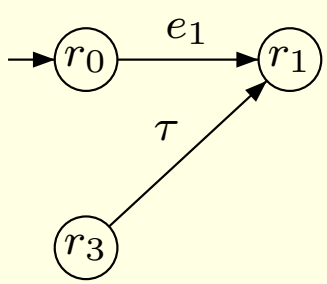
Décomposition et raffinement

La décomposition $SR = SR^1 \cup SR^2$ n'est pas toujours compatible avec le raffinement :

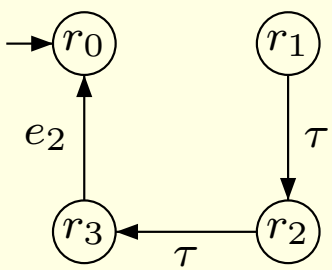
- La décomposition introduit dans les sous-systèmes SR^1 et SR^2 de *"faux" états de blocages*
- La décomposition *masque* dans SR^1 et SR^2 des τ-cycles de SR



SR



SR^1



SR^2

Décomposition et raffinement : $\mathrm{SR} \sqsubseteq^{\mathrm{D}}_{\rho_{\mathbf{w}}} \mathrm{SA}$

Relation *affaiblie* de raffinement entre SR et SA

- Relation de collage
- Simulation des "anciennes" actions
- τ-simulation des "nouvelles" actions
- $D \subseteq Q_R$ est l'ensemble des "nouveaux" états de blocage

Propriétés :

- Le raffinement affaibli *préserve* les sûretés
- Raffinement vs. raffinement affaibli :
  $SR \sqsubseteq_\eta SA$ ssi $SR \sqsubseteq^D_{\rho_w} SA$ et $D = \varnothing$ et $\neg\, div^\tau(SR)$

Décomposition et raffinement : blocages

$$\left.\begin{array}{l} SR^1 \sqsubseteq^{D_1}_{\rho_w} SA^1 \\ SR^2 \sqsubseteq^{D_2}_{\rho_w} SA^2 \end{array}\right\} SR^1 \cup SR^2 \sqsubseteq^{D}_{\rho_w} SA^1 \cup SA_2$$

"$q_R \in D_1$ n'est pas un "vrai" blocage dans $SR^1 \cup SR^2$ si $q_R \in Q^2_R$ et $q_R \notin D_2$"

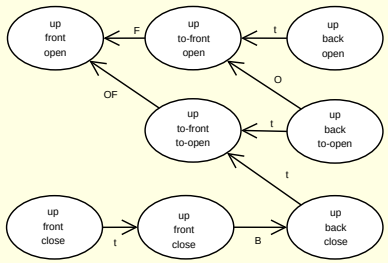
Réduction des blocages :

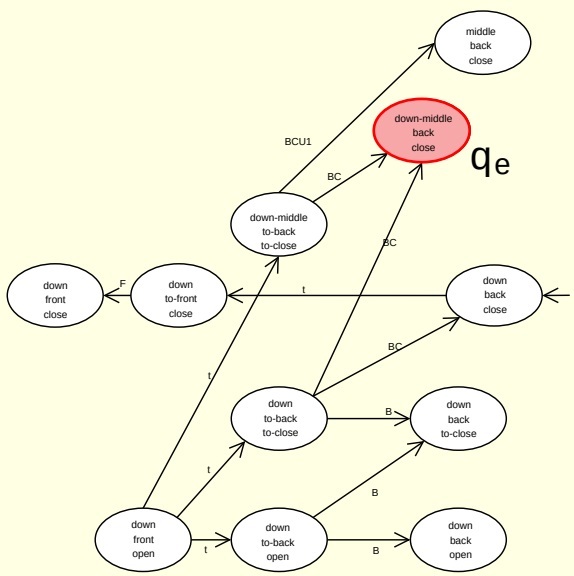
$$D = D_1 \triangle D_2 = (D_1 \cap D_2) \cup (D_1 \setminus Q^2_R) \cup (D_2 \setminus Q^1_R)$$

La réduction des blocages est associative :

$$(D_1 \triangle D_2) \triangle D_3 = D_1 \triangle (D_2 \triangle D_3)$$

Décomposition et raffinement : $Robot_R^1$

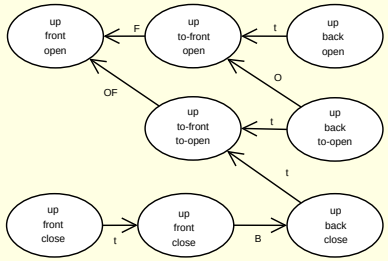


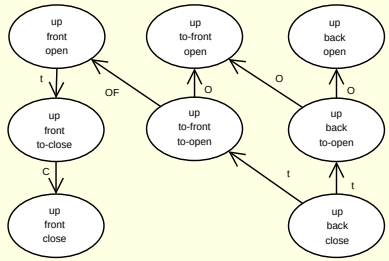


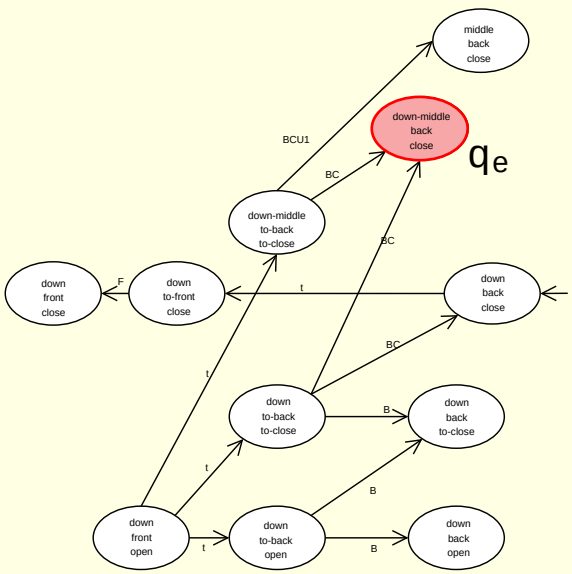
$$Robot_R^1$$

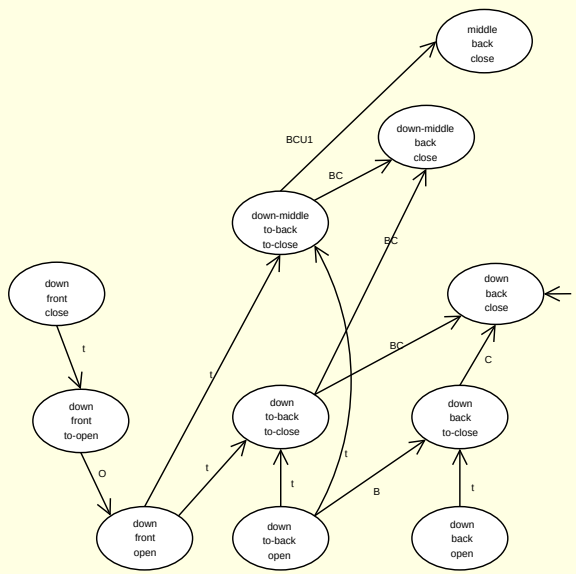
$$D_1 = \{q_e\}$$

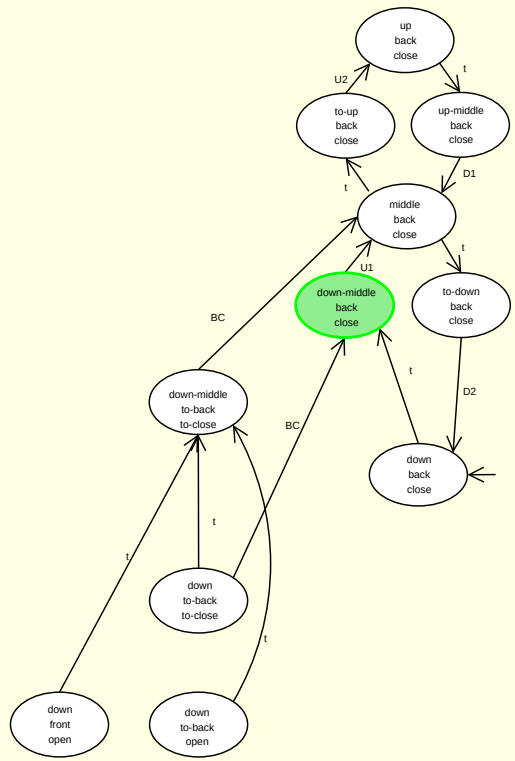
Décomposition et raffinement : $Robot^1_R$











$$Robot^1_R \quad \cup \quad Robot^2_R \quad \cup \quad Robot^3_R$$

$$D_1 = \{q_e\} \qquad D_2 = \varnothing \qquad D_3 = \varnothing$$

Décomposition et raffinement

Théorème (raffinement par décomposition).
Soient $SA = SA^1 \cup SA^2$ et $SR = SR^1 \cup SR^2$.

$$\frac{SR^1 \sqsubseteq^{D_1}_{\rho_w} SA^1, \quad SR^2 \sqsubseteq^{D_2}_{\rho_w} SA^2}{SR^1 \cup SR^2 \sqsubseteq^{D_1 \triangle D_2}_{\rho_w} SA^1 \cup SA^2}$$

Le théorème précédent se généralise à n sous-systèmes par associativité

Décomposition et propriétés

- Préservation *par décomposition* des invariants

$$\frac{SA^1 \models \Box sp, \quad SA^2 \models \Box sp}{SA^1 \cup SA^2 \models \Box sp}$$

- Préservation *par décomposition* des invariants dynamiques, un invariant dynamique étant un prédicat "avant-après" correspondant à $\Box(sp_1 \Rightarrow \bigcirc sp_2)$.

