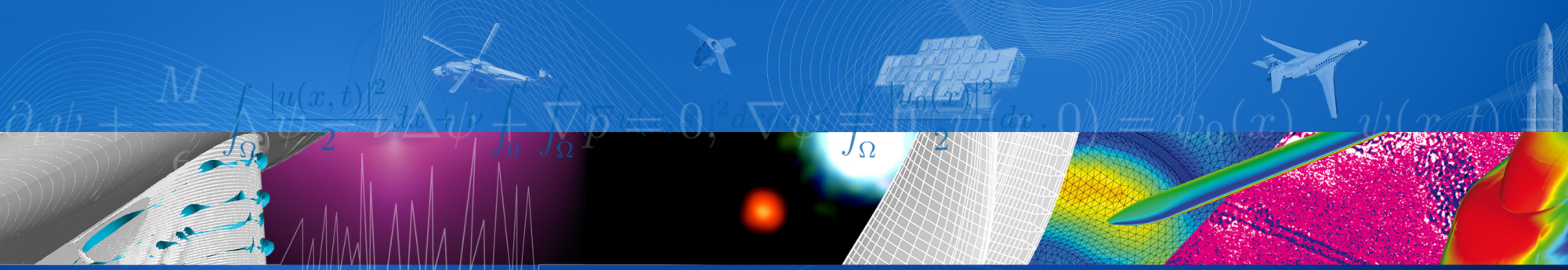


Synthèse automatique d'architectures tolérantes aux fautes

Jury de soutenance

Mireille BAYART	Prof. CRIStAL	Daniel LE BERRE	Prof. CRIL
Pierre BIEBER	Ing. ONERA	Yves LEDRU	Prof. LIG
Sylvain CONCHON	Prof. LRI	Karama KANOUN	DR LAAS

Claire PAGETTI & Rémi DELMAS — Ing. ONERA

Kevin Delmas

19 Décembre 2017

ONERA
THE FRENCH AEROSPACE LAB

Conception des systèmes critiques

Processus de conception guidée par la sûreté

1. Identification des événements redoutés et de leur gravité
   - danger pour les utilisateurs, pour l'environnement, etc
2. Formulation d'exigences de sûreté
   - formulation guidée par des standards (ARP4754, ISO26262,...)
3. Conception d'une architecture du système
4. Modélisation des défaillances du système
5. Analyses de la sûreté de fonctionnement

Conception des systèmes critiques

Processus de conception guidée par la sûreté

1. Identification des événements redoutés et de leur gravité
   - danger pour les utilisateurs, pour l'environnement, etc
2. Formulation d'exigences de sûreté
   - formulation guidée par des standards (ARP4754, ISO26262,...)
3. Conception d'une architecture du système
4. Modélisation des défaillances du système
5. Analyses de la sûreté de fonctionnement

Conception des systèmes critiques

Processus de conception guidée par la sûreté

1. Identification des événements redoutés et de leur gravité
   - danger pour les utilisateurs, pour l'environnement, etc
2. Formulation d'exigences de sûreté
   - formulation guidée par des standards (ARP4754, ISO26262,...)
3. Conception d'une architecture du système
4. Modélisation des défaillances du système
5. Analyses de la sûreté de fonctionnement

Plan

1. Contexte

2. Contributions

   Définition de KCR

   Résolution du problème DSE

3. Expérimentations

4. Conclusion

Plan

1. Contexte

2. Contributions

   Définition de KCR

   Résolution du problème DSE

3. Expérimentations

4. Conclusion

Introduction à la modélisation dysfonctionnelle

Objectif : Modéliser les pannes des composants et leurs effets sur le système

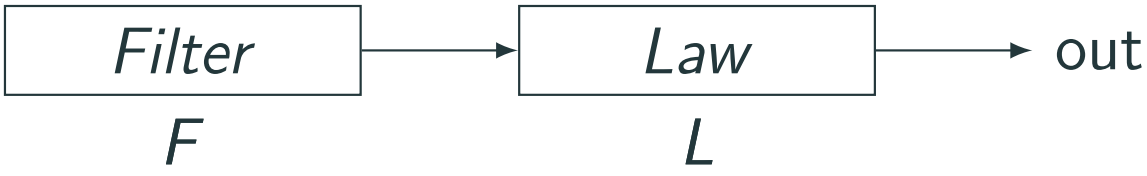
Terminologie

- événement (de défaillance) : défaut spontané,
- mode (de défaillance) : manifestation de la panne.

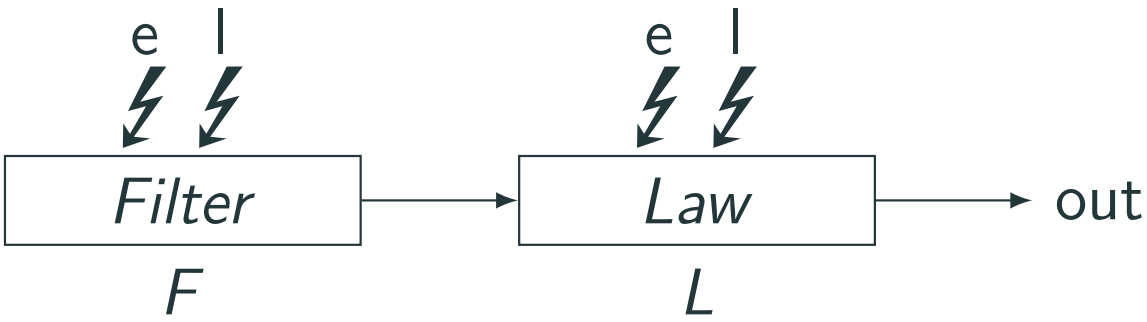
Modélisation

1. définir les événements et modes de chaque composant
2. établir les modes perçus en sortie en fonction des modes d'entrée et des événements
3. modèle système $\Rightarrow$ assemblage de modèles de ses sous-composants

Système fil rouge : Modélisation



Système fil rouge : Modélisation



Événements : e et l

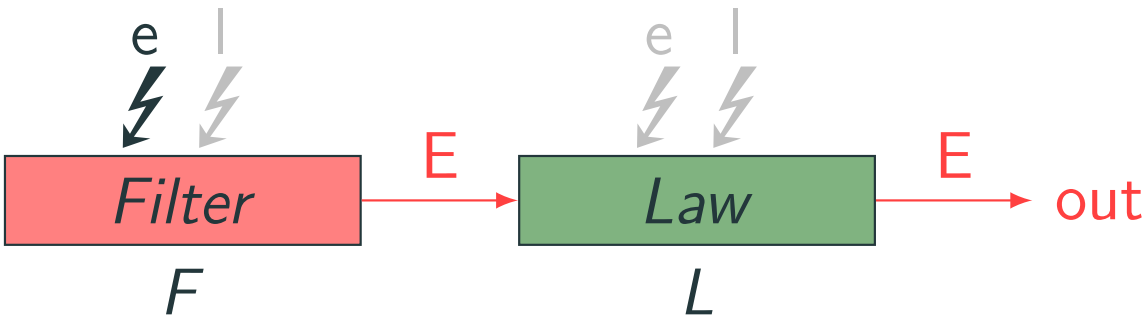
Modes :

- **E** composant produit des données erronées,
- **L** composant cesse de produire des données.

Règles de propagations :

1. si **e** se produit alors **données erronées** en sortie,
2. sinon si **l** se produit alors **absence de données** en sortie,
3. sinon mode en entrée transmis en sortie (pour Law).

Système fil rouge : Modélisation



Événements : e et l

Modes :

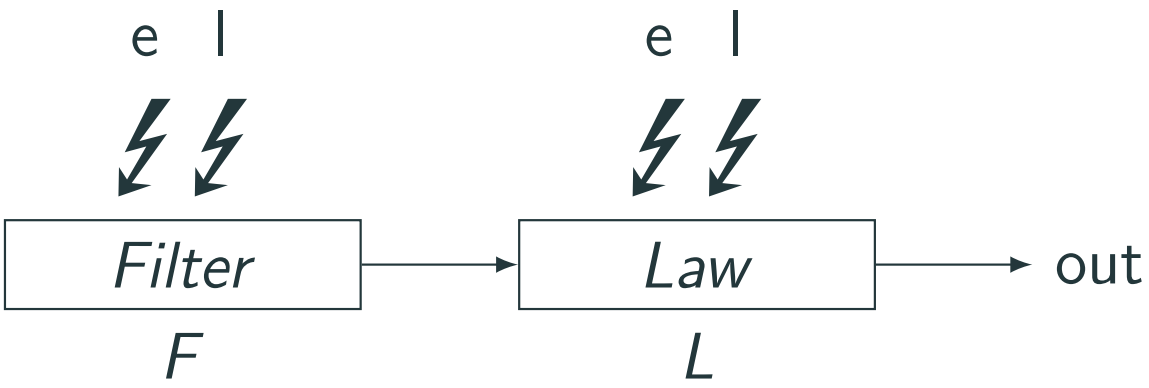
E composant produit des données erronées,

L composant cesse de produire des données.

Règles de propagations :

1. si **e** se produit alors **données erronées** en sortie,
2. sinon si **l** se produit alors **absence de données** en sortie,
3. sinon mode en entrée transmis en sortie (pour Law).

Système fil rouge : Analyse



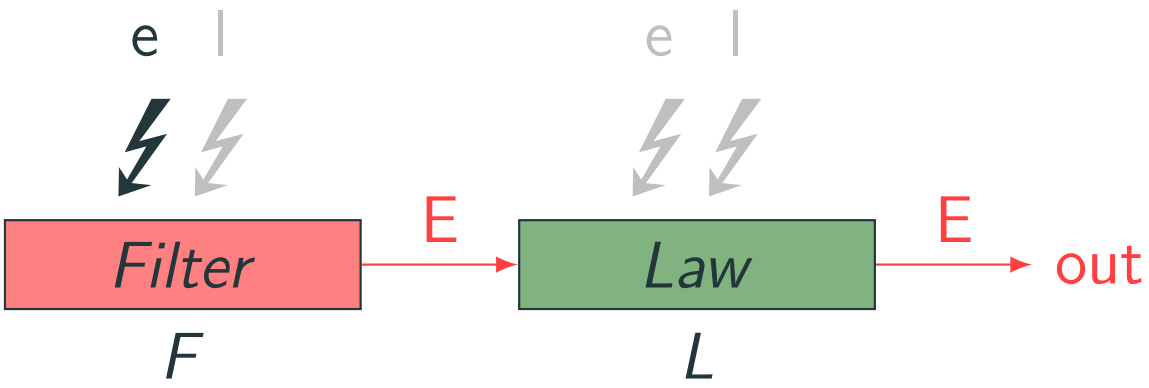
Redouté Production données erronées ou absentes

Ordre nombre minimal d'événements pour déclencher événement redouté,

Fiabilité (R) probabilité que le système ne soit pas défaillant sur un intervalle de temps $[0, t]$.

$R(1)$ *ordre*

Système fil rouge : Analyse



Redouté Production données erronées ou absentes

Ordre nombre minimal d'événements pour déclencher événement redouté,

Fiabilité (R) probabilité que le système ne soit pas défaillant sur un intervalle de temps $[0, t]$.

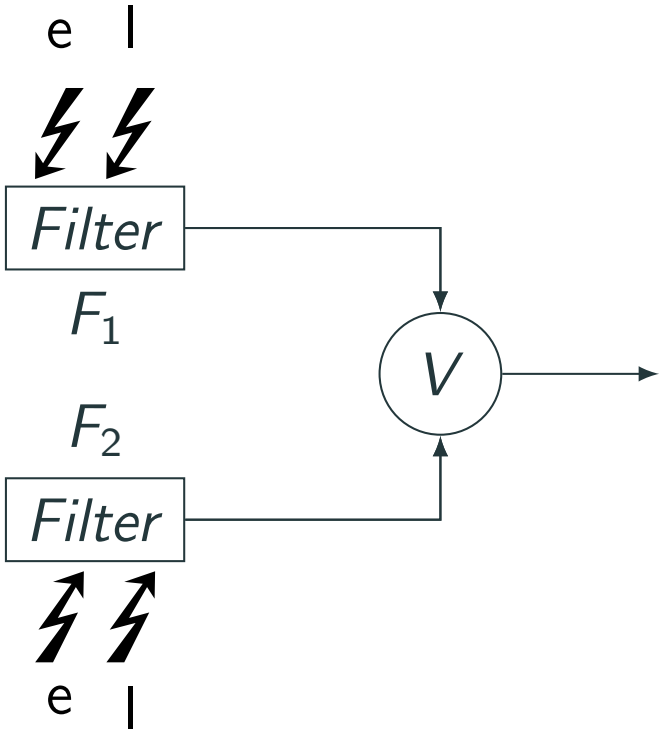
$$R(1) \overset{\text{indépendance}}{=} p(\overline{F.e})p(\overline{F.l})p(\overline{L.e})p(\overline{L.l}) \approx 0,96 \qquad ordre = 1$$

Confrontation aux exigences

Exigences Production données erronées ou absentes ssi :

$$\left.\begin{array}{l} ordre \geq 1 \\ R(1) \geq 0,99 \end{array}\right\} \text{non respectées par architecture initiale}$$

Patron de sûreté constructions améliorant la sûreté :

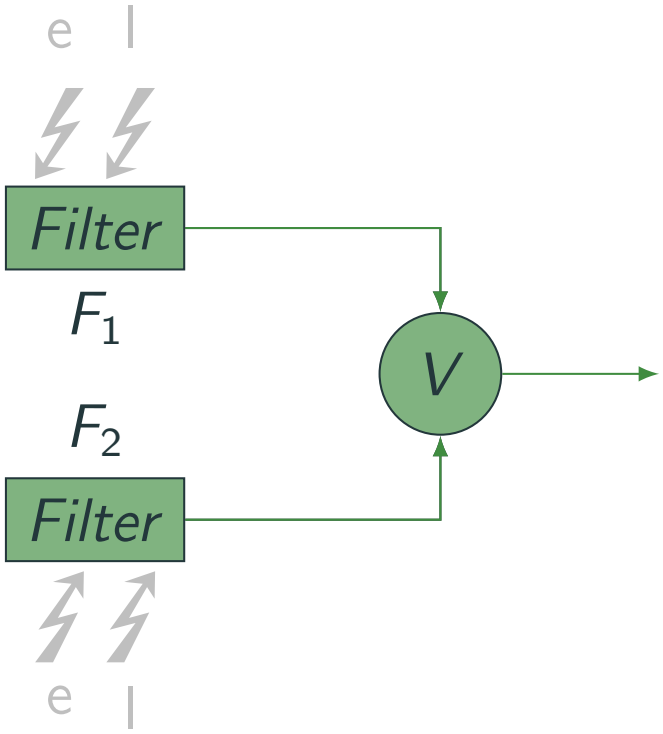


Confrontation aux exigences

Exigences Production données erronées ou absentes ssi :

$$\left.\begin{array}{l} ordre \geq 1 \\ R(1) \geq 0,99 \end{array}\right\} \text{non respectées par architecture initiale}$$

Patron de sûreté constructions améliorant la sûreté :

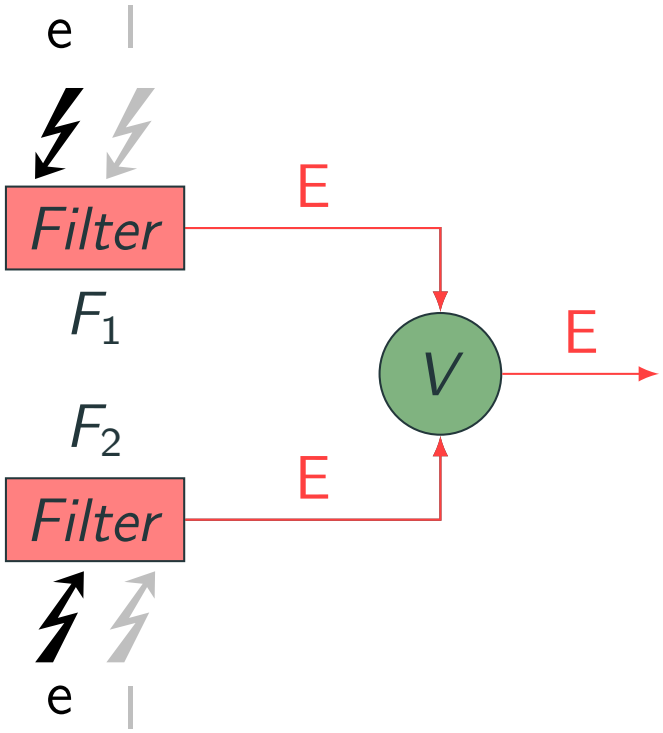


Confrontation aux exigences

Exigences Production données erronées ou absentes ssi :

$$\left.\begin{array}{l} ordre \geq 1 \\ R(1) \geq 0,99 \end{array}\right\} \text{non respectées par architecture initiale}$$

Patron de sûreté constructions améliorant la sûreté :

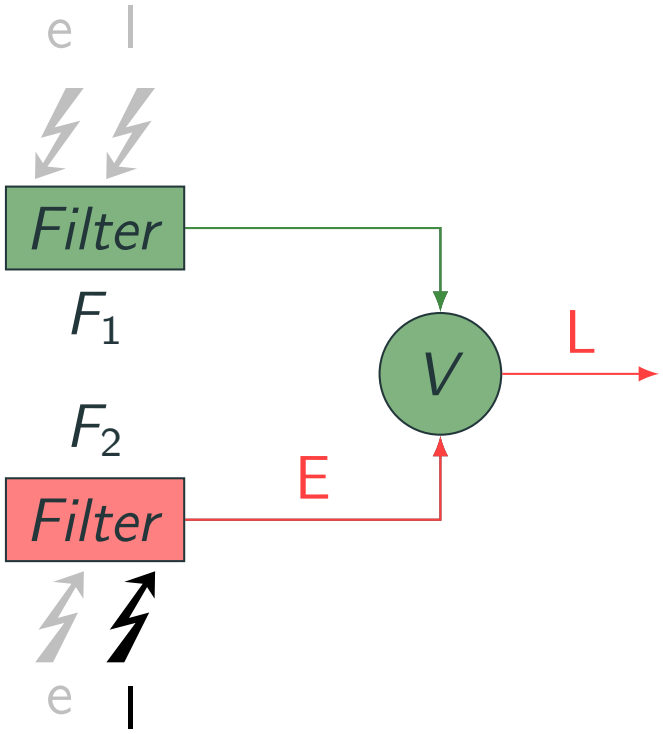


Confrontation aux exigences

Exigences Production données erronées ou absentes ssi :

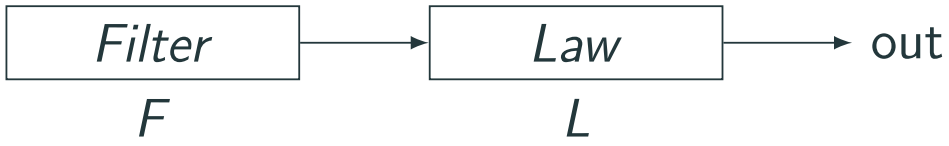
$$\left.\begin{array}{l} ordre \geq 1 \\ R(1) \geq 0,99 \end{array}\right\} \text{non respectées par architecture initiale}$$

Patron de sûreté constructions améliorant la sûreté :



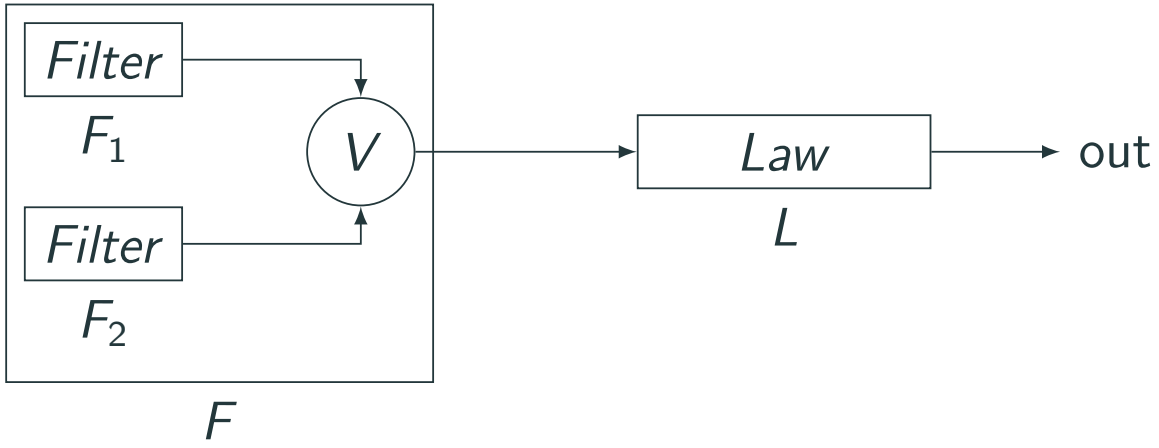
Exploration de l'espace des architectures (DSE)

Objectif Trouver une architecture obtenue par substitution composant/patron satisfaisant les exigences de sûreté.