Décomposition et propriétés

- Préservation par décomposition de la *non-satisfaction* des sûretés LTL :

$$S^1 \not\models \phi \text{ alors } S^1 \cup S^2 \not\models \phi$$

Nous n'avons pas *préservation* pour des propriétés LTL quelconques puisque $S^1 \cup S^2$ ***simule*** S^1

Décomposition et propriétés

- Préservation par décomposition de la *non-satisfaction* des sûretés LTL :

$$S^1 \not\models \phi \text{ alors } S^1 \cup S^2 \not\models \phi$$

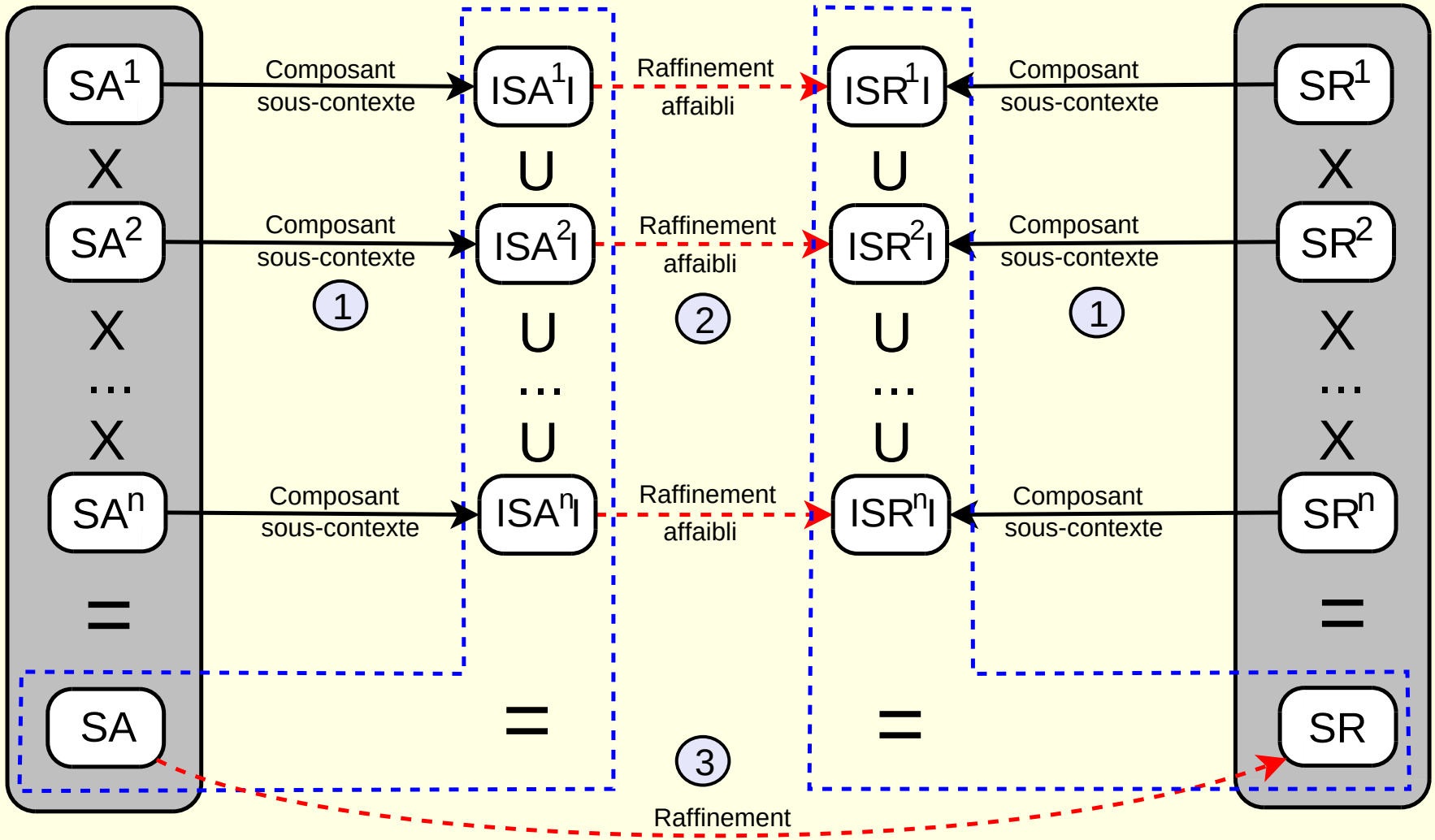
  Nous n'avons pas *préservation* pour des propriétés LTL quelconques puisque $S^1 \cup S^2$ ***simule*** S^1

- Algorithme d'*analyse d'atteignabilité compositionnelle* utilisant les sous-systèmes

Plan de la présentation

- Préliminaires
  - Systèmes de transitions doublement étiquetés
  - Propriétés des systèmes
  - Raffinement des systèmes
- Décomposition d'un système
  - Décomposition et raffinement
  - Décomposition et propriétés
- **Systèmes à composants synchronisés**
  - **Systèmes à composants et raffinement**
  - **Systèmes à composants et propriétés**
  - **Implantation SynCo**
- Conclusion et perspectives

Systèmes à composants synchronisés



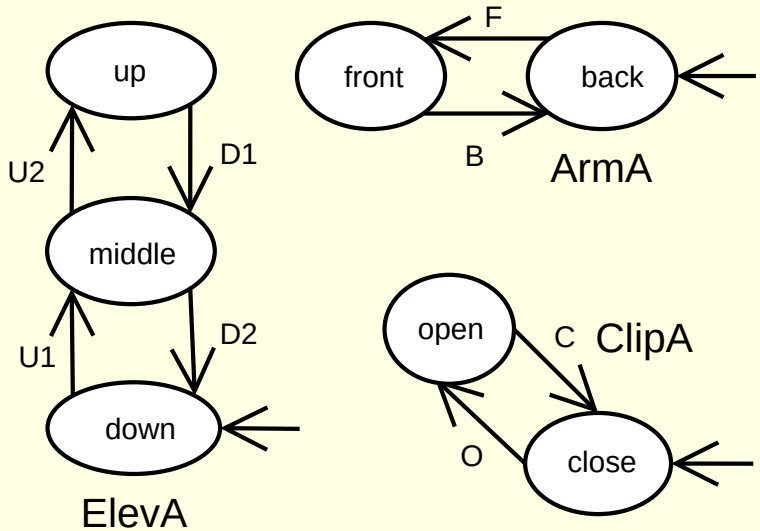
Systèmes à composants synchronisés

- Produit cartésien
- Produit synchronisé [Arnold, Nivat 82]
- Produit synchrone
- Produit asynchrone
- ST2Es communicants
- …

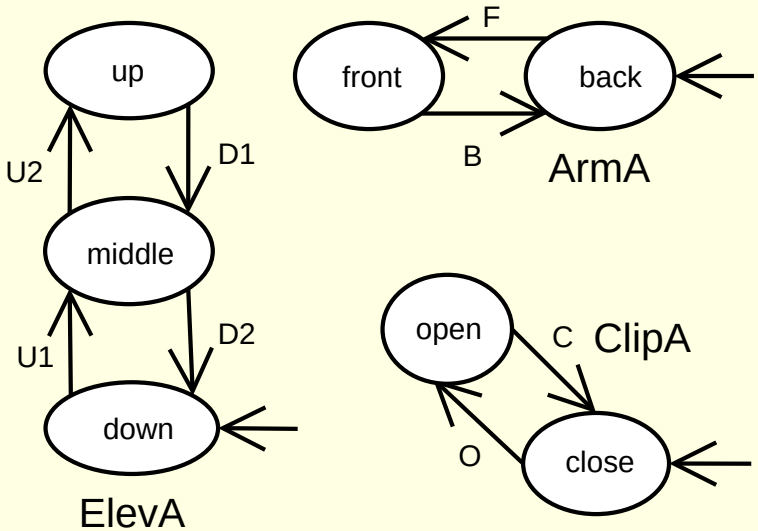
} **Systèmes à composants synchronisés**

$$= \begin{cases} \text{des composants indépendants } S^1, S^2, \ldots, S^n, \\ \text{un ensemble de synchronisations contraintes } Syn^c, \\ \text{une opération de produit } \times_{Syn^c} \end{cases}$$

Systèmes à composants : $Robot_A$

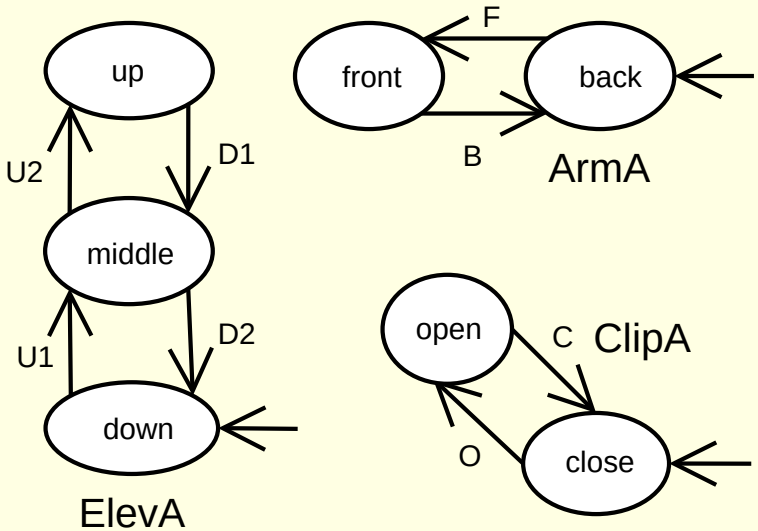


Systèmes à composants : $Robot_A$

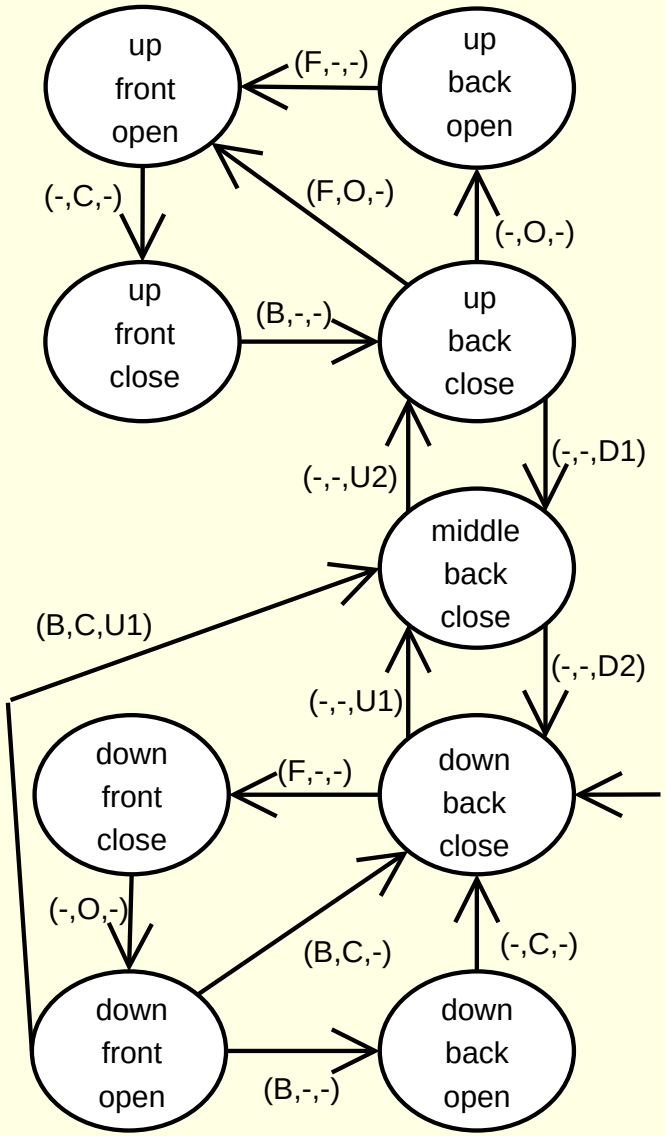


(-,O,-) **when** (ar=back $\wedge$ el=up) $\vee$ (ar=front $\wedge$ el=down),
(-,C,-) **when** (ar=front $\wedge$ el=up) $\vee$ (ar=back $\wedge$ el=down),
(F,-,-) **when** (cl=open $\wedge$ el=up) $\vee$ (cl=close $\wedge$ el=down),
(B,-,-) **when** (cl=close $\wedge$ el=up) $\vee$ (cl=open $\wedge$ el=down),
(F,O,-) **when** el=up,
(B,C,-) **when** el=down,
(B,C,U1) **when** true,
(-,-,U1) **when** cl=close $\wedge$ ar=back,
(-,-,U2) **when** cl=close $\wedge$ ar=back,
(-,-,D1) **when** cl=close $\wedge$ ar=back,
(-,-,D2) **when** cl=close $\wedge$ ar=back

Systèmes à composants : $Robot_A$



(-,O,-) **when** (ar=back ∧ el=up) ∨ (ar=front ∧ el=down),
(-,C,-) **when** (ar=front ∧ el=up) ∨ (ar=back ∧ el=down),
(F,-,-) **when** (cl=open ∧ el=up) ∨ (cl=close ∧ el=down),
(B,-,-) **when** (cl=close ∧ el=up) ∨ (cl=open ∧ el=down),
(F,O,-) **when** el=up,
(B,C,-) **when** el=down,
(B,C,U1) **when** true,
(-,-,U1) **when** cl=close ∧ ar=back,
(-,-,U2) **when** cl=close ∧ ar=back,
(-,-,D1) **when** cl=close ∧ ar=back,
(-,-,D2) **when** cl=close ∧ ar=back



Systèmes à composants : composants sous-contexte

Soit (S^1, S^2, Syn^c) un système à composants

L'ensemble de synchronisations Syn^c est *restreint* pour chacun des composants : $[Syn^c]_{S^1}$ et $[Syn^c]_{S^2}$

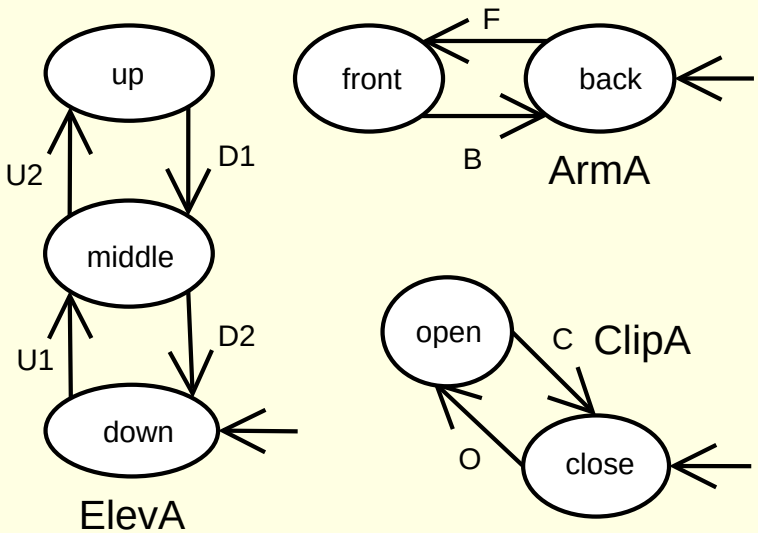
Les **composants sous-contexte** $[S^1]$ et $[S^2]$ sont obtenus ainsi :

$$[S^1] = S^1 \times_{[Syn^c]_{S^1}} S^2 \quad [S^2] = S^1 \times_{[Syn^c]_{S^2}} S^2$$