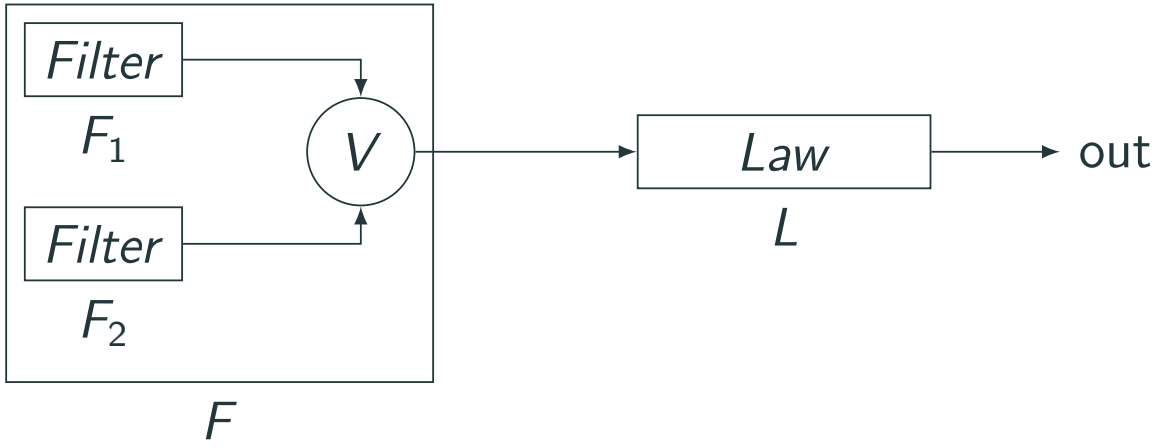
Exploration de l'espace des architectures (DSE)

Objectif Trouver une architecture obtenue par substitution composant/patron satisfaisant les exigences de sûreté.



Exploration de l'espace des architectures (DSE)

Objectif Trouver une architecture obtenue par substitution composant/patron satisfaisant les exigences de sûreté.



Problème d'exploration de l'espace des architectures (DSE : Design Space Exploration) :

- **candidat** : architecture obtenue par substitution de composant/patron dans l'architecture initiale,
- **espace des architectures** : candidats possibles.

Idée centrale

Défis

- problème combinatoire $\Rightarrow$ explosion de la taille de l'espace des architectures,
- itération modélisation & analyse manuelle $\Rightarrow$ trop lent,
- choisir le « bon » patron est difficile $\Rightarrow$ dépend du composant remplacé, du système et du *coût*.

Idée centrale

Défis

- problème combinatoire $\Rightarrow$ explosion de la taille de l'espace des architectures,
- itération modélisation & analyse manuelle $\Rightarrow$ trop lent,
- choisir le « bon » patron est difficile $\Rightarrow$ dépend du composant remplacé, du système et du *coût*.

Développer une méthode de résolution automatique du problème DSE fondée sur la résolution de problèmes SMT

Introduction à la Satisfiabilité Modulo Théories

Objectif Décider de la **S**atisfiabilité d'un ensemble de formules logiques **M**odulo des **T**héories.

Introduction à la Satisfiabilité Modulo Théories

Objectif Décider de la **S**atisfiabilité d'un ensemble de formules logiques **M**odulo des **T**héories.

$$x \geq 0 \wedge y = x + 1 \wedge (y > 2 \vee y < 1)$$

Existe-t-il une valeur de x et y telle que la formule soit vraie ?

Introduction à la Satisfiabilité Modulo Théories

Objectif Décider de la **S**atisfiabilité d'un ensemble de formules logiques **M**odulo des **T**héories.

$$x \geq 0 \wedge y = x + 1 \wedge (y > 2 \vee y < 1)$$

Existe-t-il une valeur de x et y telle que la formule soit vraie ?

Résolution En considérant des théories décidables :

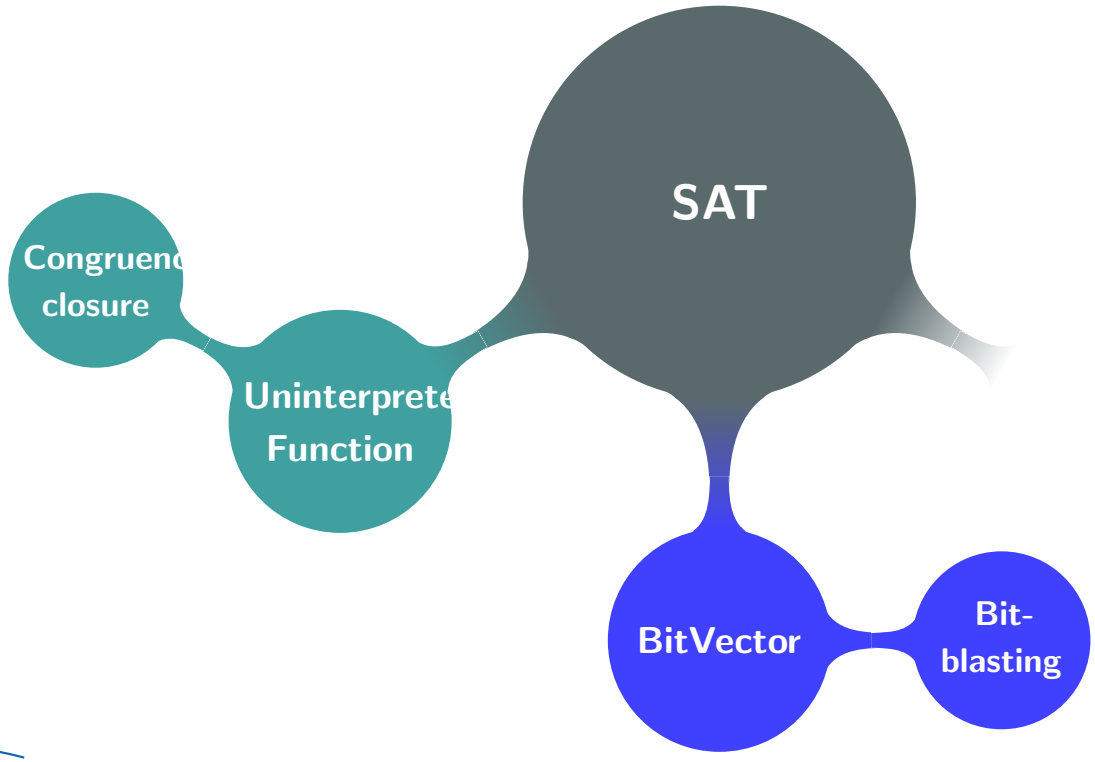
- problème est $\textsc{Sat}$ $\rightarrow$ valeur de x et y (modèle),
- problème est $\textsc{Unsat}$ $\rightarrow$ preuve (si disponible),

Résolution problème SMT

Problème Comment formuler le problème DSE et traiter les contraintes sur des indicateurs ?

Objectifs

- Formaliser le problème DSE avec SMT,
- Développer une théorie traitant les contraintes de sûreté.

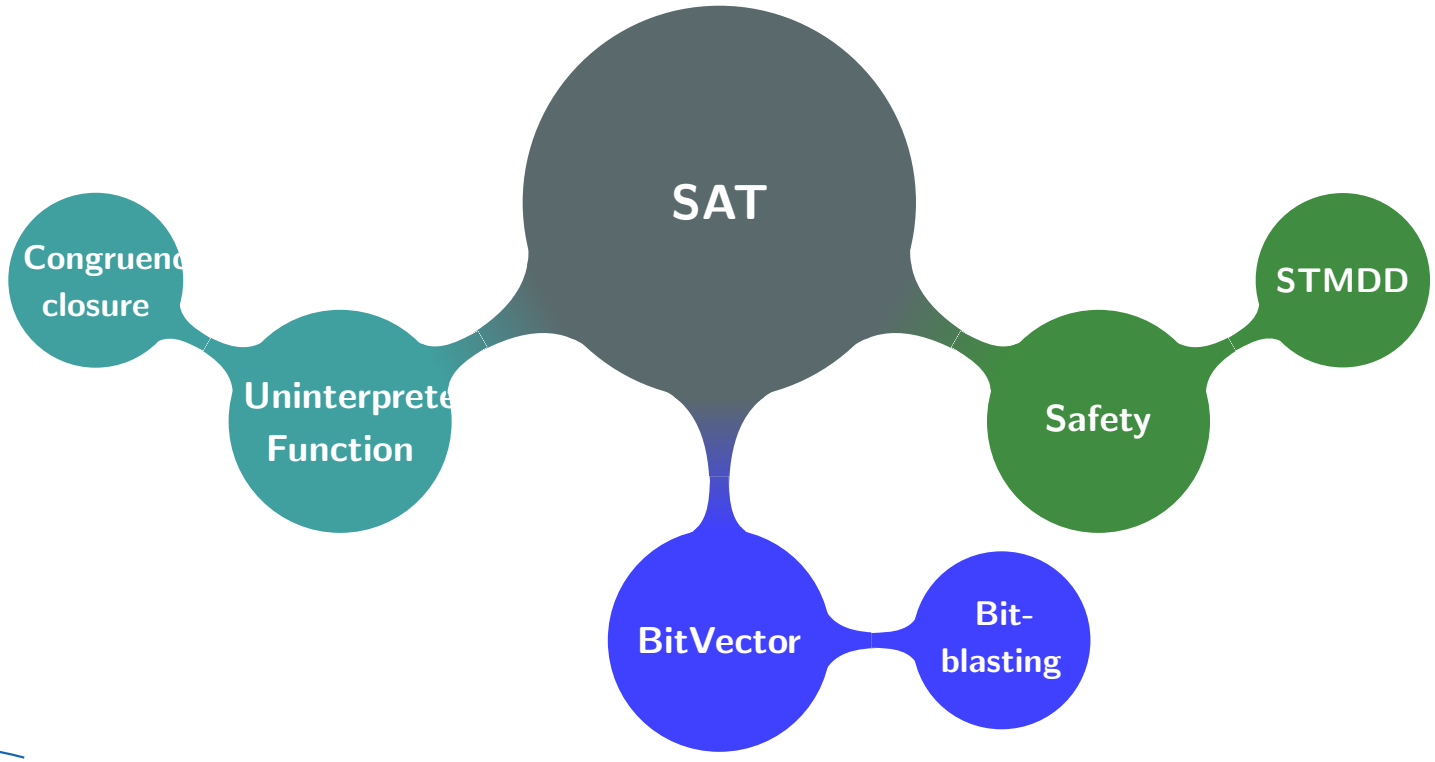


Résolution problème SMT

Problème Comment formuler le problème DSE et traiter les contraintes sur des indicateurs ?

Objectifs

- Formaliser le problème DSE avec SMT,
- Développer une théorie traitant les contraintes de sûreté.