Système à composants = **décomposition**

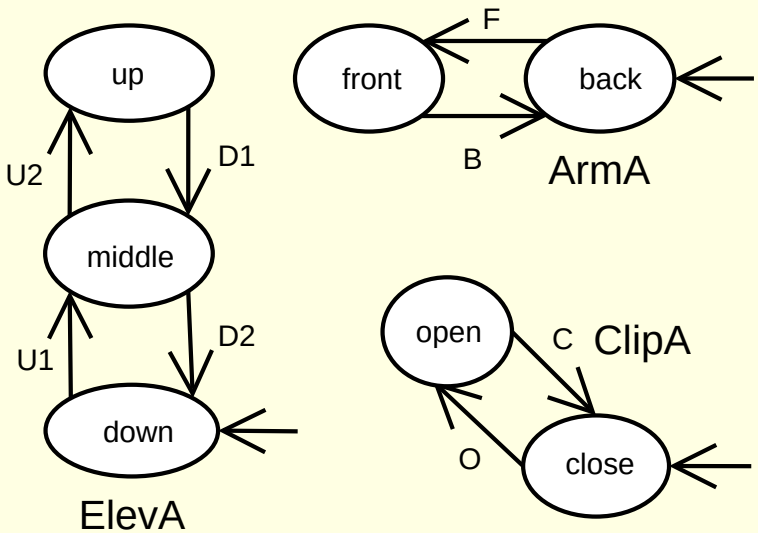
$$(S^1, S^2, Syn^c) = S^1 \times_{Syn^c} S^2 = [S^1] \cup [S^2]$$

Systèmes à composants : $[Arm_A]$



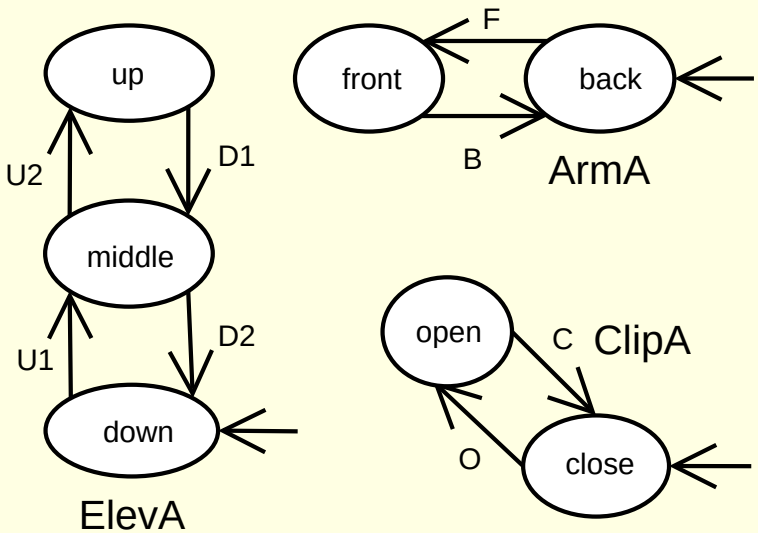
(-,O,-) **when** (ar=back $\wedge$ el=up) $\vee$ (ar=front $\wedge$ el=down),
(-,C,-) **when** (ar=front $\wedge$ el=up) $\vee$ (ar=back $\wedge$ el=down),
(F,-,-) **when** (cl=open $\wedge$ el=up) $\vee$ (cl=close $\wedge$ el=down),
(B,-,-) **when** (cl=close $\wedge$ el=up) $\vee$ (cl=open $\wedge$ el=down),
(F,O,-) **when** el=up,
(B,C,-) **when** el=down,
(B,C,U1) **when** true,
(-,-,U1) **when** cl=close $\wedge$ ar=back,
(-,-,U2) **when** cl=close $\wedge$ ar=back,
(-,-,D1) **when** cl=close $\wedge$ ar=back,
(-,-,D2) **when** cl=close $\wedge$ ar=back

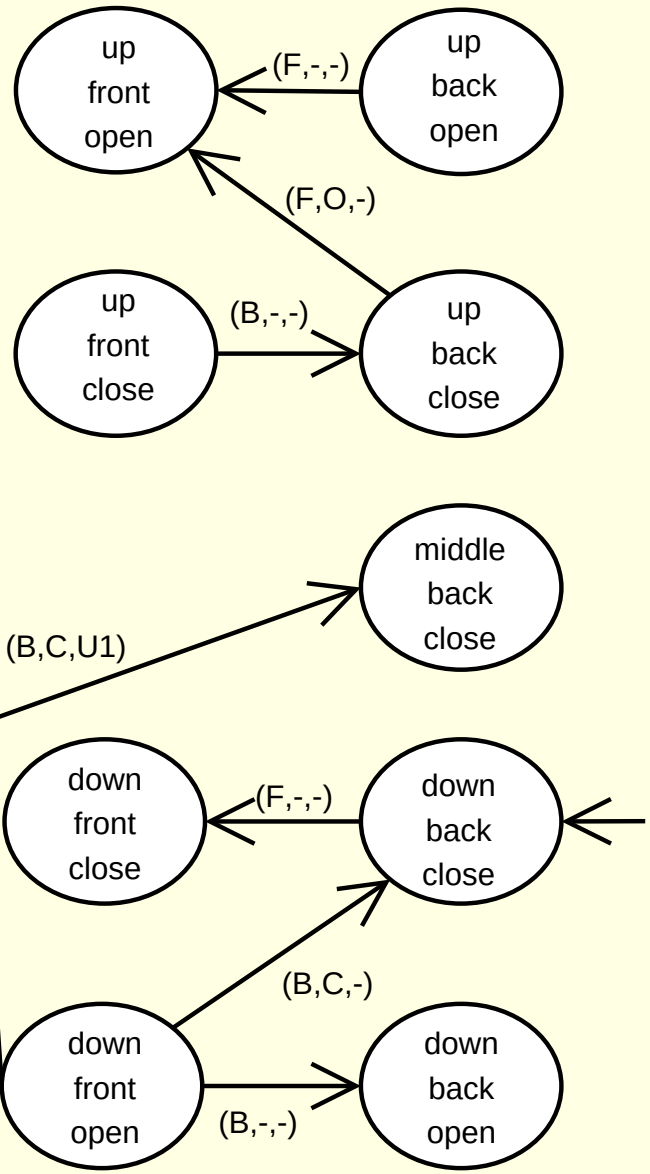
Systèmes à composants : $[Arm_A]$



(F,-,-) **when** (cl=open $\wedge$ el=up) $\vee$ (cl=close $\wedge$ el=down),
(B,-,-) **when** (cl=close $\wedge$ el=up) $\vee$ (cl=open $\wedge$ el=down),
(F,O,-) **when** el=up,
(B,C,-) **when** el=down,
(B,C,U1) **when** true,

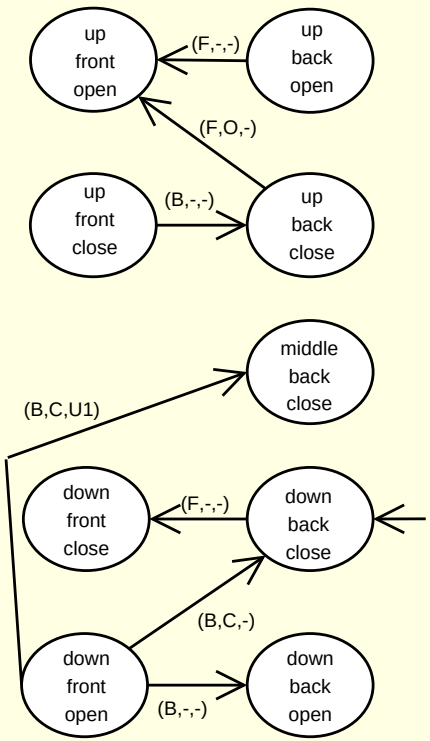
Systèmes à composants : $[Arm_A]$





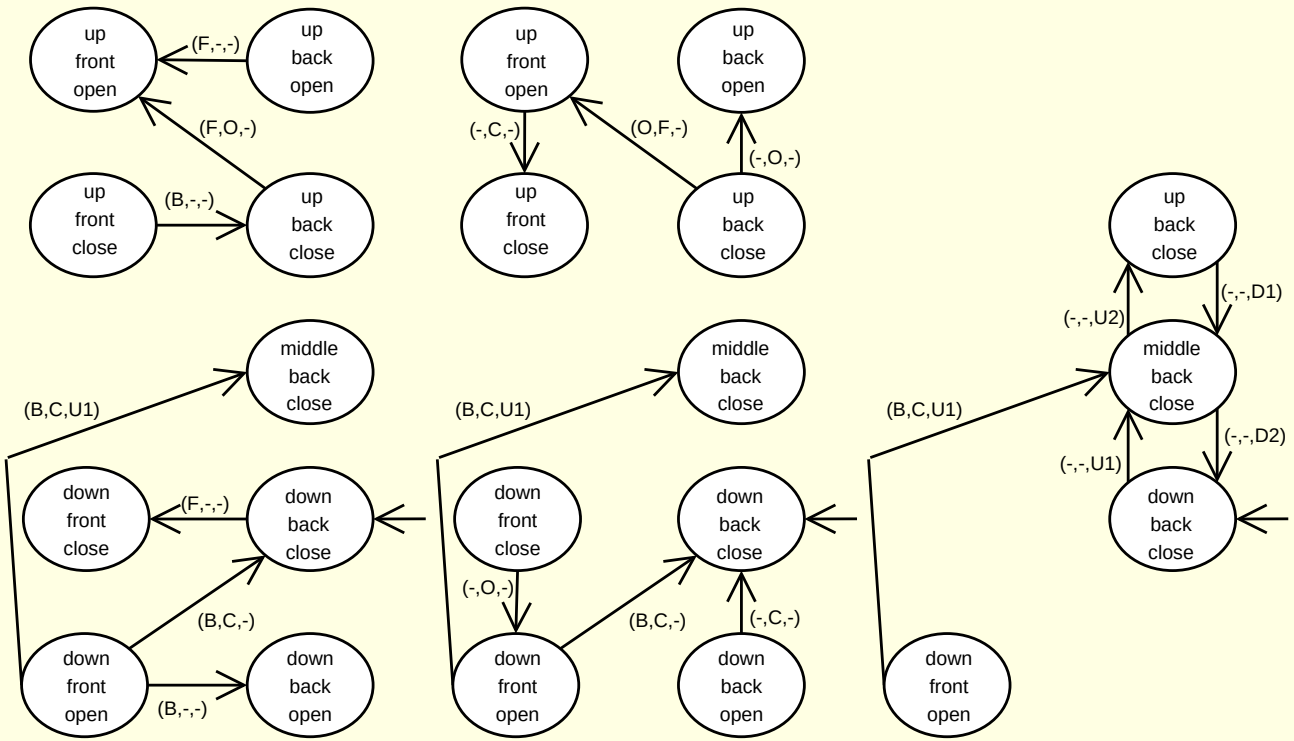
(F,-,-) **when** (cl=open $\wedge$ el=up) $\vee$ (cl=close $\wedge$ el=down),
(B,-,-) **when** (cl=close $\wedge$ el=up) $\vee$ (cl=open $\wedge$ el=down),
(F,O,-) **when** el=up,
(B,C,-) **when** el=down,
(B,C,U1) **when** true,

Systèmes à composants : décomposition



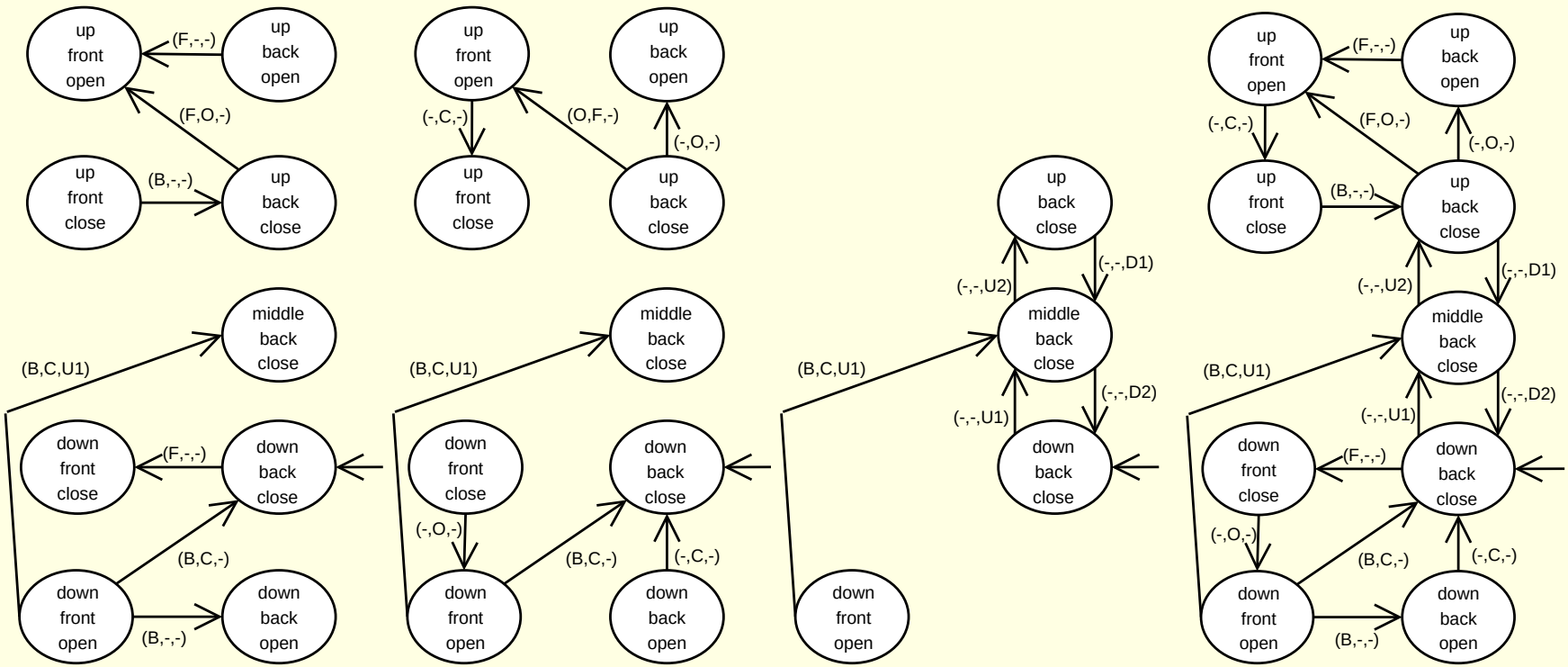
$$[Arm_A]$$

Systèmes à composants : décomposition



$$[Arm_A] \cup [Clip_A] \cup [Elev_A]$$

Systèmes à composants : décomposition



$$[Arm_A] \cup [Clip_A] \cup [Elev_A] = Robot_A$$

Systèmes à composants et raffinement

Soient (SA^1, SA^2, Syn^c_A) et (SR^1, SR^2, Syn^c_R).

$$\frac{[SR^1] \sqsubseteq^{D_1}_{\rho_w} [SA^1], \quad [SR^2] \sqsubseteq^{D_2}_{\rho_w} [SA^2]}{(SR^1, SR^2, Syn^c_R) \sqsubseteq^{D_1 \triangle D_2}_{\rho_w} (SA^1, SA^2, Syn^c_A)}$$

Pour avoir le **raffinement**, il reste à montrer que

- $\neg\, div^\tau(SR^1, SR^2, Syn^c_R)$?
- $D_1 \triangle D_2 = \varnothing$?

Systèmes à composants et raffinement : τ-cycles

Soit (SR^1, SR^2, Syn^c_R) un système à composants.

$$\left.\begin{array}{l} \neg\, div^\tau(SR^1) \\ \neg\, div^\tau(SR^2) \end{array}\right\} \text{ alors } \neg\, div^\tau(SR^1, SR^2, Syn^c_R)$$

Idée de preuve par contraposition : $(q_1, q_2) \xrightarrow{\tau} (q'_1, q'_2) \xrightarrow{\tau} (q_1, q_2)$ est un τ-cycle dans (SR^1, SR^2, Syn^c_R) :

- $q_1 = q'_1$ et $q_2 \xrightarrow{\tau} q'_2 \xrightarrow{\tau} q_2$
- $q_1 \xrightarrow{\tau} q'_1 \xrightarrow{\tau} q_1$ et $q_2 = q'_2$
- $q_1 \xrightarrow{\tau} q'_1 \xrightarrow{\tau} q_1$ et $q_2 \xrightarrow{\tau} q'_2 \xrightarrow{\tau} q_2$

Pour avoir $\neg\, div^\tau(SR^1)$, il suffit d'avoir $SR^1 \sqsubseteq_\eta SA^1$

Systèmes à composants et raffinement : blocages

Soit $[SR^1] \sqsubseteq^{D_1}_{\rho_w} [SA^1]$

On définit uniquement à partir de D_1 et de Syn^c_R l'ensemble RD_1 des blocages *réductibles* : $q_R \in RD_1$ ssi

- q_R appartient à D_1
- il existe dans Syn^c_R une transition de SR^2 *activable* depuis q_R

Systèmes à composants et raffinement : blocages

Soit $[SR^1] \sqsubseteq^{D_1}_{\rho_w} [SA^1]$

On définit uniquement à partir de D_1 et de Syn^c_R l'ensemble RD_1 des blocages *réductibles* : $q_R \in RD_1$ ssi

- q_R appartient à D_1
- il existe dans Syn^c_R une transition de SR^2 *activable* depuis q_R

Ensembles de blocages réductibles vs. réduction des blocages :

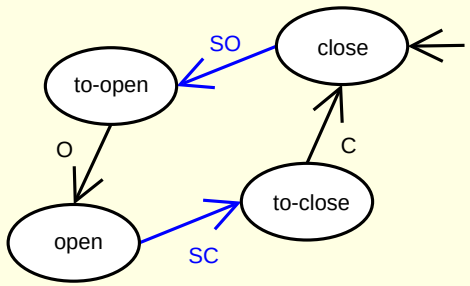
$$\left.\begin{array}{l} D_1 = RD_1 \\ D_2 = RD_2 \end{array}\right\} \Rightarrow D_1 \triangle D_2 = \varnothing$$