Plan

1. Contexte

2. Contributions

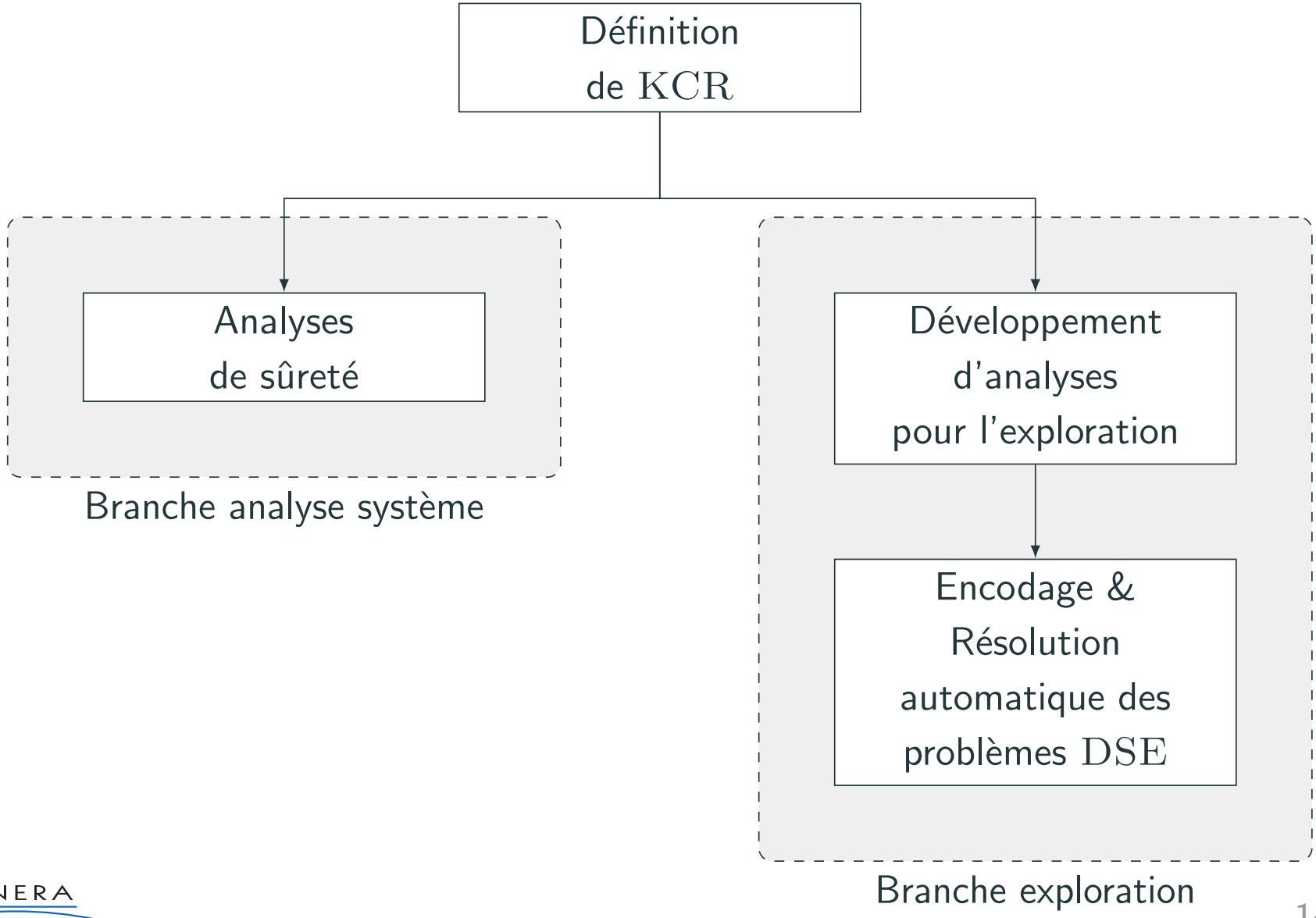
   Définition de KCR

   Résolution du problème DSE

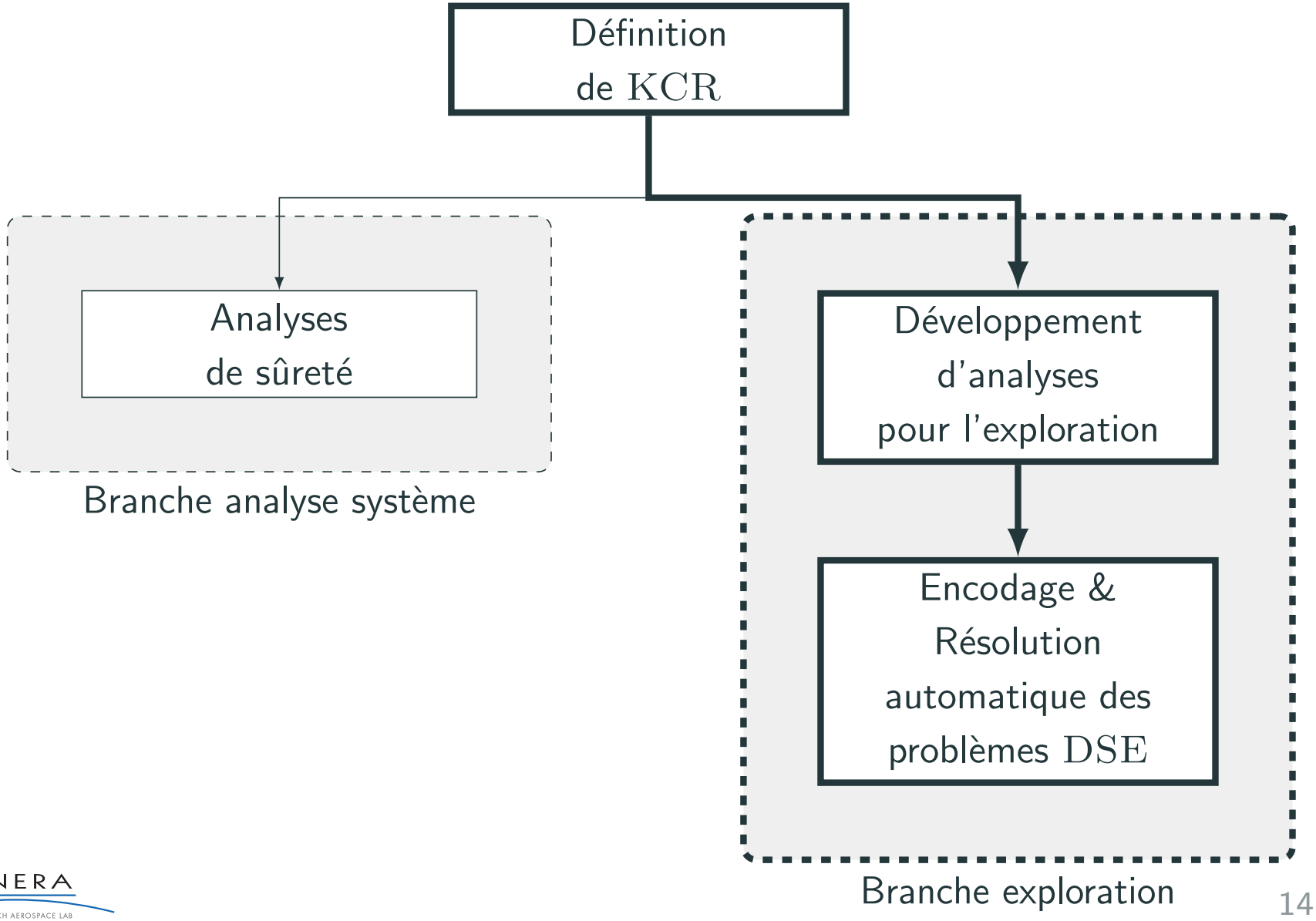
3. Expérimentations

4. Conclusion

Contributions



Contributions



Plan

1. Contexte

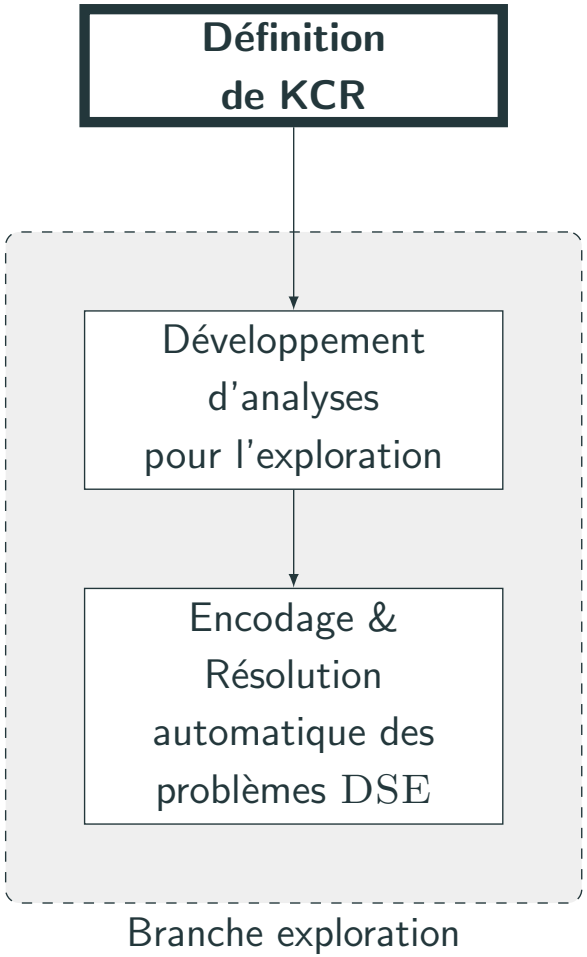
2. Contributions

   Définition de KCR

   Résolution du problème DSE

3. Expérimentations

4. Conclusion



Cadre de modélisation

Hypothèses de modélisation

- **Statique** : État dysfonctionnel indépendant de l'ordre d'arrivée des événements,
- **Non réparable** : Composant défaillant ne peut retourner dans état fonctionnel.

Objectif langage de modélisation :

- pour décrire les systèmes statiques,
- formuler les exigences et les patrons utilisables,
- avec notion de composant,
- séparant modèle et exigences.

Langages existants

Dynamiques	Statiques
ALTARICA [APGR99]	HIPHOPS [APS+11]
+ modélisation fine des défaillances	+ systèmes statiques par construction
+ notion de composant	+ analyses efficaces
− analyses coûteuses	− pas de notion de composant

$\Downarrow$

Langages existants

Dynamiques	Statiques
ALTARICA [APGR99]	HIPHOPS [APS+11]
+ modélisation fine des défaillances	+ systèmes statiques par construction
+ notion de composant	+ analyses efficaces
− analyses coûteuses	− pas de notion de composant

$\Downarrow$

Définir un nouveau langage appelé KCR

- inspiré par la description modulaire de ALTARICA,
- inspiré par la modélisation statique de HIPHOPS.

Fil rouge : Modélisation avec KCR

Modes de défaillances

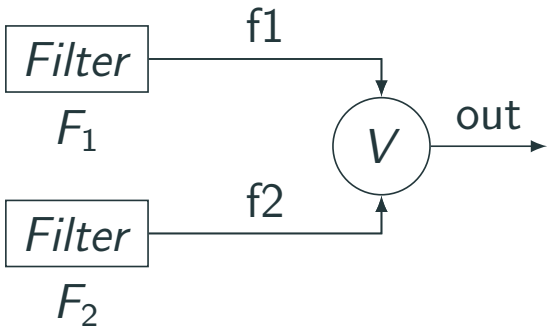
```
type fm := {E, L};
```

f :fm $\Rightarrow$ modes observables sur f sont {empty, E, L , E + L}

Composant

```
primary comp Filter() returns (out:fm) {
  evts: e, l ;
  defs:
   out := if e then E
          else if l then L
          else empty; };
```

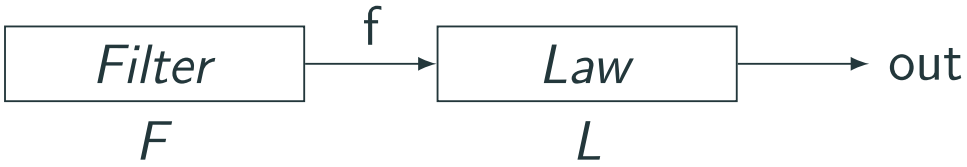
Fil rouge : Modélisation avec KCR



Composant alternatif

```
comp DupFilter() returns (out:fm) {
  locs: f1, f2:t;
  defs:
   f1 := Filter@F1();
   f2 := Filter@F2();
   out := if f1=empty & f2=empty then empty
          else if f1=E & f2=E then E
          else L;
};
```

Fil rouge : Modélisation avec KCR



Système

```
comp System() returns (out:fm) {
  locs: f:t;
  defs: f := Filter@F();
        out := Law@L(f);
};
```

Fil rouge : Modélisation avec KCR

Configuration

```
config C {
 //donnees de calcul
 root:=System; failure:= out!=empty; duration:=1;
 //exigences
 minorder:=1;  minreliability:=0.99;
 //espace des architectures
 design space {
  L-> {Law(e=0.01, l=0.01),
       DupLaw(L1.e=0.001, L1.l=0.001,
              L2.e=0.001, L2.l=0.001)};
  F-> {Filter(e=0.01, l=0.01),
       DupFilter(F1.e=0.001, F1.l=0.001,
                 F2.e=0.001, F2.l=0.001)};};
};
```

Plan

1. Contexte

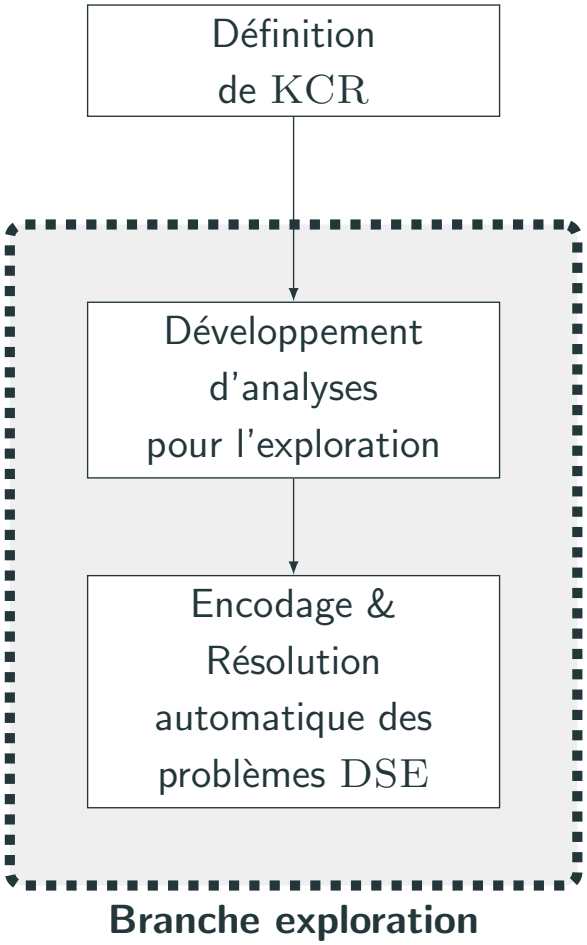
2. Contributions

   Définition de KCR

   Résolution du problème DSE

3. Expérimentations

4. Conclusion



Méthodes existantes de résolution du problème DSE

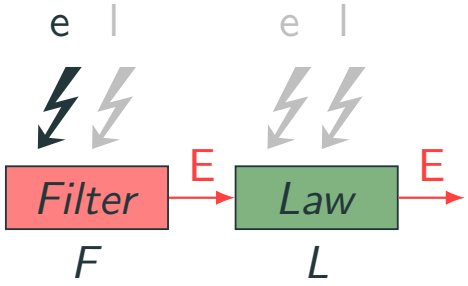
Programmation par contraintes : Modélisation problème DSE comme ensemble de contraintes $\Rightarrow$ résolution déléguée aux solveurs [Bil08]

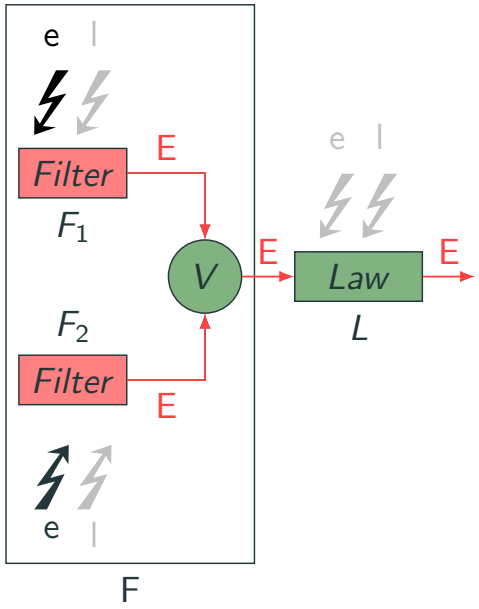
- \+ Garantie de trouver solution
- – Formalisation $\Rightarrow$ limitation exigences et systèmes admissibles

Algorithmes génétiques : Exploration basée sur boucle génération (mutation & croisement) / sélection (critère).

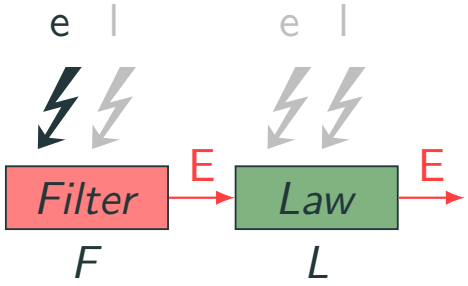
- \+ Formalisation $\not\Rightarrow$ limitations exigences et systèmes (HIPHOPS [APS+11])
- – Aucune garantie de trouver solution
- – Phase de sélection chronophage

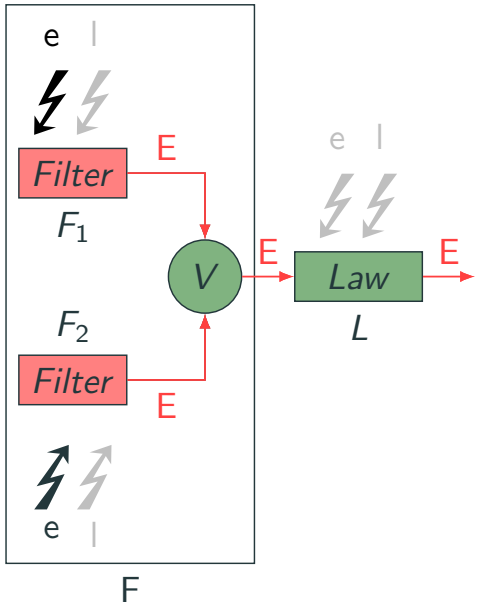
Analyse basée événements vs modes de défaillance





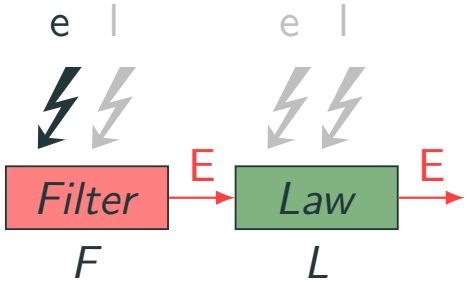
Analyse basée événements vs modes de défaillance

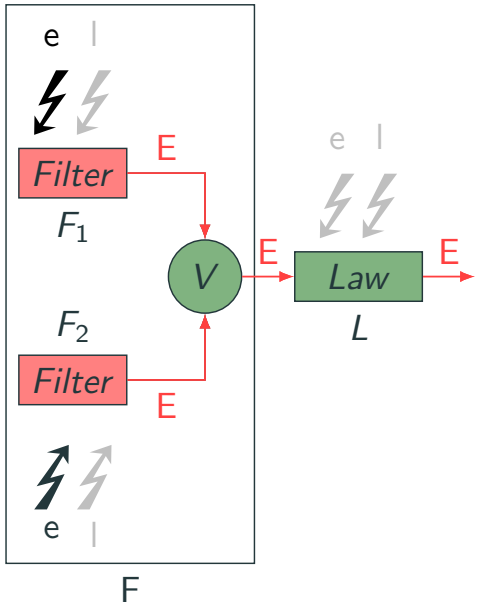




événements $\{F.e, \neg F.l, \neg L.e, \neg L.l\}$ $\neq$ $\{F1.e, \neg F1.l, F2.e, \neg F2.l, \neg L.e, \neg L.l\}$

Analyse basée événements vs modes de défaillance





événements $\{F.e, \neg F.l, \neg L.e, \neg L.l\} \neq \{F1.e, \neg F1.l, F2.e, \neg F2.l, \neg L.e, \neg L.l\}$

modes $\{(F, \{out \mapsto E\}), (L, \{in \mapsto E, out \mapsto E\})\} \supseteq \{(F, \{out \mapsto E\}), (L, \{in \mapsto E, out \mapsto E\})\}$

Stabilité des analyses vis-à-vis d'une substitution

Basée événements :

+ utilisable pour calculer directement indicateur,
− analyse à plat ⇒ recalcul obligatoire pour chaque candidat
  ⇒ chronophage

Basée modes :

+ analyse modulaire ⇒ réutilisable pour analyser candidats,
− pas de méthode directe de calcul des indicateurs.

Stabilité des analyses vis-à-vis d'une substitution

Basée événements :

+ utilisable pour calculer directement indicateur,
− analyse à plat ⇒ recalcul obligatoire pour chaque candidat
⇒ chronophage

Basée modes :

+ analyse modulaire ⇒ réutilisable pour analyser candidats,
− ~~pas de méthode directe de calcul des indicateurs.~~

⇓ Contribution

+ définir méthodes de calcul à partir des modes observés aux interfaces des composants

Plan

1. Contexte

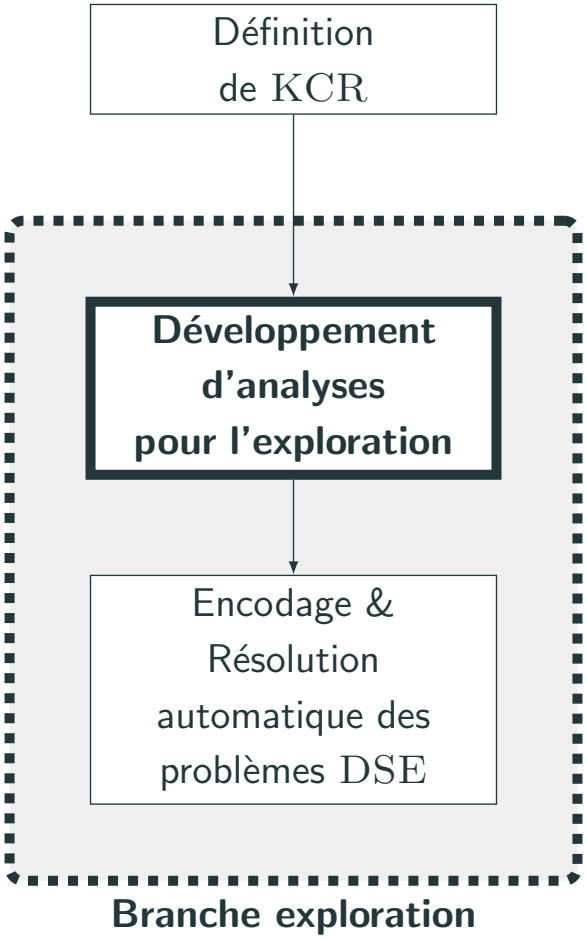
2. Contributions

   Définition de KCR

   Résolution du problème DSE

3. Expérimentations

4. Conclusion



Méthode d'analyse d'un composant

$F : \{out \mapsto E\}$

$F : \{out \mapsto L\}$

$F : \{out \mapsto empty\}$

Génération

Méthode d'analyse d'un composant

$F : \{out \mapsto E\}$

trig	e	$F_1.e \wedge F_2.e$

$F : \{out \mapsto L\}$

trig	l	$F_1.l \vee F_2.l \vee F_1.e \veebar F_2.e$

$F : \{out \mapsto empty\}$

trig	$\neg e \wedge \neg l$	$\neg F_1.e \wedge \neg F_2.e \wedge \neg F_1.l \wedge \neg F_2.l$

Analyse

Méthode d'analyse d'un composant

$F : \{out \mapsto E\}$

trig	e	$F_1.e \wedge F_2.e$
order	1	2

$F : \{out \mapsto L\}$

trig	l	$F_1.l \vee F_2.l \vee F_1.e \veebar F_2.e$
order	1	1

$F : \{out \mapsto empty\}$

trig	$\neg e \wedge \neg l$	$\neg F_1.e \wedge \neg F_2.e \wedge \neg F_1.l \wedge \neg F_2.l$
order	0	0

Calcul ordre

Méthode d'analyse d'un composant

$F : \{out \mapsto E\}$

trig	e	$F_1.e \wedge F_2.e$
order	1	2
prob	10^{-2}	10^{-6}

$F : \{out \mapsto L\}$

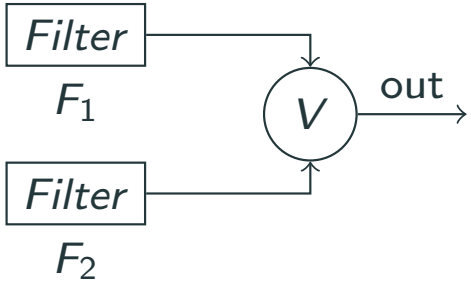
trig	l	$F_1.l \vee F_2.l \vee F_1.e \veebar F_2.e$
order	1	1
prob	10^{-2}	$3,999.10^{-3}$

$F : \{out \mapsto empty\}$

trig	$\neg e \wedge \neg l$	$\neg F_1.e \wedge \neg F_2.e \wedge \neg F_1.l \wedge \neg F_2.l$
order	0	0
prob	$0,98$	$0,996$

Calcul probabilité

Méthode d'analyse d'un composant



$F : \{out \mapsto E\}$

order	1	2
prob	10^{-2}	10^{-6}

$F : \{out \mapsto L\}$

order	1	1
prob	10^{-2}	$3,999.10^{-3}$

$F : \{out \mapsto empty\}$

order	0	0
prob	$0,98$	$0,996$

Oubli des événements

Méthode d'analyse du système

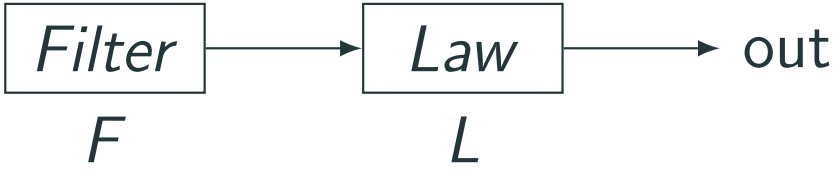
Objectif Calculer & encoder scénarios de modes (au niveau système) déclenchant l'événement redouté.

Scénario système vecteur de modes observés aux interfaces des composants

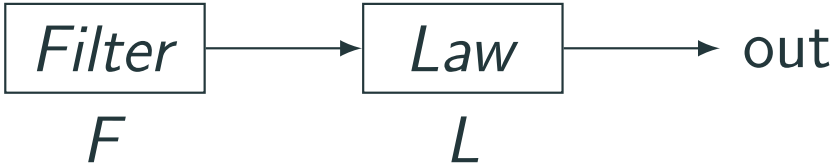
Idée utiliser les analyses des composants pour encoder les scénarios par Diagramme de Décisions Mutli-valués (STMDD)

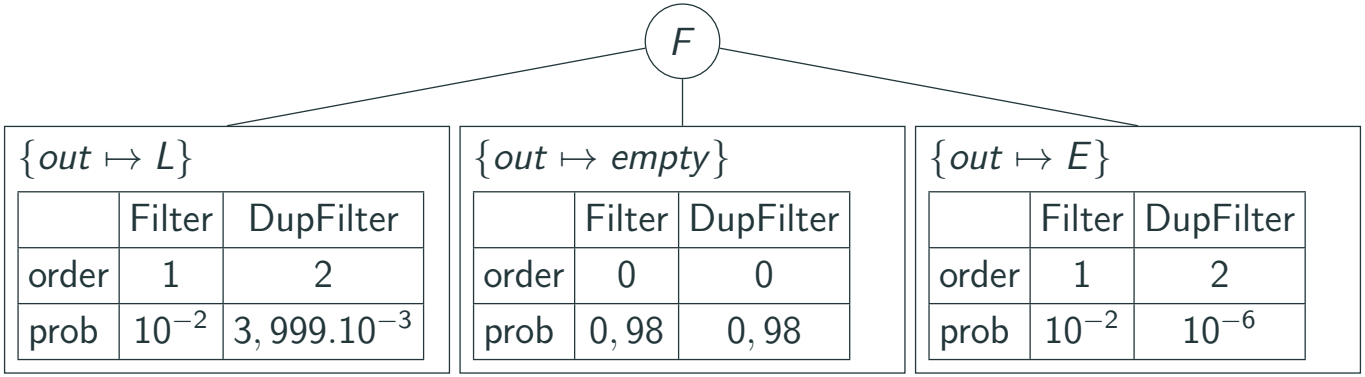
- nœuds $\Rightarrow$ composants
- arcs $\Rightarrow$ modes observés sur composant
- terminal 1 : chemin encode scénario déclenchant l'événement redouté

Fil rouge : construction du STMDD



Fil rouge : construction du STMDD





$\{out \mapsto L\}$

	Filter	DupFilter
order	1	2
prob	10^{-2}	$3,999.10^{-3}$

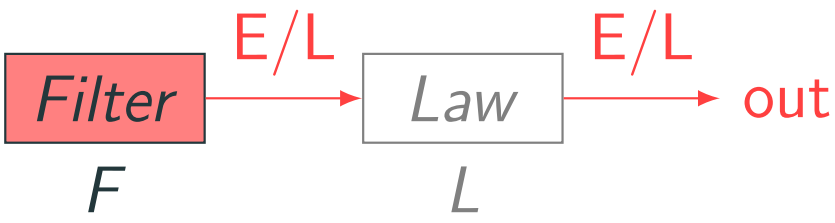
$\{out \mapsto empty\}$

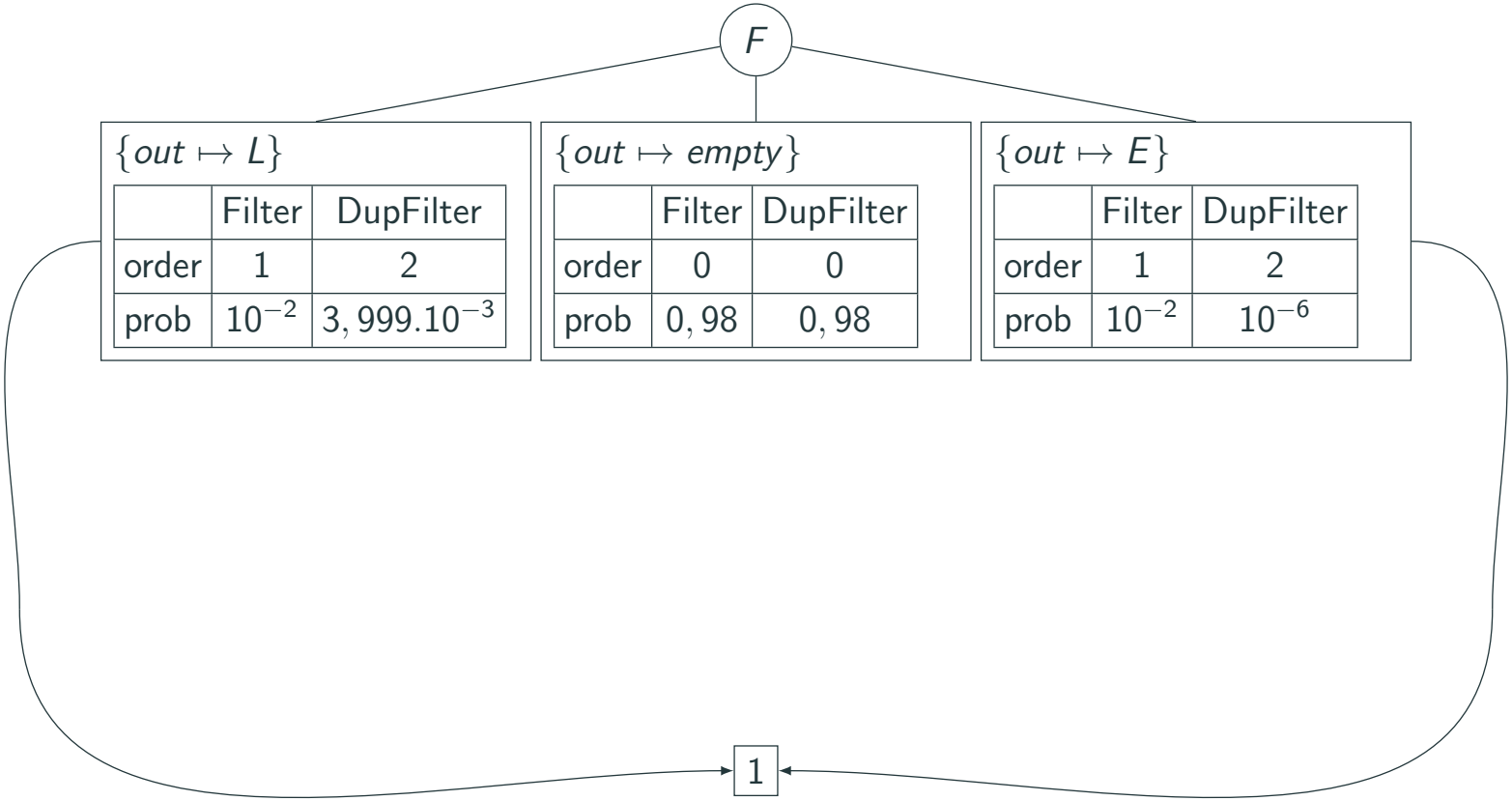
	Filter	DupFilter
order	0	0
prob	$0,98$	$0,98$

$\{out \mapsto E\}$

	Filter	DupFilter
order	1	2
prob	10^{-2}	10^{-6}

Fil rouge : construction du STMDD



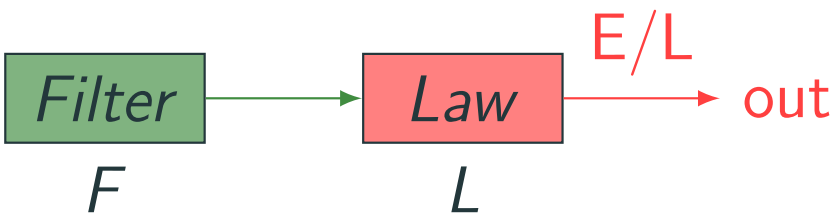


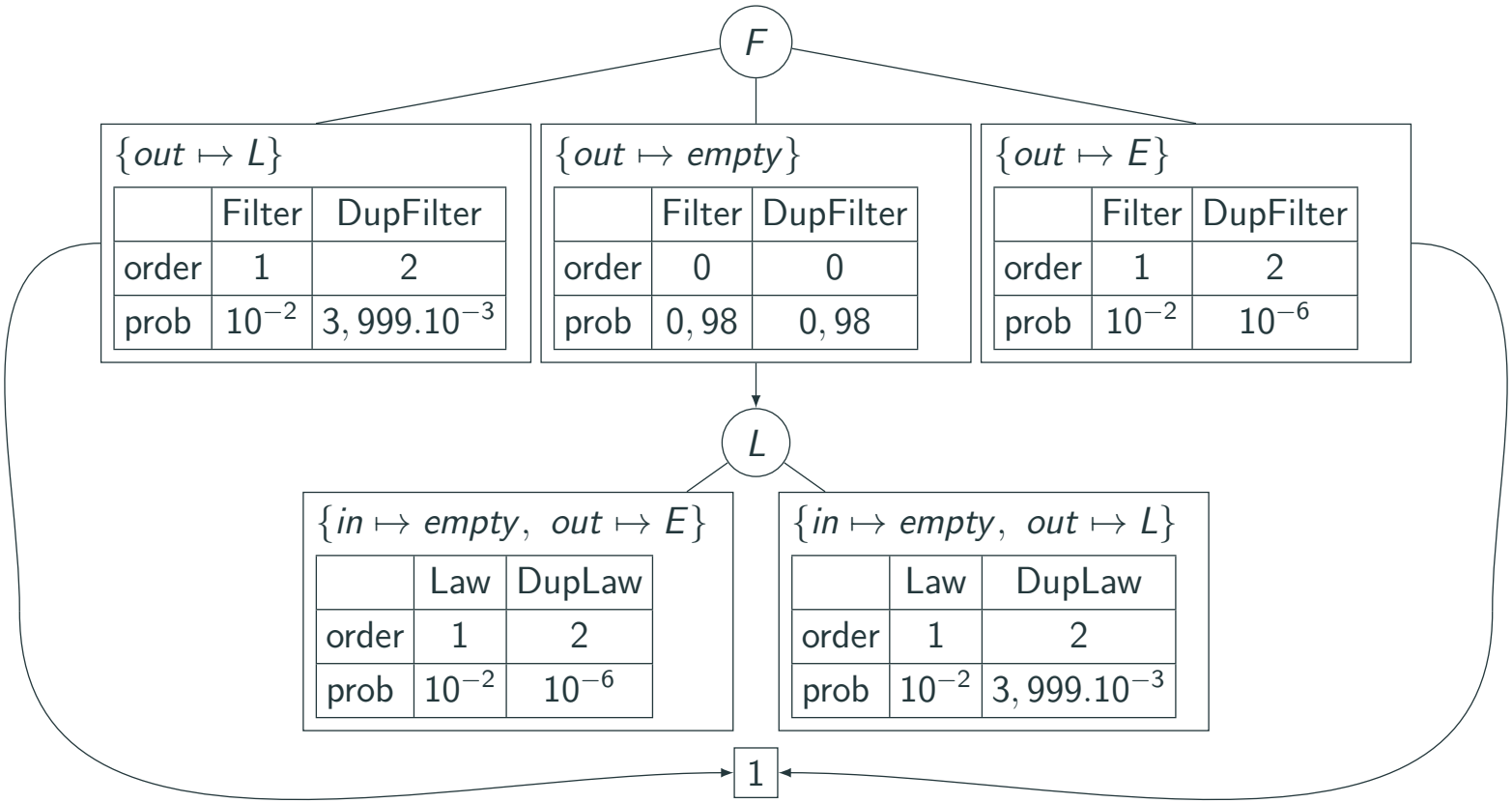
	Filter	DupFilter
order	1	2
prob	10^{-2}	$3,999.10^{-3}$

	Filter	DupFilter
order	0	0
prob	$0,98$	$0,98$

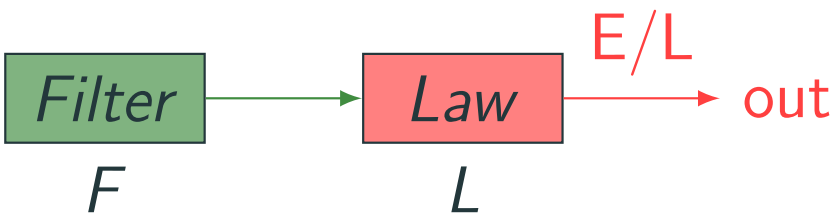
	Filter	DupFilter
order	1	2
prob	10^{-2}	10^{-6}

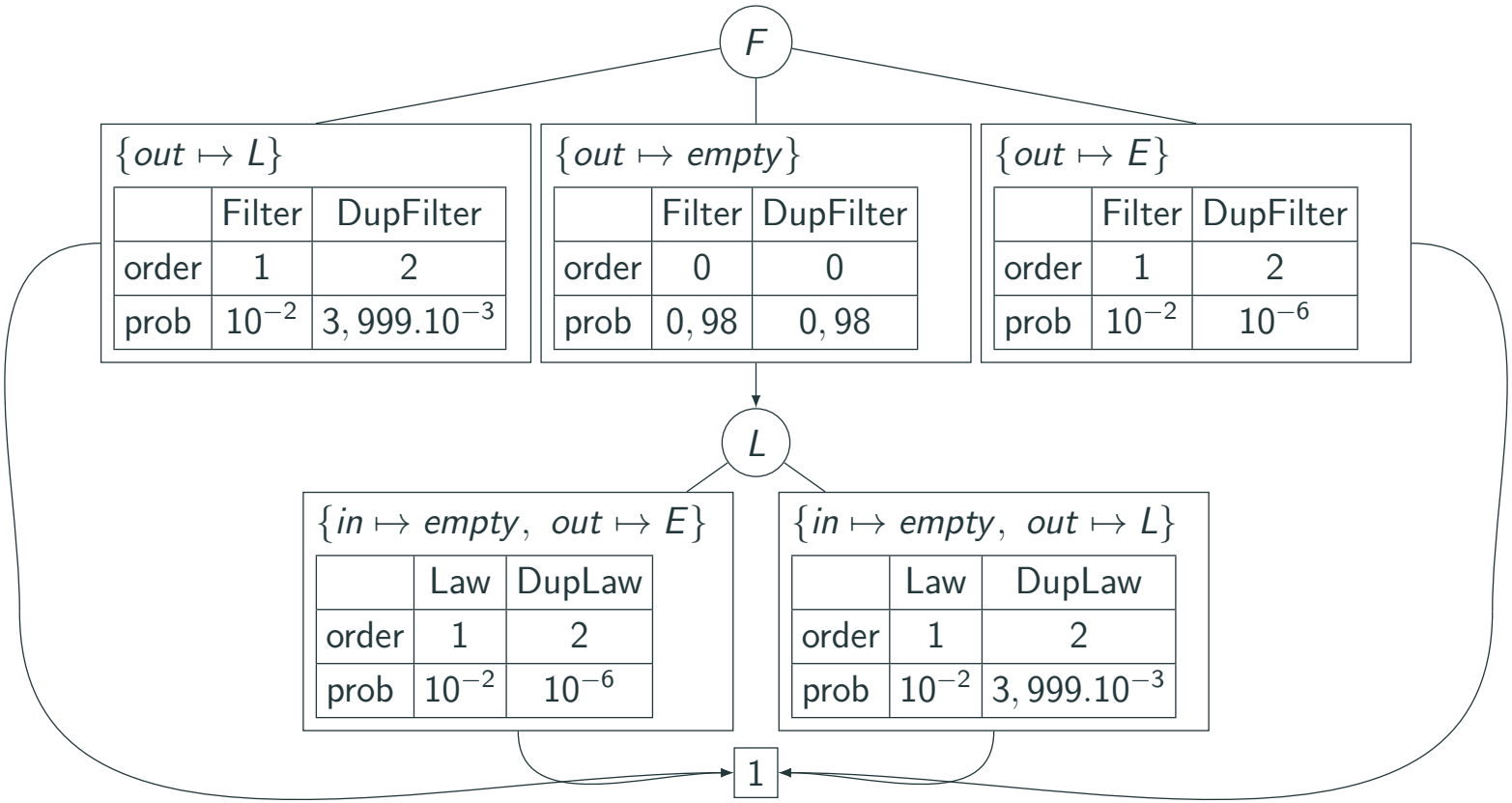
Fil rouge : construction du STMDD





Fil rouge : construction du STMDD





	Filter	DupFilter
order	1	2
prob	10^{-2}	$3,999.10^{-3}$

	Filter	DupFilter
order	0	0
prob	$0,98$	$0,98$

	Filter	DupFilter
order	1	2
prob	10^{-2}	10^{-6}

	Law	DupLaw
order	1	2
prob	10^{-2}	10^{-6}

	Law	DupLaw
order	1	2
prob	10^{-2}	$3,999.10^{-3}$

Impact d'une substitution sur le STMDD

Hypothèse (Inclusion)

C remplaçable par C' $\Rightarrow$ modes observables sur C' sont observables sur C

	Modes			
Composants	$\{out \mapsto E\}$	$\{out \mapsto L\}$	$\{out \mapsto empty\}$	$\{out \mapsto E + L\}$
Filter	✓	✓	✓	✗
DupFilter	✓	✓	✓	✗

$\Rightarrow$ Filter remplaçable par DupFilter

Impact d'une substitution sur le STMDD

Hypothèse (Inclusion)

C remplaçable par C' $\Rightarrow$ modes observables sur C' sont observables sur C

	Modes			
Composants	$\{out \mapsto E\}$	$\{out \mapsto L\}$	$\{out \mapsto empty\}$	$\{out \mapsto E + L\}$
Filter	✓	✓	✓	✗
DupFilter	✓	✓	✓	✗

$\Rightarrow$ Filter remplaçable par DupFilter

Permet de définir deux analyses :

1. choix de substitution complet $\rightarrow$ valeur des indicateurs,
2. choix de substitution partiel $\rightarrow$ encadrement sur des indicateurs.