Systèmes à composants et raffinement

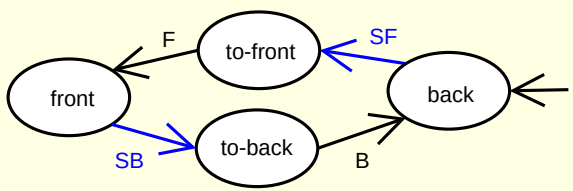
Théorème (raffinement d'un système à composants).
Soient $SA = (SA^1, SA^2, Syn^c_A)$
et $SR = (SR^1, SR^2, Syn^c_R)$

$$\frac{\begin{array}{ll} 1. & \neg\, div^\tau(SR^1),\ \neg\, div^\tau(SR^2) \\ 2. & [SR^1] \sqsubseteq^{D_1}_{\rho_w} [SA^1],\ D_1 = RD_1, \\ 3. & [SR^2] \sqsubseteq^{D_2}_{\rho_w} [SA^2],\ D_2 = RD_2 \end{array}}{SR \sqsubseteq_\eta SA}$$

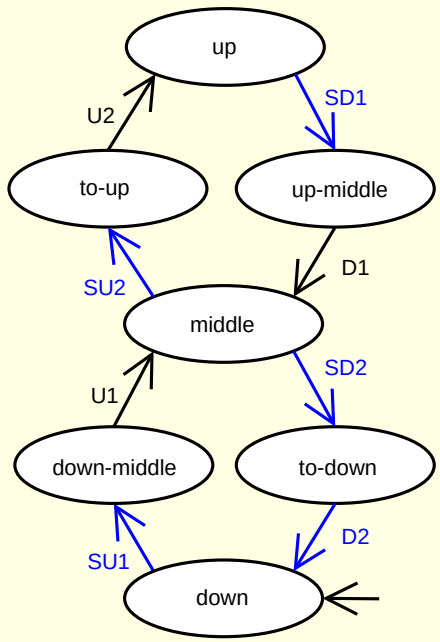
Systèmes à composants et raffinement : $[Arm_R]$



ClipR



ArmR

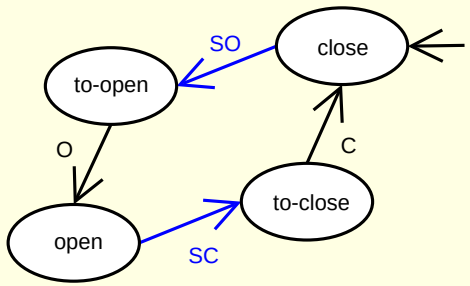


ElevR

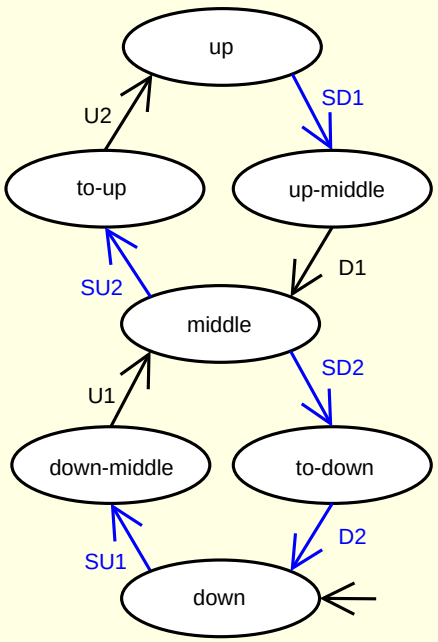
Nous constatons que $\neg\, div^{\tau}(ArmR)$, $\neg\, div^{\tau}(ClipR)$ et $\neg\, div^{\tau}(ElevR)$.

Nous donnons aussi Syn_R^C un ensemble raffiné de synchronisations contraintes.

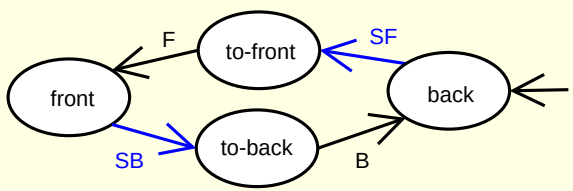
Systèmes à composants et raffinement : $[Arm_R]$



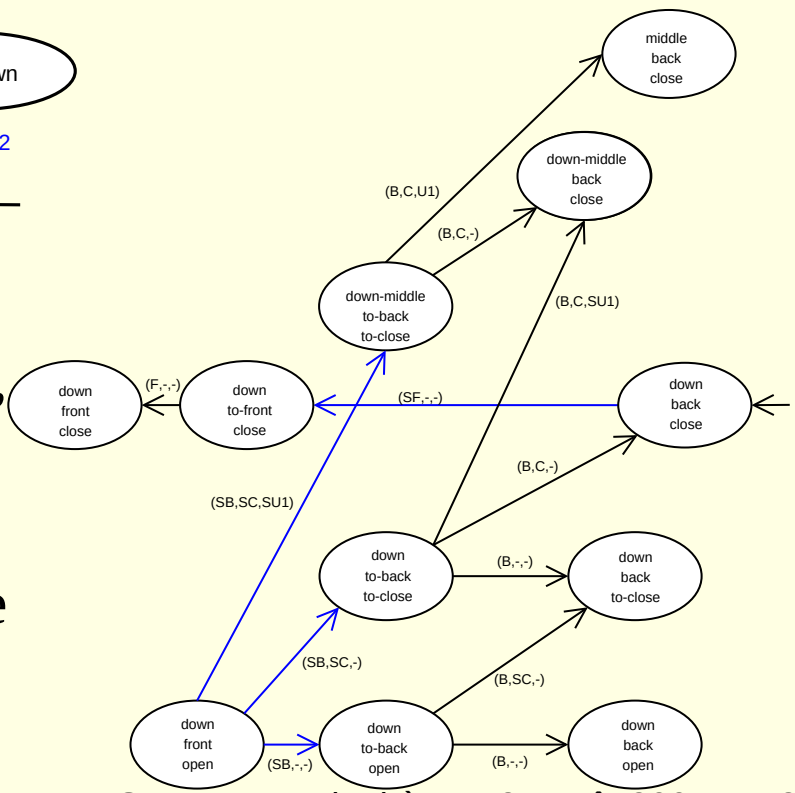
ClipR



ElevR

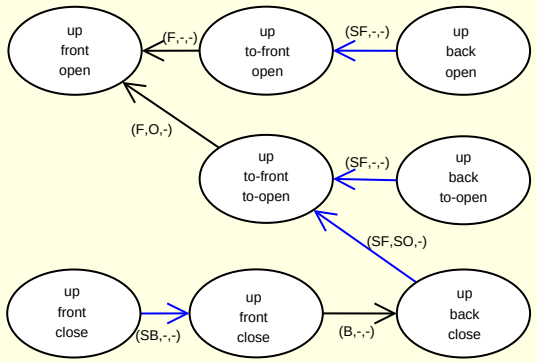


ArmR

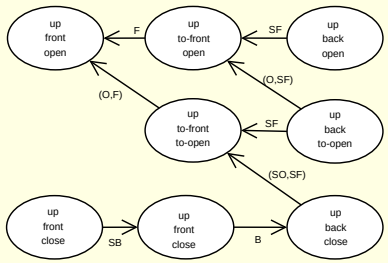


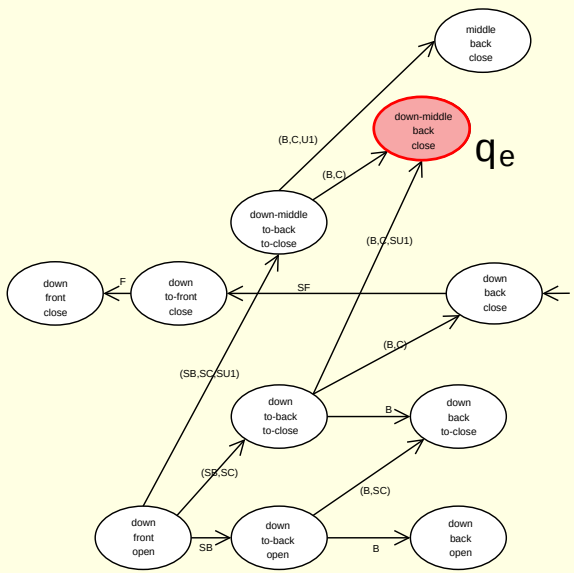
Nous constatons que $\neg\, div^{\tau}(ArmR)$, $\neg\, div^{\tau}(ClipR)$ et $\neg\, div^{\tau}(ElevR)$.