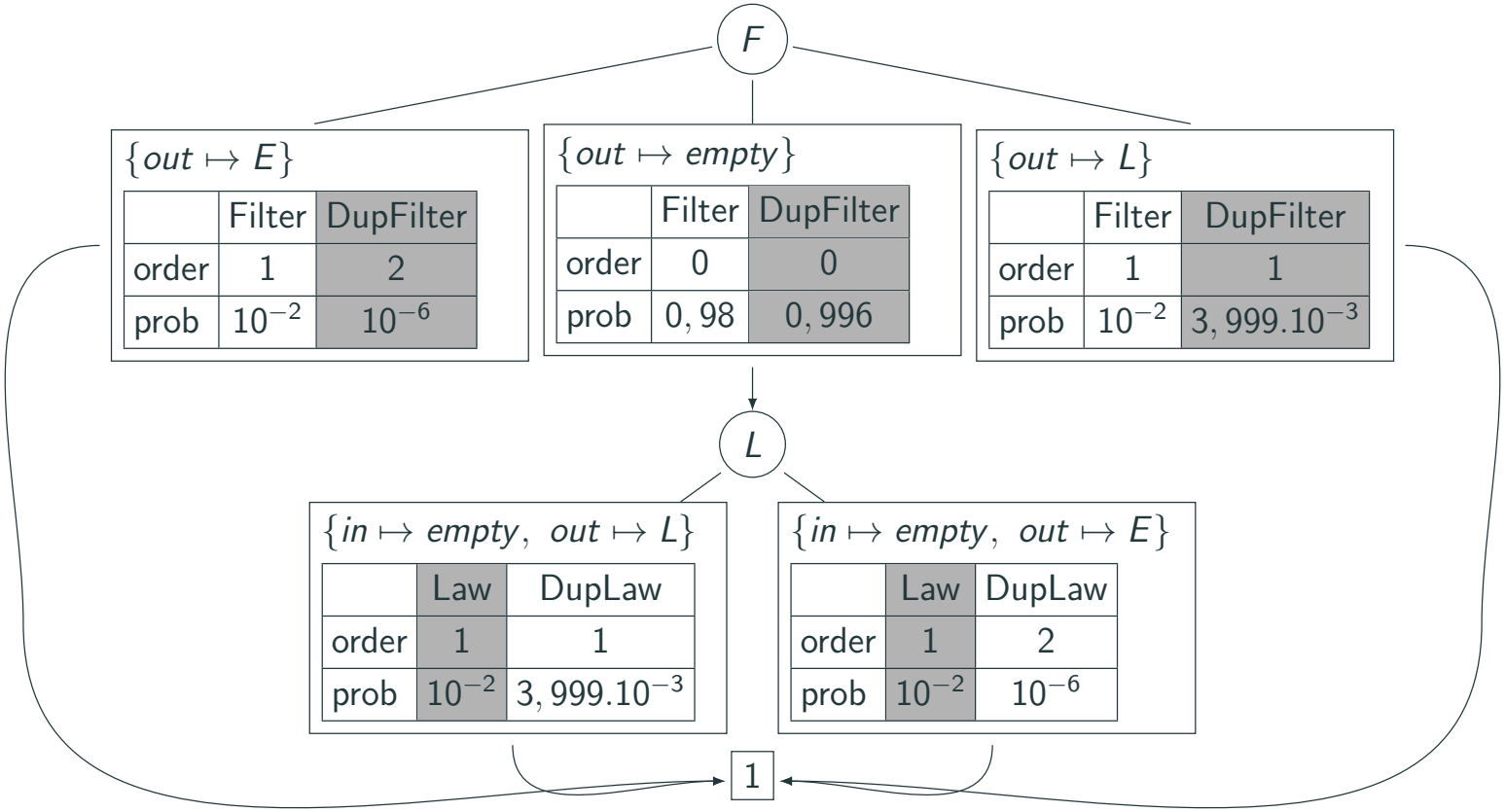
ONERA
THE FRENCH AEROSPACE LAB

Calcul des indicateurs avec le STMDD

Si $F \mapsto DupFilter$ et $L \mapsto Law$ alors

$$ordre = min(\qquad\qquad\qquad\qquad)$$

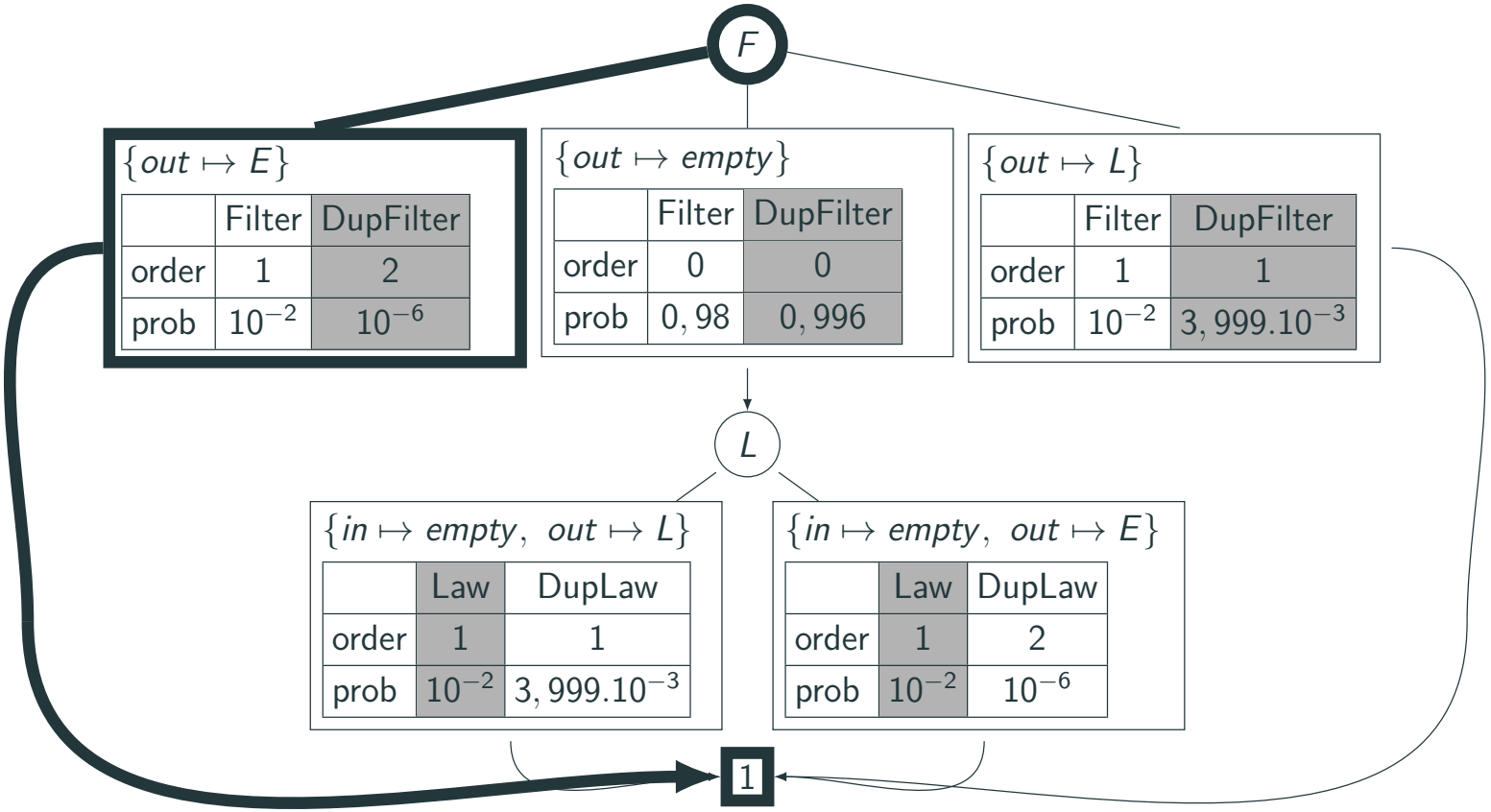
$$R = 1 - (\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad)$$



Calcul des indicateurs avec le STMDD

Si $F \mapsto DupFilter$ et $L \mapsto Law$ alors

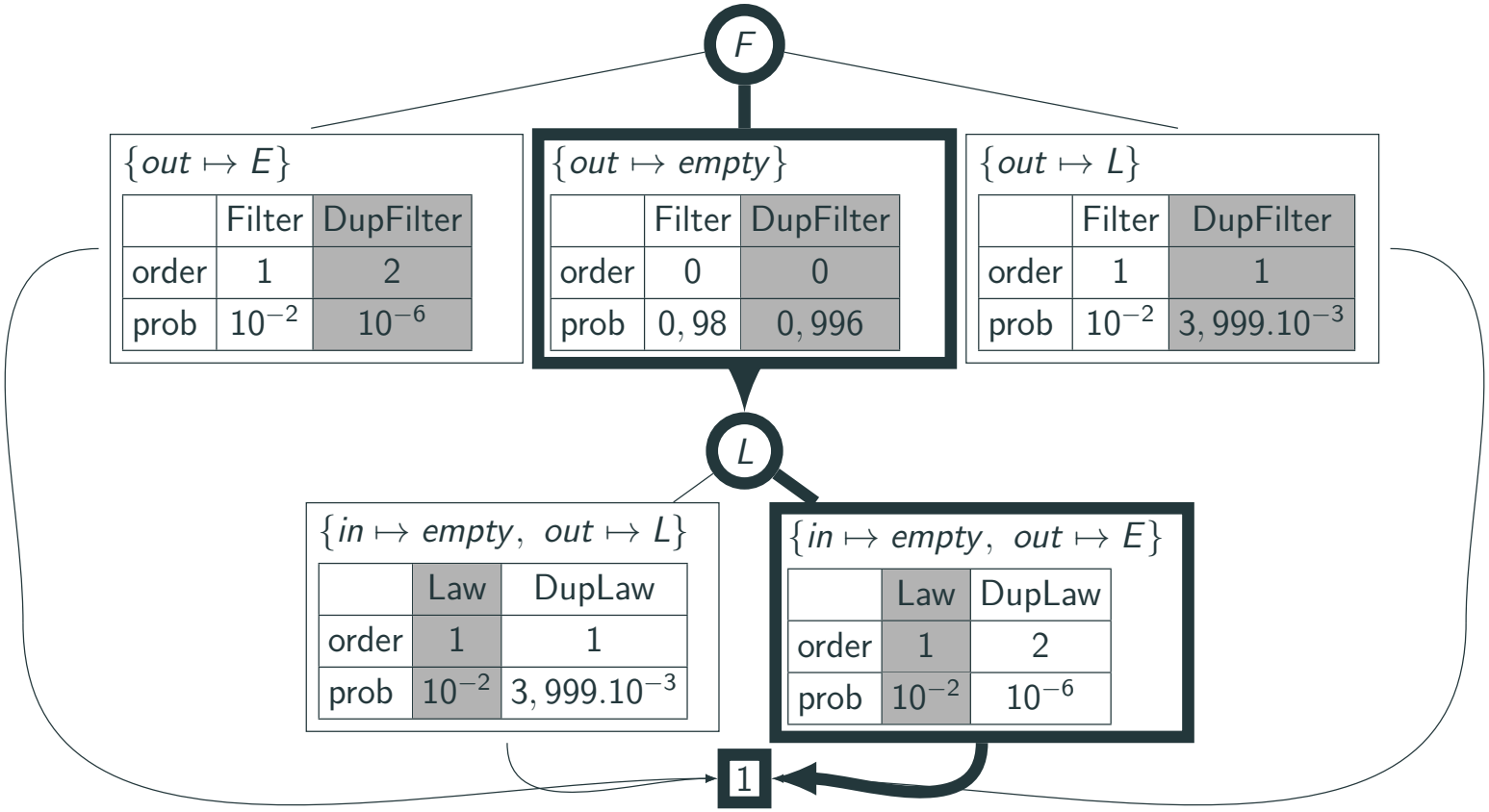
$$\begin{aligned} ordre &= min(2; \qquad\qquad\qquad\qquad) \\ R &= 1 - (10^{-6} + \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad) \end{aligned}$$



Calcul des indicateurs avec le STMDD

Si $F \mapsto DupFilter$ et $L \mapsto Law$ alors

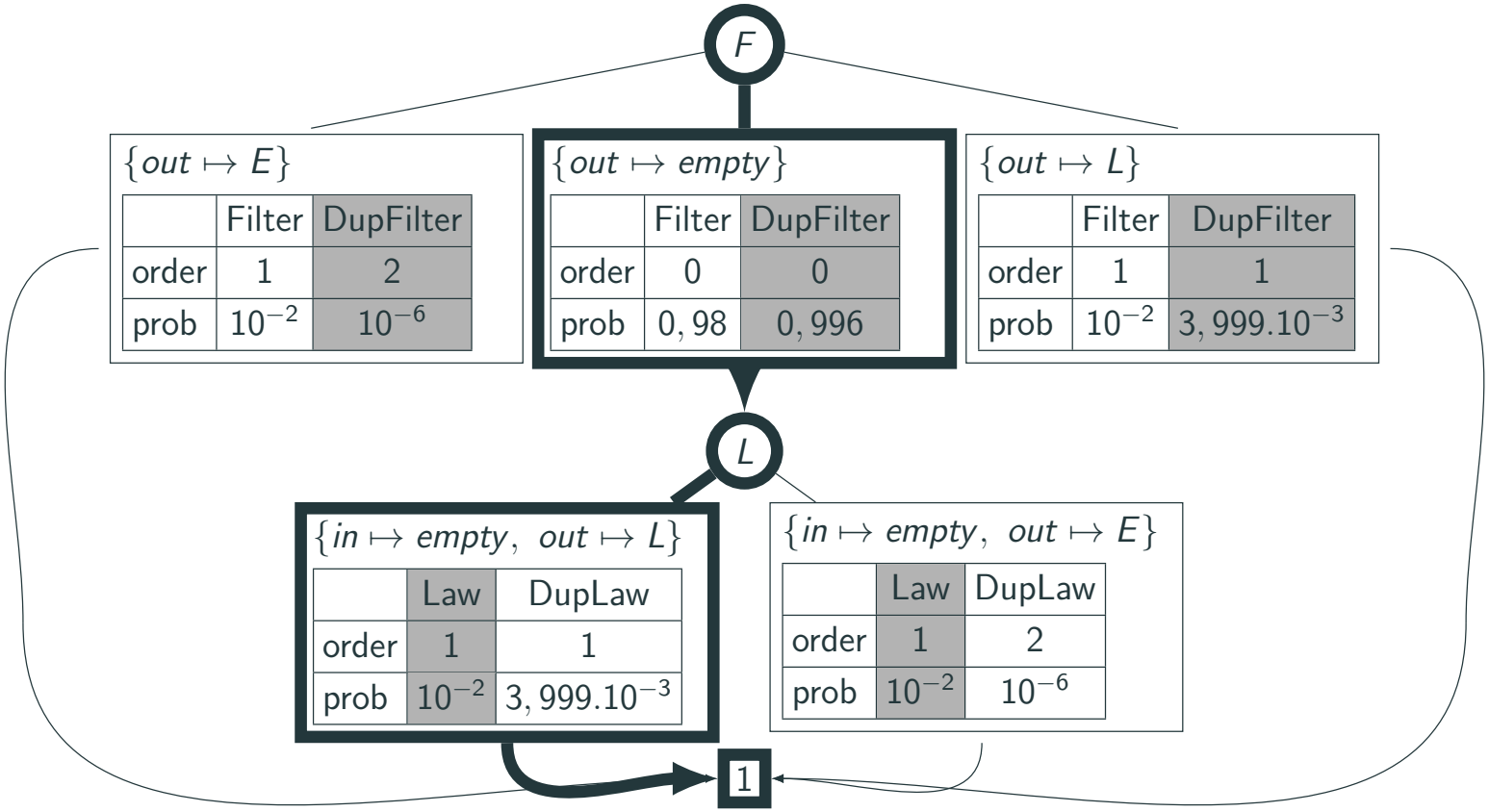
$$\begin{aligned} ordre &= min(2; 0+1; \qquad\qquad) \\ R &= 1-(10^{-6}+0,996(10^{-2} \qquad\qquad)+ \qquad\qquad) \end{aligned}$$



Calcul des indicateurs avec le STMDD

Si $F \mapsto DupFilter$ et $L \mapsto Law$ alors

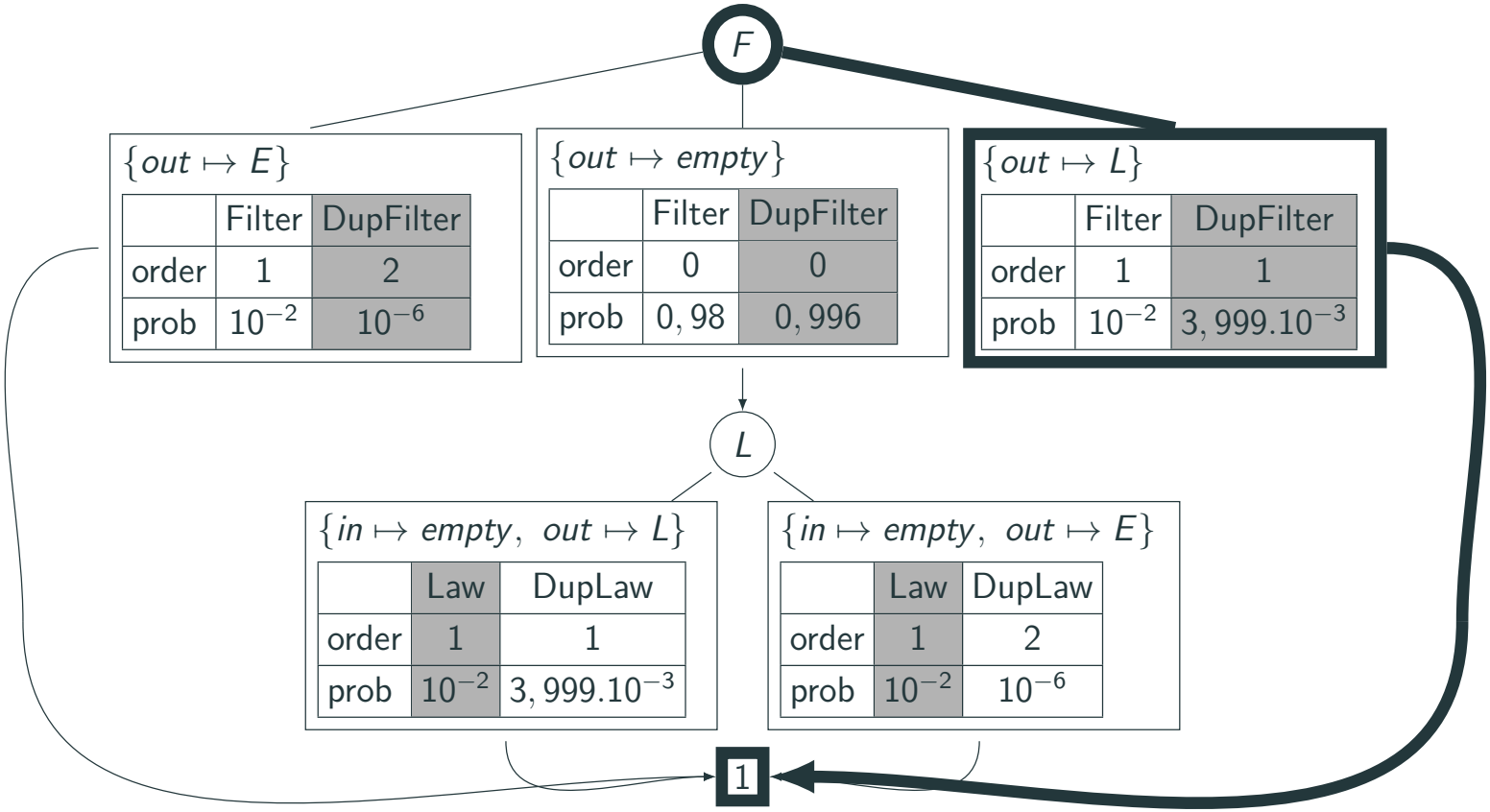
$$\begin{aligned} ordre &= min(2; 0+1; 0+1; \quad) \\ R &= 1 - (10^{-6} + 0,996(10^{-2} + 10^{-2}) + \qquad\qquad) \end{aligned}$$



Calcul des indicateurs avec le STMDD

Si $F \mapsto DupFilter$ et $L \mapsto Law$ alors

$$\begin{aligned} ordre &= min(2; 0+1; 0+1; 1) = 1 \\ R &= 1 - (10^{-6} + 0,996(10^{-2} + 10^{-2}) + 3,999.10^{-3}) \simeq 0,986 \end{aligned}$$

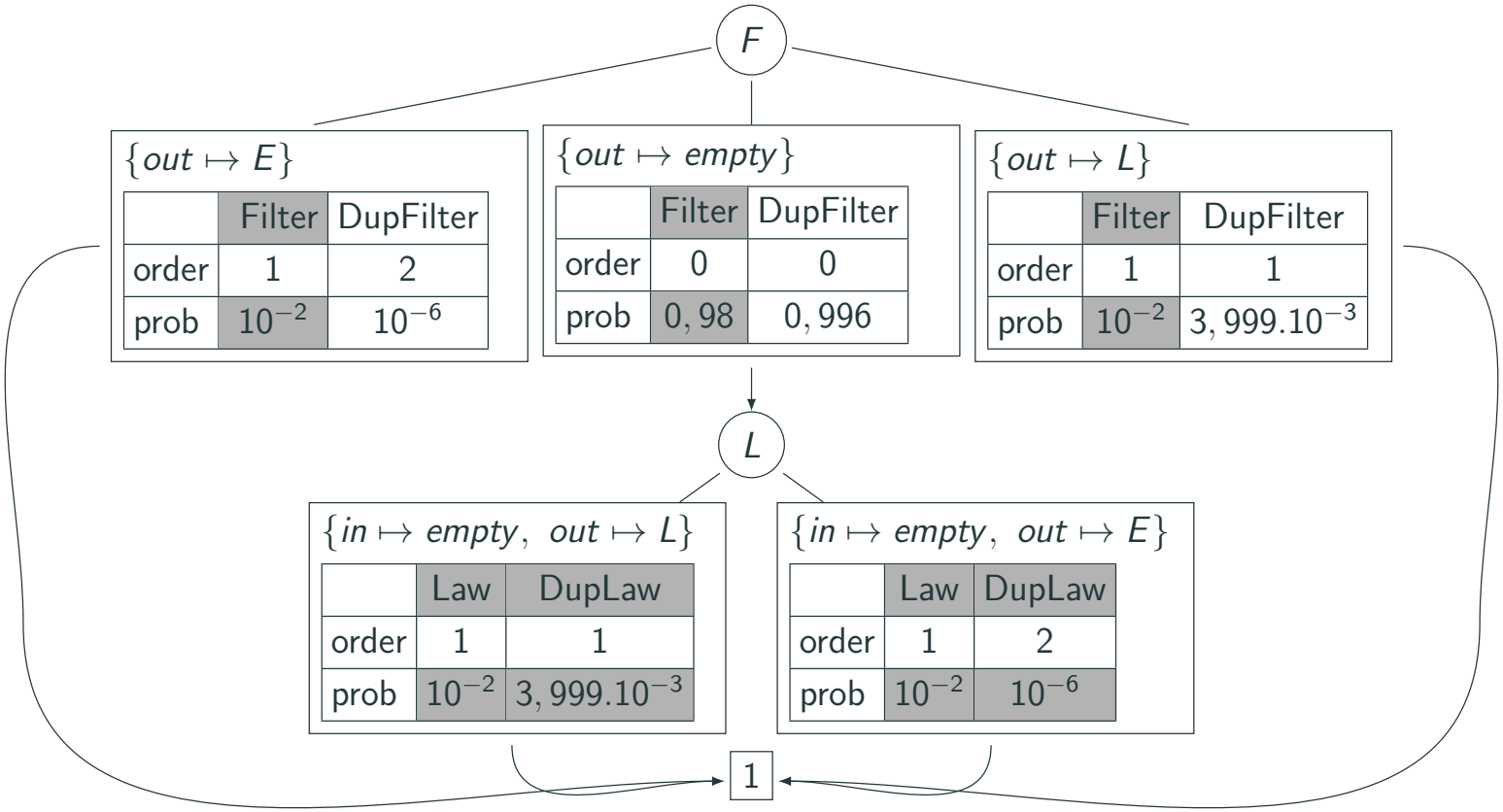


Approximation des indicateurs

Si $F \mapsto \mathit{Filter}$ alors

$R^+ = 1 - ($ $)$

$R^- = 1 - ($ $)$



Approximation des indicateurs

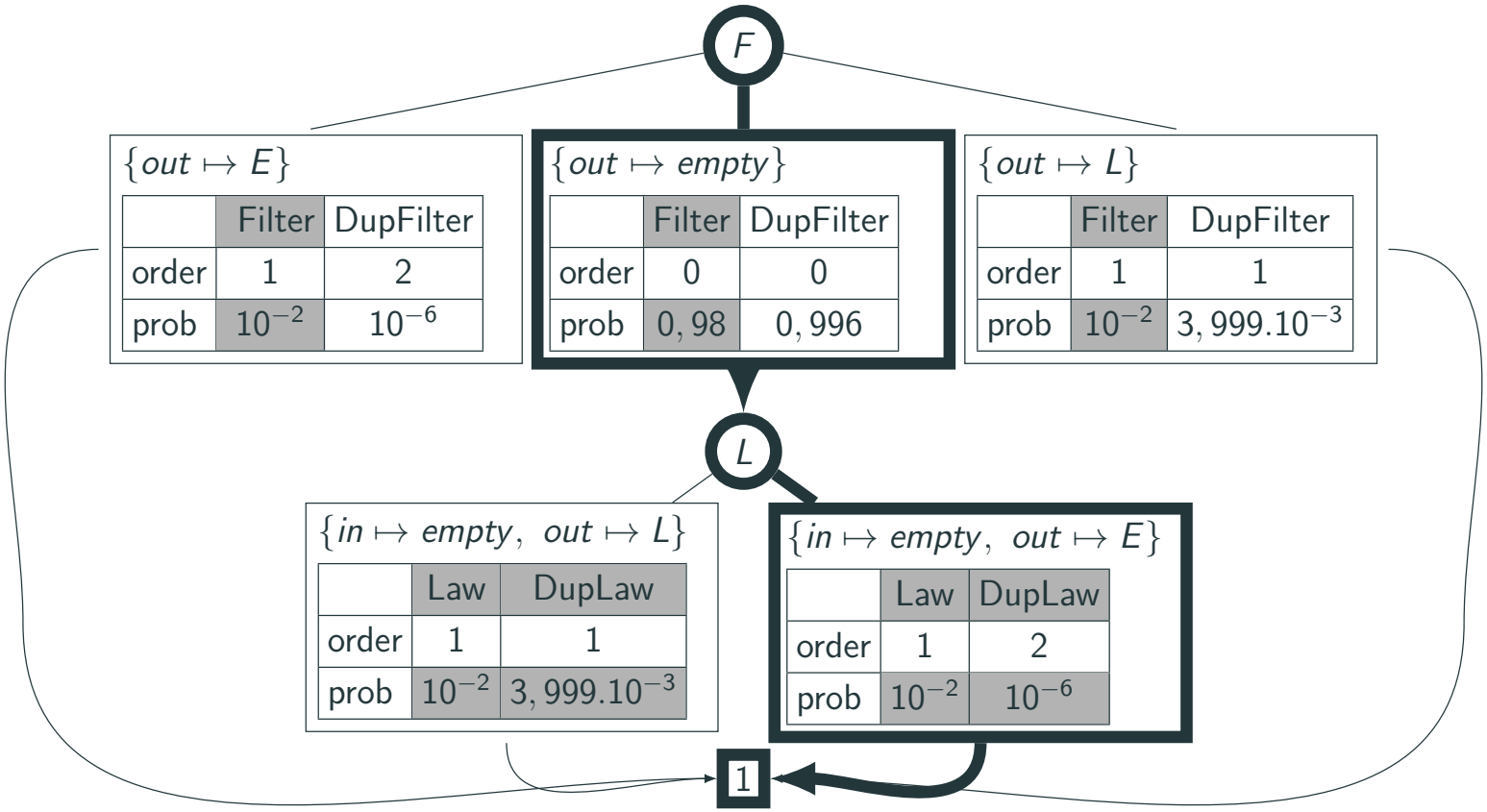
Si $F \mapsto \mathit{Filter}$ alors

$R^+ = 1 - (10^{-2} + \qquad\qquad\qquad\

Approximation des indicateurs

Si $F \mapsto Filter$ alors

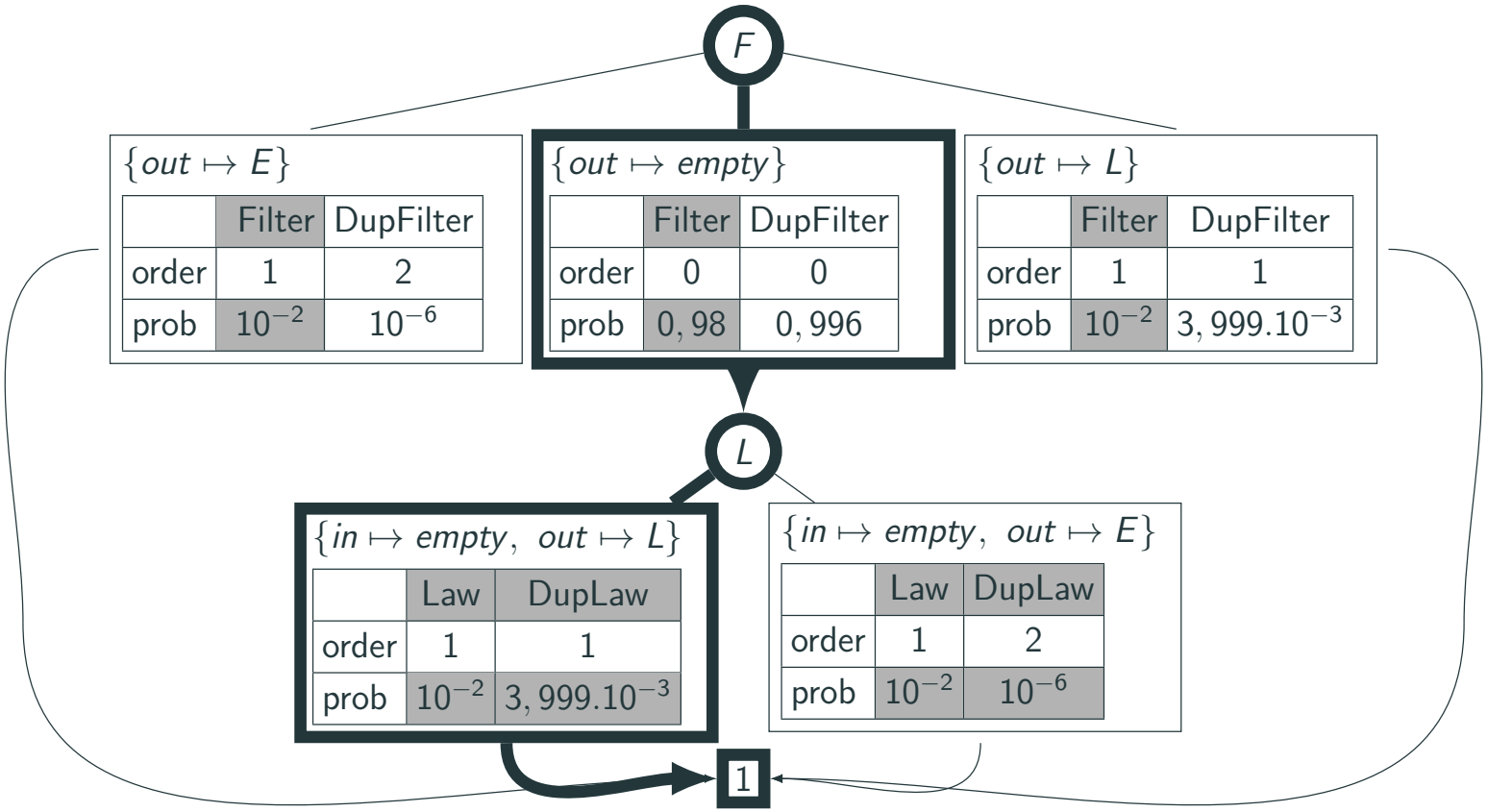
$$R^+ = 1 - (10^{-2} + 0,98(min(10^{-2}; 10^{-6}) + \qquad)$$
$$R^- = 1 - (10^{-2} + 0,98(max(10^{-2}; 10^{-6}) + \qquad)$$



Approximation des indicateurs

Si $F \mapsto Filter$ alors

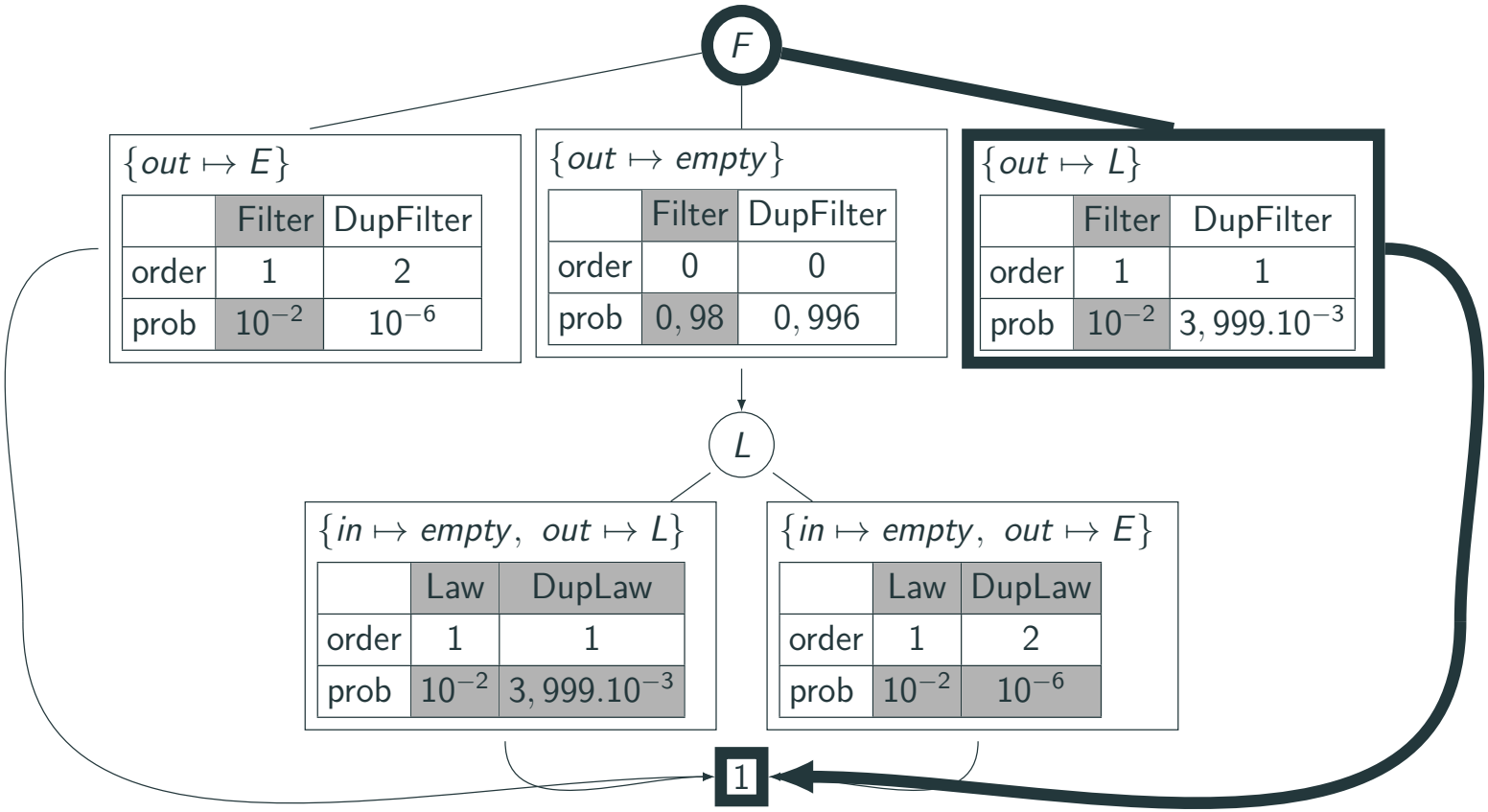
$$R^{+} = 1 - (10^{-2} + 0,98(min(10^{-2}; 10^{-6}) + min(10^{-2}; 3,999.10^{-3})) + \qquad)$$
$$R^{-} = 1 - (10^{-2} + 0,98(max(10^{-2}; 10^{-6}) + max(10^{-2}; 3,999.10^{-3})) + \qquad)$$