Nous donnons aussi Syn_R^C un ensemble raffiné de synchronisations contraintes.



Systèmes à composants et raffinement : $Robot_R$

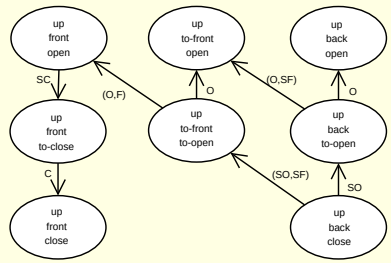


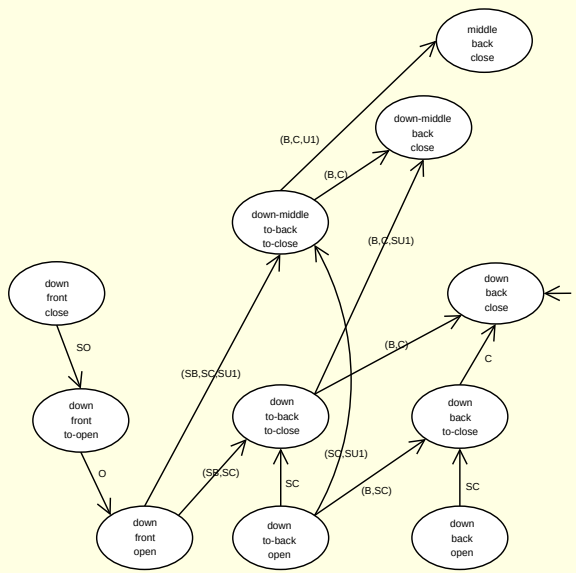


$$[Arm_R] \sqsubseteq^{D_A}_{\rho_w} [Arm_A]$$

$$D_A = \{q_e\} = RD_A$$

Systèmes à composants et raffinement : $Robot_R$

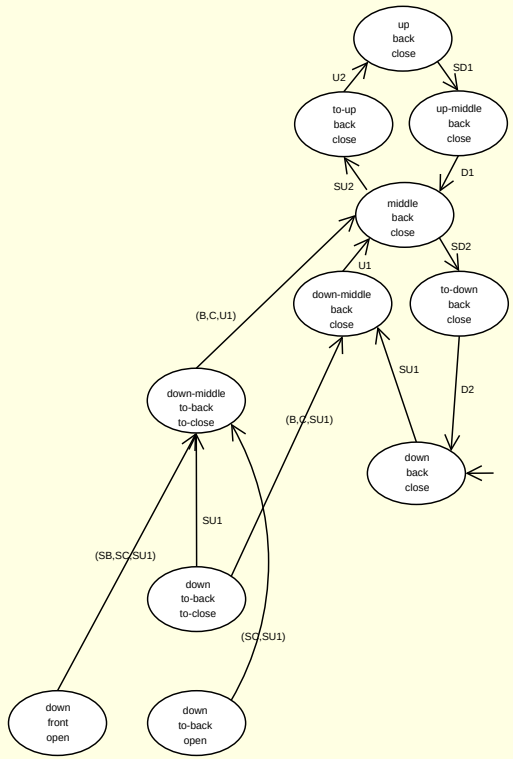




$$[Clip_R] \sqsubseteq_{\rho_w}^{D_C} [Clip_A]$$

$$D_C = \varnothing$$

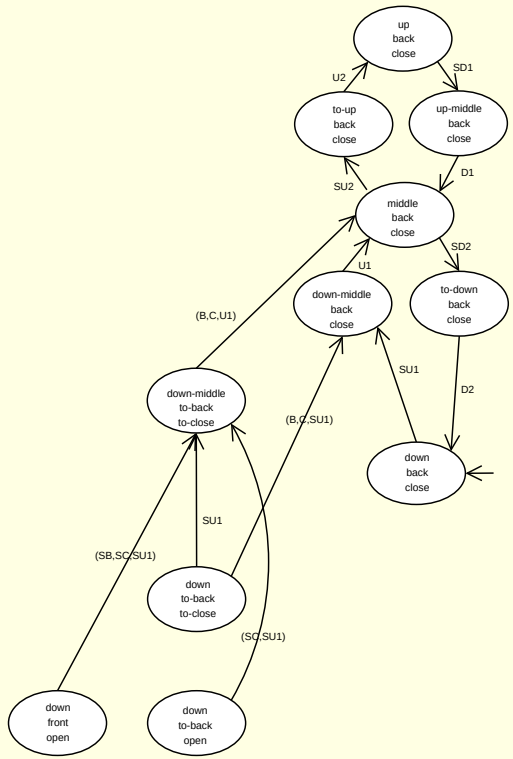
Systèmes à composants et raffinement : $Robot_R$



$$[Elev_R] \sqsubseteq_{\rho_w}^{D_E} [Elev_A]$$

$$D_E = \varnothing$$

Systèmes à composants et raffinement : $Robot_R$



$$[Elev_R] \sqsubseteq_{\rho_w}^{D_E} [Elev_A]$$
$$D_E = \varnothing$$

$$(Arm_R, Clip_R, Elev_R, Syn_R^c) \sqsubseteq_\eta (Arm_A, Clip_A, Elev_A, Syn_A^c)$$

Systèmes à composants et propriétés locales

- Préservation *par composition* des invariants locaux

$$\frac{SA^1 \models \Box sp_{A1},\ SA^2 \models \Box sp_{A2}}{(SA^1, SA^2, Syn^c_A) \models \Box(sp_{A1} \wedge sp_{A2})}$$

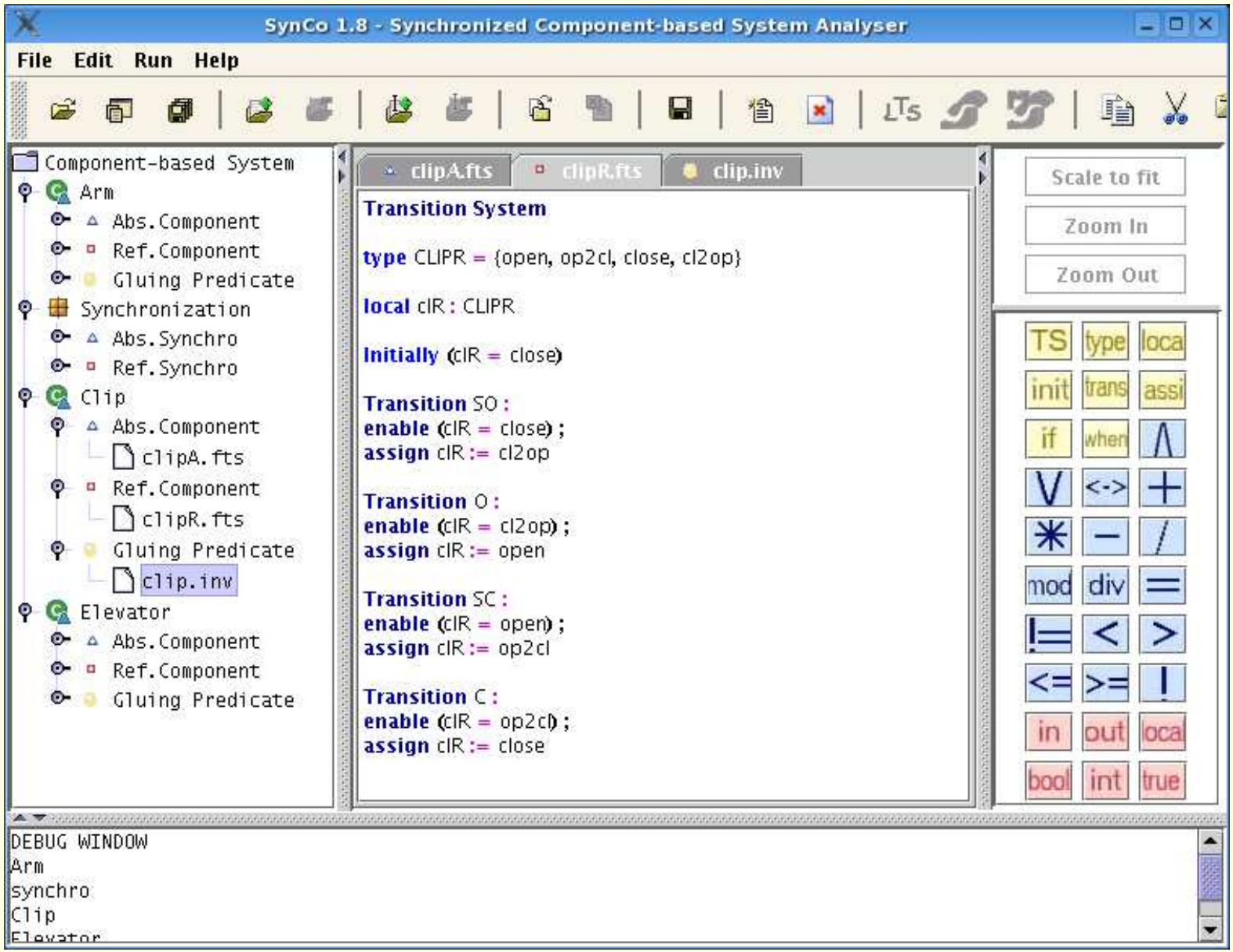
- Préservation des propriétés LTL de sûreté
  - si $\phi \in LTL_{surete}$ et si $SA^1 \models \phi$ alors $(SA^1, SA^2, Syn^c_A) \models \phi$,
  - Si $\phi_s \wedge \phi_l \in LTL$ et si $SA^1 \models \phi_s \wedge \phi_l$ alors $(SA^1, SA^2, Syn^c_A) \models \phi_s$