Approximation des indicateurs

Si $F \mapsto Filter$ alors

$$R^+ = 1 - (10^{-2} + 0,98(min(10^{-2}; 10^{-6}) + min(10^{-2}; 3,999.10^{-3})) + 10^{-2}) = 0,976$$
$$R^- = 1 - (10^{-2} + 0,98(max(10^{-2}; 10^{-6}) + max(10^{-2}; 3,999.10^{-3})) + 10^{-2}) = 0,96$$



Plan

1. Contexte

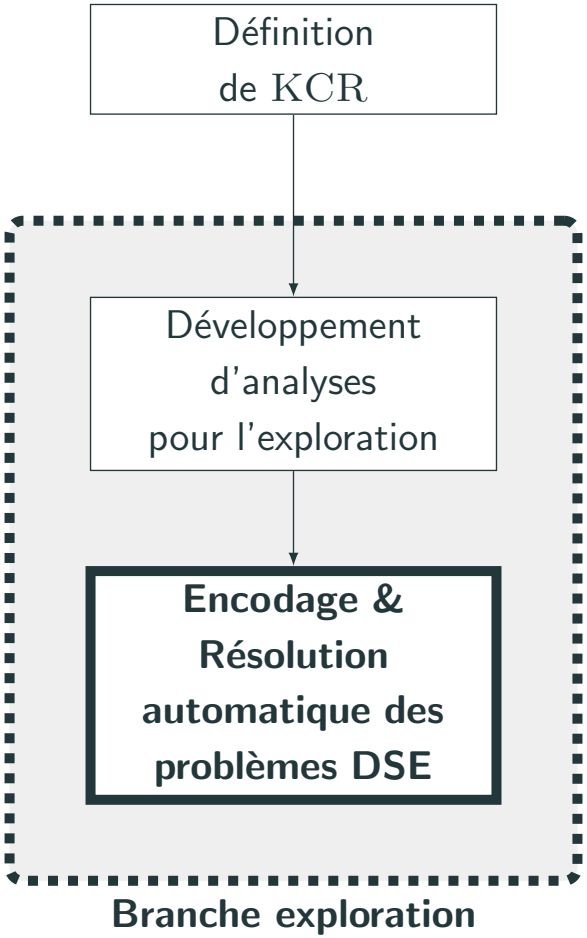
2. Contributions

   Définition de KCR

   Résolution du problème DSE

3. Expérimentations

4. Conclusion



Intégration paresseuse de la théorie Safety

Objectif : trouver un modèle de ϕ où les atomes : variables booléennes ou prédicats de théorie

Intégration paresseuse de la théorie Safety

Objectif : trouver un modèle de ϕ où les atomes : variables booléennes ou prédicats de théorie

Formuler un problème DSE

- considérer des contraintes sur des indicateurs de sûreté,
- définir prédicat pour exprimer contraintes au sein de la théorie métier **Safety**

Intégration paresseuse de la théorie Safety

Objectif : trouver un modèle de ϕ où les atomes : variables booléennes ou prédicats de théorie

Formuler un problème DSE

- considérer des contraintes sur des indicateurs de sûreté,
- définir prédicat pour exprimer contraintes au sein de la théorie métier **Safety**

Prédicats de Safety :

- `(choose comp alt)` : alt est choisie pour comp ;
- `(isSafeOrder stmdd req)` : ordre $\geq$ req ;
- `(isSafeR stmdd req)` : fiabilité $\geq$ req.

Intégration paresseuse de la théorie Safety

Avec *stmdd* calculé, le problème d'exploration devient :

$$\overbrace{(\texttt{isSafeR}\ \mathit{stmdd}\ 0,99)}^{p_1} \wedge \overbrace{(\texttt{isSafeOrder}\ \mathit{stmdd}\ 1)}^{p_2} \wedge (\overbrace{(\texttt{choose}\ F\ \mathit{Filter})}^{p_3} \vee\!\!\vee \underbrace{(\texttt{choose}\ F\ \mathit{DupFilter})}_{p_4}) \wedge (\underbrace{(\texttt{choose}\ L\ \mathit{Law})}_{p_5} \vee\!\!\vee \underbrace{(\texttt{choose}\ L\ \mathit{DupLaw})}_{p_6})$$

$\Downarrow$ Abstraction

Intégration paresseuse de la théorie Safety

Avec *stmdd* calculé, le problème d'exploration devient :

$$\overbrace{(\texttt{isSafeR}\ \mathit{stmdd}\ 0,99)}^{p_1} \wedge \overbrace{(\texttt{isSafeOrder}\ \mathit{stmdd}\ 1)}^{p_2} \wedge (\overbrace{(\texttt{choose}\ F\ \mathit{Filter})}^{p_3} \mathbin{\mathbb{W}} \underbrace{(\texttt{choose}\ F\ \mathit{DupFilter})}_{p_4}) \wedge (\underbrace{(\texttt{choose}\ L\ \mathit{Law})}_{p_5} \mathbin{\mathbb{W}} \underbrace{(\texttt{choose}\ L\ \mathit{DupLaw})}_{p_6})$$

$\Downarrow$ Abstraction

$$p_1 \wedge p_2 \wedge (p_3 \mathbin{\mathbb{W}} p_4) \wedge (p_5 \mathbin{\mathbb{W}} p_6)$$

$\Downarrow$ Résolution SAT

Intégration paresseuse de la théorie Safety

Avec *stmdd* calculé, le problème d'exploration devient :

$$\overbrace{(\texttt{isSafeR}\ \mathit{stmdd}\ 0,99)}^{p_1} \wedge \overbrace{(\texttt{isSafeOrder}\ \mathit{stmdd}\ 1)}^{p_2} \wedge (\overbrace{(\texttt{choose}\ F\ \mathit{Filter})}^{p_3} \mathbin{\mathbb{W}} \underbrace{(\texttt{choose}\ F\ \mathit{DupFilter})}_{p_4}) \wedge (\underbrace{(\texttt{choose}\ L\ \mathit{Law})}_{p_5} \mathbin{\mathbb{W}} \underbrace{(\texttt{choose}\ L\ \mathit{DupLaw})}_{p_6})$$

$$\Downarrow \text{Abstraction}$$

$$p_1 \wedge p_2 \wedge (p_3 \mathbin{\mathbb{W}} p_4) \wedge (p_5 \mathbin{\mathbb{W}} p_6)$$

$$\Downarrow \text{Résolution } \textsc{Sat}$$

$$\{p_1 \mapsto \mathbf{T}, p_2 \mapsto \mathbf{T}, p_3 \mapsto \mathbf{T}, p_4 \mapsto \mathbf{F}, p_5 \mapsto \mathbf{T}, p_6 \mapsto \mathbf{F}\}$$

$$\Downarrow$$

Intégration paresseuse de la théorie Safety

Avec *stmdd* calculé, le problème d'exploration devient :

$$\overbrace{(\texttt{isSafeR}\ \mathit{stmdd}\ 0,99)}^{p_1} \wedge \overbrace{(\texttt{isSafeOrder}\ \mathit{stmdd}\ 1)}^{p_2} \wedge (\overbrace{(\texttt{choose}\ F\ \mathit{Filter})}^{p_3} \mathbin{\mathbb{W}} \underbrace{(\texttt{choose}\ F\ \mathit{DupFilter})}_{p_4}) \wedge (\underbrace{(\texttt{choose}\ L\ \mathit{Law})}_{p_5} \mathbin{\mathbb{W}} \underbrace{(\texttt{choose}\ L\ \mathit{DupLaw})}_{p_6})$$

$$\Downarrow \text{Abstraction}$$

$$p_1 \wedge p_2 \wedge (p_3 \mathbin{\mathbb{W}} p_4) \wedge (p_5 \mathbin{\mathbb{W}} p_6)$$

$$\Downarrow \text{Résolution } \textsc{Sat}$$

$$\{p_1 \mapsto \mathbf{T}, p_2 \mapsto \mathbf{T}, p_3 \mapsto \mathbf{T}, p_4 \mapsto \mathbf{F}, p_5 \mapsto \mathbf{T}, p_6 \mapsto \mathbf{F}\}$$

$$\Downarrow$$

Est-ce que pour $F \mapsto \mathit{Filter}$ et $L \mapsto \mathit{Law}$

$R \geq 0,99$ et $\mathit{ordre} \geq 1$?

Intégration paresseuse de la théorie Safety

Résultat du calcul des indicateurs : **R=0,96** et **ordre=1** $\Rightarrow$ conflit

$\Downarrow$ Minimiser l'explication du conflit

Intégration paresseuse de la théorie Safety

Résultat du calcul des indicateurs : **R=0,96** et **ordre=1** $\Rightarrow$ conflit

$\Downarrow$ Minimiser l'explication du conflit

Vérifier itérativement si chaque choix de substitution est nécessaire pour expliquer le conflit :

$$\{F \mapsto Filter, L \mapsto Law\}$$

Intégration paresseuse de la théorie Safety

Résultat du calcul des indicateurs : **R=0,96** et **ordre=1** $\Rightarrow$ conflit

$\Downarrow$ Minimiser l'explication du conflit

Vérifier itérativement si chaque choix de substitution est nécessaire pour expliquer le conflit :

$$\{F \mapsto Filter, L \mapsto Law\}$$

Recalculer les indicateurs : $R \in [0,96; 0,976]$ et ordre=$[1; 1]$

$\Rightarrow$ $L \mapsto Law$ pas nécessaire pour expliquer le conflit

Intégration paresseuse de la théorie Safety

Résultat du calcul des indicateurs : **R=0,96** et **ordre=1** $\Rightarrow$ conflit

$\Downarrow$ Minimiser l'explication du conflit

Vérifier itérativement si chaque choix de substitution est nécessaire pour expliquer le conflit :

$$\{F \mapsto Filter\}$$

Intégration paresseuse de la théorie Safety

Résultat du calcul des indicateurs : **R=0,96** et **ordre=1** $\Rightarrow$ conflit

$\Downarrow$ Minimiser l'explication du conflit

Vérifier itérativement si chaque choix de substitution est nécessaire pour expliquer le conflit :

$$\{F \mapsto Filter\}$$

Recalculer les indicateurs : $R \in [0,96; 0,992]$ et ordre=$[1; 1]$

$\Rightarrow$ $F \mapsto Filter$ nécessaire pour expliquer le conflit

Intégration paresseuse de la théorie Safety

Résultat du calcul des indicateurs : **R=0,96** et **ordre=1** $\Rightarrow$ conflit

$\Downarrow$ Minimiser l'explication du conflit

Vérifier itérativement si chaque choix de substitution est nécessaire pour expliquer le conflit :

$$\{F \mapsto \mathit{Filter}\}$$

$$\underbrace{(\texttt{isSafeR}\ \mathit{stmdd}\ 0,99)}_{p_1} \Rightarrow \neg\underbrace{(\texttt{choose}\ F\ \mathit{Filter})}_{p_3}$$

clause renvoyée : $\neg p_1 \vee \neg p_3$

Intégration paresseuse de la théorie Safety

Nouveau problème :

$$p_1 \wedge p_2 \wedge (p_3 \mathbin{\mathbb{W}} p_4) \wedge (p_5 \mathbin{\mathbb{W}} p_6) \wedge \underbrace{(\neg p_1 \vee \neg p_3)}_{\textit{clause de conflit}}$$

$\Downarrow$ Résolution SAT

Intégration paresseuse de la théorie Safety

Nouveau problème :

$$p_1 \wedge p_2 \wedge (p_3 \mathbin{\mathbb{W}} p_4) \wedge (p_5 \mathbin{\mathbb{W}} p_6) \wedge \underbrace{(\neg p_1 \vee \neg p_3)}_{\textit{clause de conflit}}$$

$$\Downarrow \text{Résolution } \textsc{Sat}$$

$$\{p_1 \mapsto \mathbf{T}, p_2 \mapsto \mathbf{T}, p_3 \mapsto \mathbf{F}, p_4 \mapsto \mathbf{T}, p_5 \mapsto \mathbf{F}, p_6 \mapsto \mathbf{T}\}$$

Intégration paresseuse de la théorie Safety

Nouveau problème :

$$p_1 \wedge p_2 \wedge (p_3 \mathbin{\mathbb{W}} p_4) \wedge (p_5 \mathbin{\mathbb{W}} p_6) \wedge \underbrace{(\neg p_1 \vee \neg p_3)}_{\textit{clause de conflit}}$$

$$\Downarrow \text{Résolution } \textsc{Sat}$$

$$\{p_1 \mapsto \mathbf{T}, p_2 \mapsto \mathbf{T}, p_3 \mapsto \mathbf{F}, p_4 \mapsto \mathbf{T}, p_5 \mapsto \mathbf{F}, p_6 \mapsto \mathbf{T}\}$$

Est-ce que pour $F \mapsto \mathit{DupFilter}$ et $L \mapsto \mathit{DupLaw}$
$R \geq 0,99$ et $\mathit{ordre} \geq 1$?

Intégration paresseuse de la théorie Safety

Nouveau problème :

$$p_1 \wedge p_2 \wedge (p_3 \mathbin{\mathbb{W}} p_4) \wedge (p_5 \mathbin{\mathbb{W}} p_6) \wedge \underbrace{(\neg p_1 \vee \neg p_3)}_{clause\ \ de\ \ conflit}$$

$\Downarrow$ Résolution $\textsc{Sat}$

$$\{p_1 \mapsto \mathbf{T}, p_2 \mapsto \mathbf{T}, p_3 \mapsto \mathbf{F}, p_4 \mapsto \mathbf{T}, p_5 \mapsto \mathbf{F}, p_6 \mapsto \mathbf{T}\}$$

Est-ce que pour $F \mapsto DupFilter$ et $L \mapsto DupLaw$

$R \geq 0,99$ et $ordre \geq 1$?

Résultat du calcul des indicateurs : **R=0,992** et **ordre=1**

Intégration paresseuse de la théorie Safety

Nouveau problème :

$$p_1 \wedge p_2 \wedge (p_3 \mathbin{\mathbb{W}} p_4) \wedge (p_5 \mathbin{\mathbb{W}} p_6) \wedge \underbrace{(\neg p_1 \vee \neg p_3)}_{clause\ \ de\ \ conflit}$$

$\Downarrow$ Résolution $\textsc{Sat}$

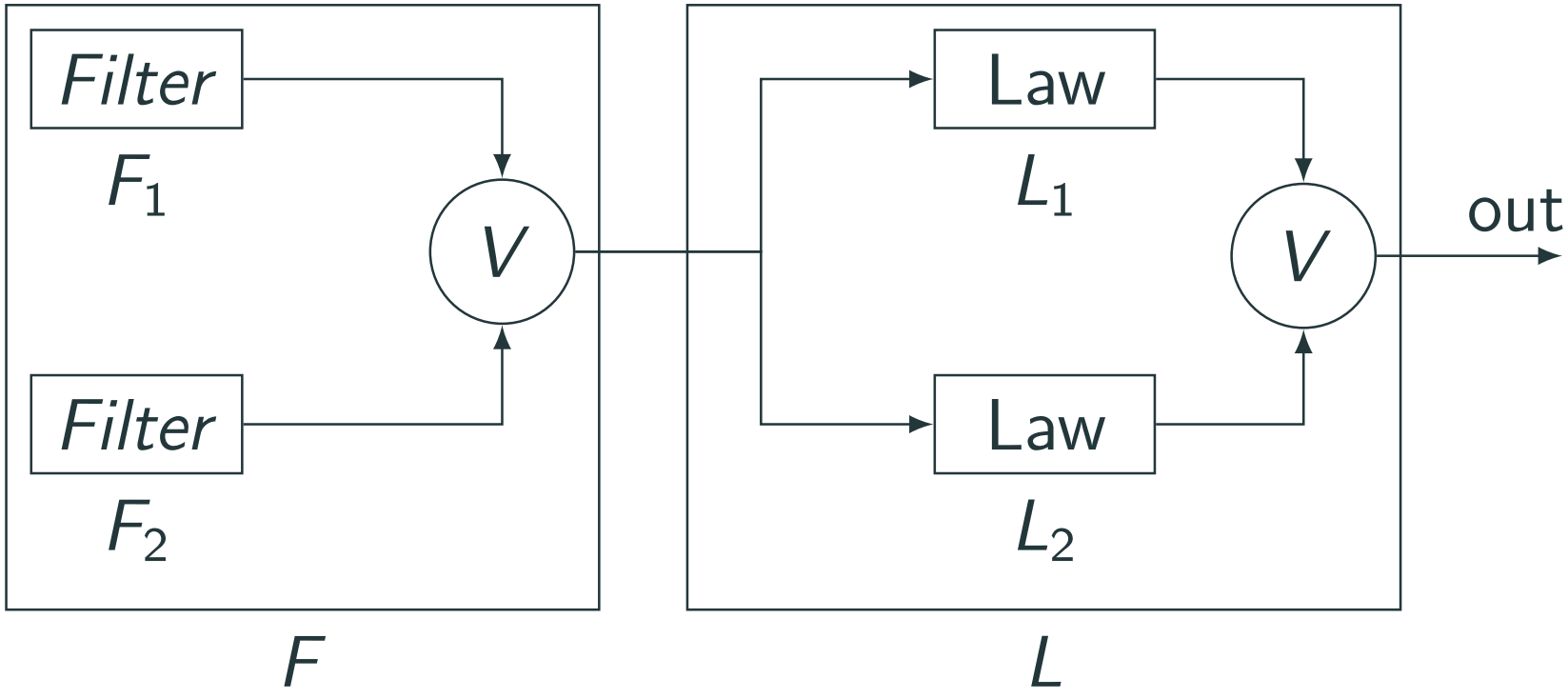
$$\{p_1 \mapsto \mathbf{T}, p_2 \mapsto \mathbf{T}, p_3 \mapsto \mathbf{F}, p_4 \mapsto \mathbf{T}, p_5 \mapsto \mathbf{F}, p_6 \mapsto \mathbf{T}\}$$

Est-ce que pour $F \mapsto DupFilter$ et $L \mapsto DupLaw$
$R \geq 0,99$ et $ordre \geq 1$?
Résultat du calcul des indicateurs : **R=0,992** et **ordre=1**

$\Downarrow$

$\textsc{Sat} : \{F \mapsto DupFilter, L \mapsto DupLaw\}$

Fil rouge : Résultat de la synthèse



Plan

1. Contexte

2. Contributions

   Définition de KCR

   Résolution du problème DSE

3. Expérimentations

4. Conclusion

Cas d'études

Nom	Description	Nb composants
ROSACE	contrôleur longitudinal avion	7
FUEL	système alimentation carburant	11
HBS	système freinage	10
QUADCOPTER	contrôleur de drones	7