Systèmes à composants et propriétés globales

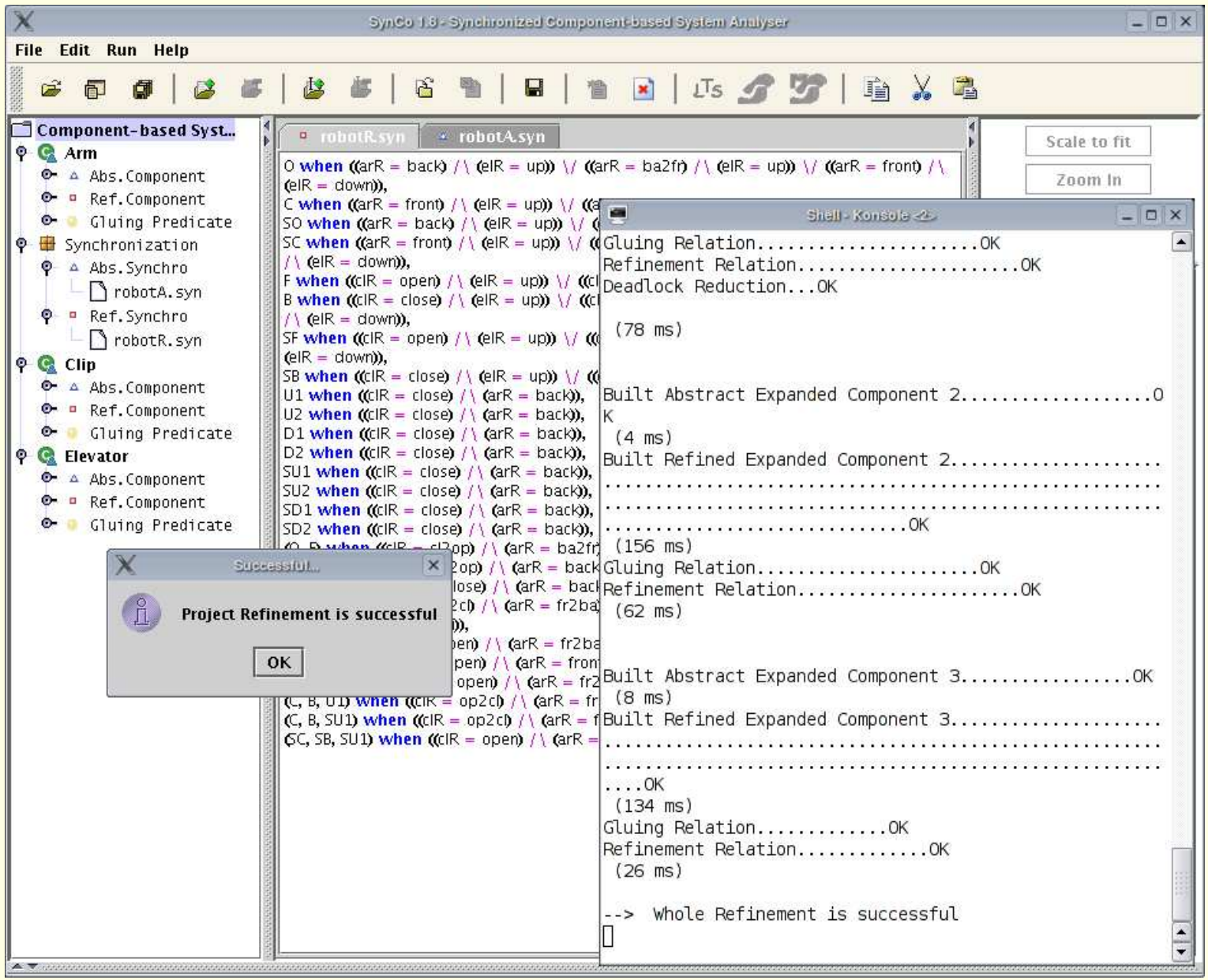
Préservation par *décomposition* des propriétés *globales* puisque $(S^1, S^2, Syn^c) = [S^1] \cup [S^2]$

- invariants
- invariants dynamiques
- non-satisfaction des propriétés LTL de sûreté
- atteignabilité compositionnelle

Systèmes à composants : implantation SynCo



Systèmes à composants : implantation SynCo



Systèmes à composants : implantation SynCo

LIFC

UNIVERSITÉ DE FRANCHE-COMTÉ

Bras mobile robotisé

	$\|Q\| + \|T\|$
$[Arm_A]$	9+7=16
$[Clip_A]$	9+7=16
$[Elev_A]$	4+5=9
SA	**9+15=24**
$[Arm_R]$	19+19=38
$[Clip_R]$	*19+20=39*
$[Elev_R]$	11+12=23
SR	**24+40=64**

Essuyage-avant

	$\|Q\| + \|T\|$
$[Comodo_A]$	5+10=15
$[Sensor_A]$	5+14=19
$[Left_A]$	7+6=13
$[Right_A]$	7+6=13
SA	**8+22=30**
$[Comodo_R]$	8+17=25
$[Sensor_R]$	10+25=35
$[Left_R]$	*18+20=38*
$[Right_R]$	*18+20=38*
SR	**20+47=67**

CEPS

	$\|Q\| + \|T\|$
$[Card_A]$	10+18=28
$[Load_A]$	5+6=11
$[Pos_A]$	7+11=18
SA	**10+18=28**
$[Card_R]$	*544+561=1105*
$[Load_R]$	182+188=370
$[Pos_R]$	378+402=780
SR	**544+705=1249**

Conclusion et perspectives : contributions

- Démarche générale de raffinement par décomposition
  - Relation affaiblie de raffinement
  - Théorème de raffinement par décomposition
  - Propriétés et décomposition : invariant et invariant dynamique
- Raffinement systèmes à composants synchronisés
  - Systèmes à composants <-> décomposition
  - Adaptation du raffinement par décomposition
    -> raffinement compositionnel des systèmes à composants
  - Préservation par composition des propriétés LTL de sûreté
  - Implantation d'un prototype SynCo

Conclusion et perspectives : publications

- 2 publications en conférences internationales
  - O. Kouchnarenko, A. Lanoix. Refinement and verification of synchronized component-based systems. *Formal Methods (FM'03)*.
  - O. Kouchnarenko, A. Lanoix. Verifying invariants of component-based systems through refinement. *Algebraic Methodology And Software Technology (AMAST'04)*.
- 1 publication en conférence nationale
  - O. Kouchnarenko, A. Lanoix. Raffinement de systèmes à composants synchronisés. *Modélisation des systèmes réactifs (MSR'03)*.
- 2 publications en session outils
  - O. Kouchnarenko, A. Lanoix. SynCo: a refinement analysis tool for synchronized component-based systems. *FM'03 Tool Exhibition Notes*.
  - A. Lanoix. SynCo: vérification du raffinement des systèmes à composants synchronisés. *Session outils, AFADL'04*.
- 2 autres communications
  - A. Lanoix. A compositional framework using refinement. *MOVEP'04*.
  - A. Lanoix. Vérifier le raffinement de manière compositionnelle. *MAJECSTIC'04*.

Conclusion et perspectives : perspectives

- Améliorer SynCo pour pouvoir passer à l'échelle et valider notre approche sur des études de cas industrielles
- Etendre la démarche à d'autres modèles
  - décomposition <-> systèmes à variables partagées sous-système = module [Kupferman, Vardi 96, Alur 99]
  - raffinement des systèmes à composants <-> raffinement de systèmes communicants [Sidorova et al.]
- Etudier le raffinement par ajout de nouveaux composants : $SA^1 \| SA^2 \sqsubseteq SA^1$ (systèmes non-bloquants -> [Sifakis 03])