Figure 1: Cas d'études

Performance de l'énumération des coupes

			Outil			
Systèmes	k	$\|MCS\|$	HipHOPS	XSAP	XFTA	KCR Analyser
Rosace	1	4	0,383	timeout	0,045	**0,035**
	2	18	0,426	timeout	**0,048**	0,119
	3	48	0,489	timeout	**0,047**	0,287
Fuel	1	9	timeout	timeout	**0,047**	0,062
	2	18	timeout	timeout	**0,063**	0,141
	3	36	timeout	timeout	**0,302**	0,314
HBS	1	2	21,552	timeout	0,073	**0,044**
	2	48	23,236	timeout	**0,064**	0,322
	3	84	34,494	timeout	**0,154**	0,735
Quadcopter	1	1	17,511	timeout	0,039	**0,026**
	2	6	22,372	timeout	**0,038**	0,044
	3	15	37,088	timeout	**0,039**	0,076

Table 1: Temps de calcul (en s) des coupes (timeout=100s)

Cas d'études

Nom	Description	Taille DS
ROSACE	contrôleur longitudinal avion	4.10^8
FUEL	système alimentation carburant	$1,7.10^{13}$
HBS	système freinage	$6,5.10^4$
QUADCOPTER	contrôleur de drones	$1,3.10^6$

Figure 2: Cas d'études

Performance de la résolution du problème DSE

Systèmes	$1 - R(1)$	Outils	
		HipHOPS	KCR Analyser
Rosace	10^{-3}	**timeout**	7,686
	10^{-5}	**timeout**	3,512
	10^{-7}	**timeout**	4,442
	10^{-9}	**timeout**	2,559
Fuel	10^{-3}	37,431	0,602
	10^{-5}	40,142	0,145
	10^{-7}	54,024	0,366
	10^{-9}	**max itération**	0,041(Unsat)
HBS	10^{-3}	**timeout**	0,617
	10^{-5}	**timeout**	3,373
	10^{-7}	**timeout**	0,738(Unsat)
	10^{-9}	**timeout**	0,744(Unsat)
Quadcopter	10^{-3}	8,230	0,557
	10^{-5}	7,997	0,349
	10^{-7}	7,769	0,565
	10^{-9}	7,729	0,510

Table 2: Temps de résolution (en s) du problème DSE (timeout=600s)

ONERA
THE FRENCH AEROSPACE LAB

Performance : impact de l'analyse par STMDD

Temps calcul STMDD de ROSACE : 2,3s

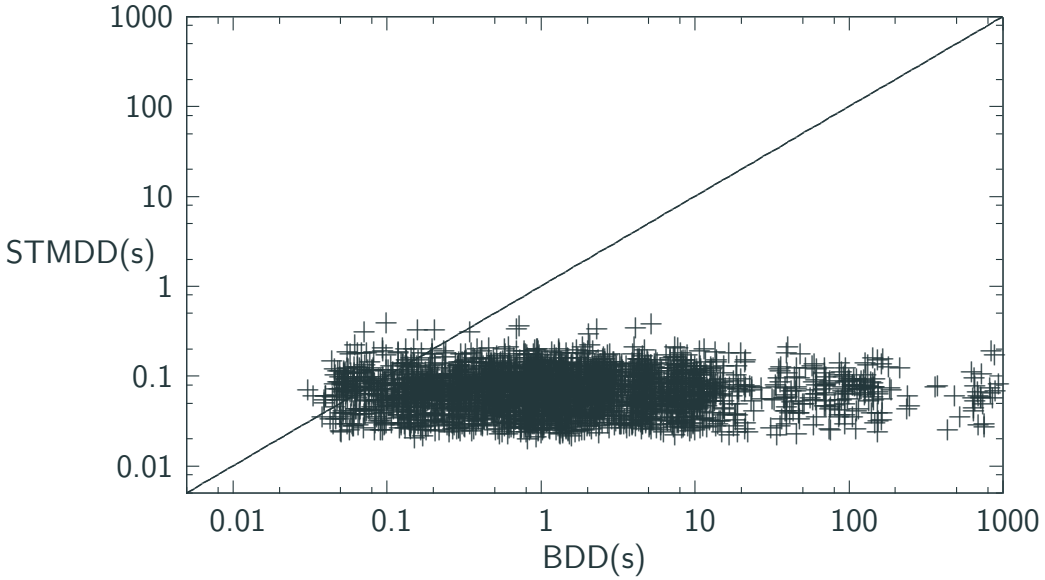


Figure 3: Temps de calcul fiabilité : BDD vs STMDD

Temps de calcul fiabilité pour un candidat aléatoire :

STMDD $\Rightarrow$ constant car réutilisation ($[0,02s; 0,2s]$),

BDD $\Rightarrow$ dépend substitutions choisies ($[0,02s; 10^3 s]$).

Plan

1. Contexte

2. Contributions

   Définition de KCR

   Résolution du problème DSE

      Développement d'analyses de sûreté pour l'exploration

      Encodage & résolution à l'aide des solveurs SMT

3. Expérimentations

4. Conclusion

Conclusion : Modélisation

Contributions (publiées dans [DDP17a]) :

- Développement de KCR :
  - modélisation dysfonctionnelle des systèmes
  - définition des exigences
  - description de l'espace des architectures

Améliorations :

- Proposer plusieurs choix densité probabilité pour événements

Perspectives :

- Modélisation générique de la notion de patron de sûreté

Conclusion : Résolution problème DSE

Contributions (publiées dans [DDP17b]) :

- Développement d'analyses de sûreté basées STMDD
- Définition théorie Safety & solveur associé
- Encodage et résolution du problème DSE

Améliorations :

✓ Considération d'exigences de sûreté sur taux de défaillance

✓ Considération coûts et préférences de substitution

- Intégration Safety plus proche du solveur SMT

Perspectives :

- Extension de la méthode aux systèmes dynamiques
- Synthèse sous contraintes multi-domaines

Merci pour votre attention

Bibliography i

André Arnold, Gérald Point, Alain Griffault, and Antoine Rauzy.
The altarica formalism for describing concurrent systems.
Fundamanta Informaticae, 40(2-3) :109–124, 1999.

Masakazu Adachi, Yiannis Papadopoulos, Septavera Sharvia, David Parker, and Tetsuya Tohdo.
An approach to optimization of fault tolerant architectures using hip-hops.
Software : Practice and Experience, 41(11) :1303–1327, 2011.

Bibliography ii

Alain Billionnet.
Redundancy allocation for series-parallel systems using integer linear programming.
Reliability, IEEE Transactions on, 57(3) :507–516, 2008.

Kevin Delmas, Rémi Delmas, and Claire Pagetti.
Smt-based architecture modelling.
In 12th IEEE International Symposium on Industrial Embedded Systems, SIES. Springer, 2017.

Kevin Delmas, Rémi Delmas, and Claire Pagetti.
Smt-based synthesis of fault-tolerant architectures.
In International Conference on Computer Safety, Reliability, and Security. Springer, 2017.

Pourquoi définir un nouveau langage textuel et pas un système d'annotation sur modèle d'architecture (UML) ?

But premier : développer un langage spécifique pour modélisation dysfonctionnelle

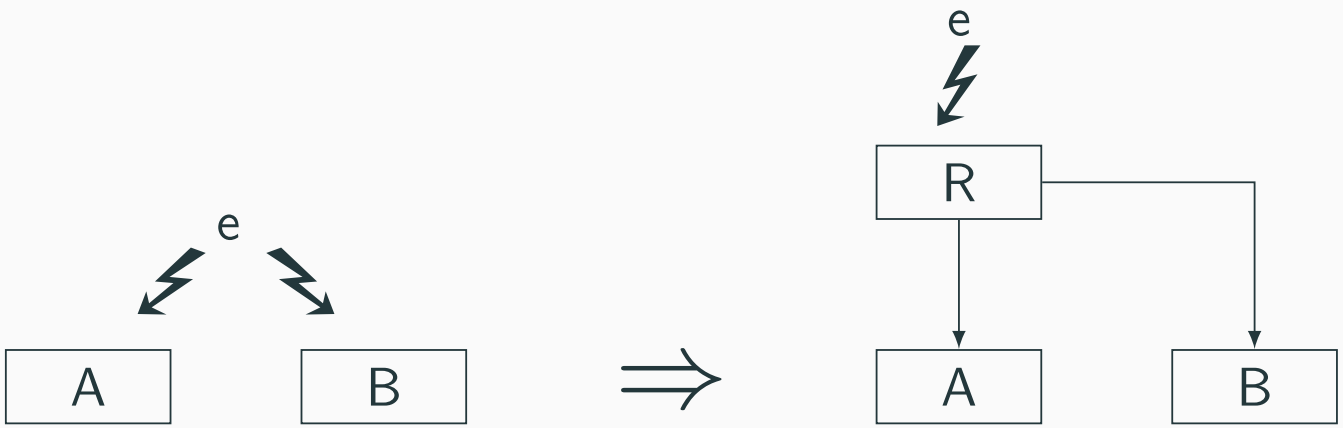
- limiter nombre de notions en jeu,
- pourvoir définir librement syntaxe et sémantique en adéquation avec notions.

Mais possible de fournir une extension d'annotation de modèle d'architecture.

Comment traiter les modes communs (puisque hypothèse d'indépendance) ?

Modéliser mode commun :

- modéliser comme ressource (entrée) nécessaire aux composants ;
- relier entrées composant unique modélisant ressource (contient événement).

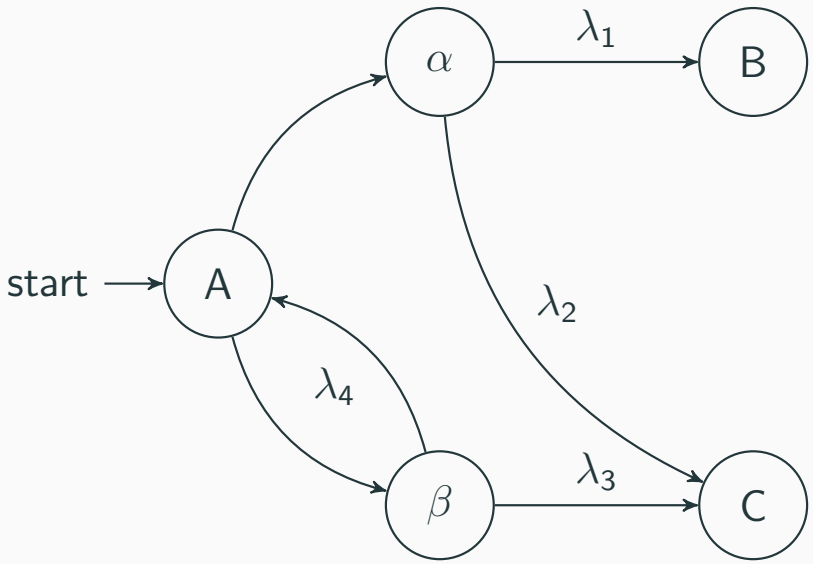


Pourquoi s'être restreint aux systèmes statiques ?

- Formalismes statiques très utilisés pour modéliser et évaluer sûreté systèmes (arbres, BDD, diagrammes fiabilité,...),
- Comportement réductible à fonction booléenne $\Rightarrow$ possibilité d'analyse avec solveurs SAT.

Comment étendre la méthode aux systèmes dynamiques ?

Modélisation utiliser langages existants comme ALTARICA
Analyse basée sur model-checking probabiliste
Exploration encoder problème comme un MDP, exploration $\Rightarrow$ synthétiser politique pour respecter exigences.



Pour quels types de systèmes peut-on utiliser cette approche ?

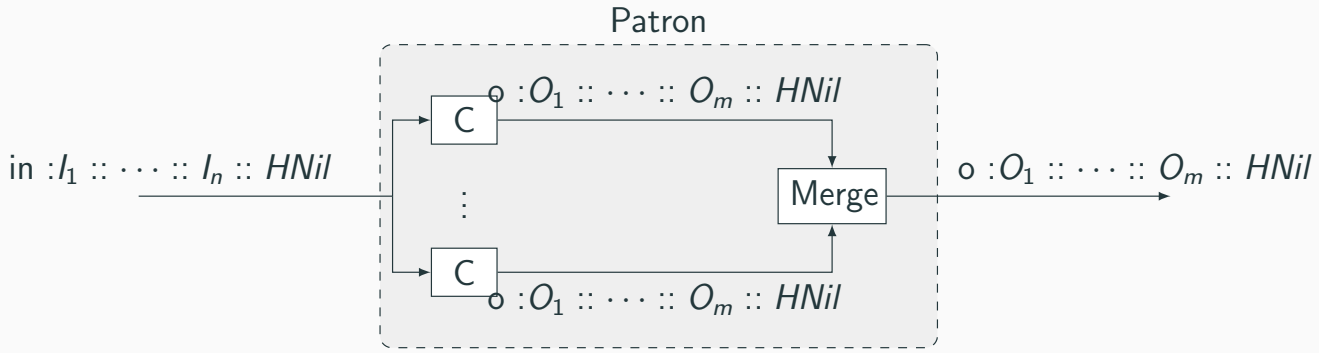
Motivation initiale tolérance aux fautes sur many cores

- pour système logiciel
- possibilité de réplication sur cœurs
- calculer et répartir application pour respecter exigences en cas rayons cosmique

Plus généralement pas contrainte sur *nature* système $\Rightarrow$ domaine application large.

Comment modéliser un patron de manière générique ?

- S'inspirer de programmation générique SCALA et librairie SHAPELESS (liste hétérogène et fonctions polymorphes)
- Composant ⇒ fonction sur liste hétérogènes
- Patron ⇒ fonction manipule composants (c'est-à-dire des fonctions)



Pourquoi s'être restreint aux systèmes non réparables ?

- Si réparation au sens statique avec des événements de réparation, possible de les prendre en compte modulo extension de KCR,
- Mais réparation généralement processus dynamique (survient à prés une panne) $\Rightarrow$ conflit avec système statique. d'analyse avec solveurs SAT.

Les analyses sont t-elles facilement adaptables à une autre distribution ?

Analyses reposes pas sur propriétés distribution

- pas restrictions sur distributions admissibles.

Adaptation : KCR doit fournir moyen de spécifier distribution.

Pourquoi les patrons respectent souvent l'hypothèse d'inclusion ?

Patron : construction améliore sûreté

- mitige ou réduit probabilité de défaillance,
- produit sous-ensemble modes de de défaillance composant,
- inclusion des traces.

Pourquoi utiliser un solveur SMT pour résoudre le problème d'énumération réductible à Sat ?

Solveur SMT : utilisé pour calculer fonction structure (besoin théorie vecteurs bit & fonctions non-interprétées).
Si φ disponible $\Rightarrow$ analyse possible utilisant uniquement $\textsc{Sat}$.

Que faire si les patrons ne préservent pas l'interface (sorties de validation) ?

Méthode non applicable car :

- pas de comparaison possibles des modes produits au interfaces,
- problème de la reconnexion $\Rightarrow$ espace des architecture $\neq$ ensemble des combinaisons des substitution possibles
- pas les mêmes flots entre composant $\Rightarrow$ impossible d'utiliser le STMDD pour représenter les scénarios système.

Comment étendre le solveur pour traiter les règles de Décision et Propagation de CDCL ?

$\mathcal{T}$ – *Propagate* Parcourir STMDD et récupérer choix de substitution indispensables pour satisfaire les exigences,

$\mathcal{T}$ – *Decision* Évaluer des facteurs d'importances (Birnbaum) pour choisir substitution.

Comment étendre le solveur pour traiter les règles de Décision et Propagation de CDCL ?

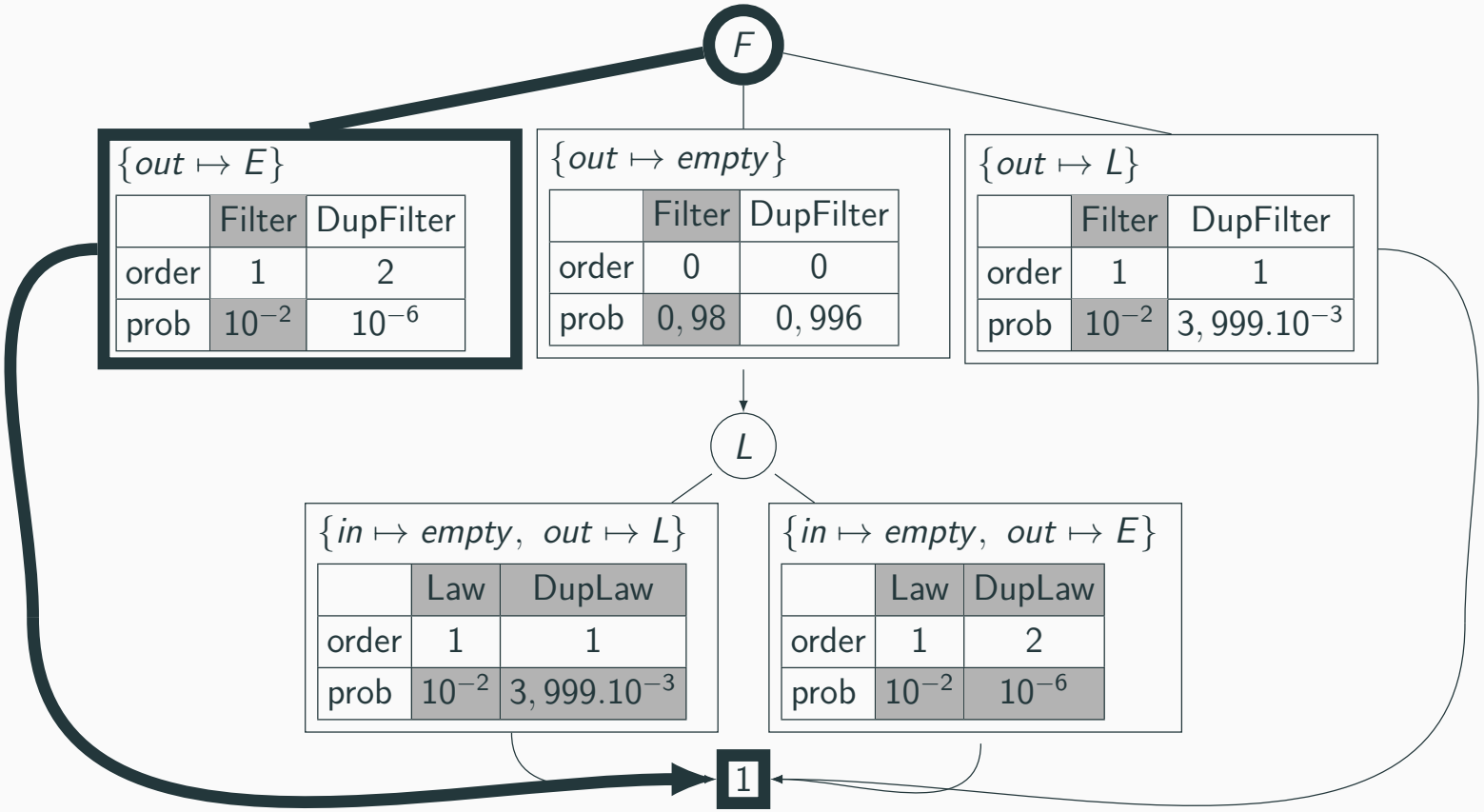
Si $F \mapsto \mathit{Filter}$ et $R \geq 0,99$ alors

$$R \leq 1 - (\qquad\qquad\qquad

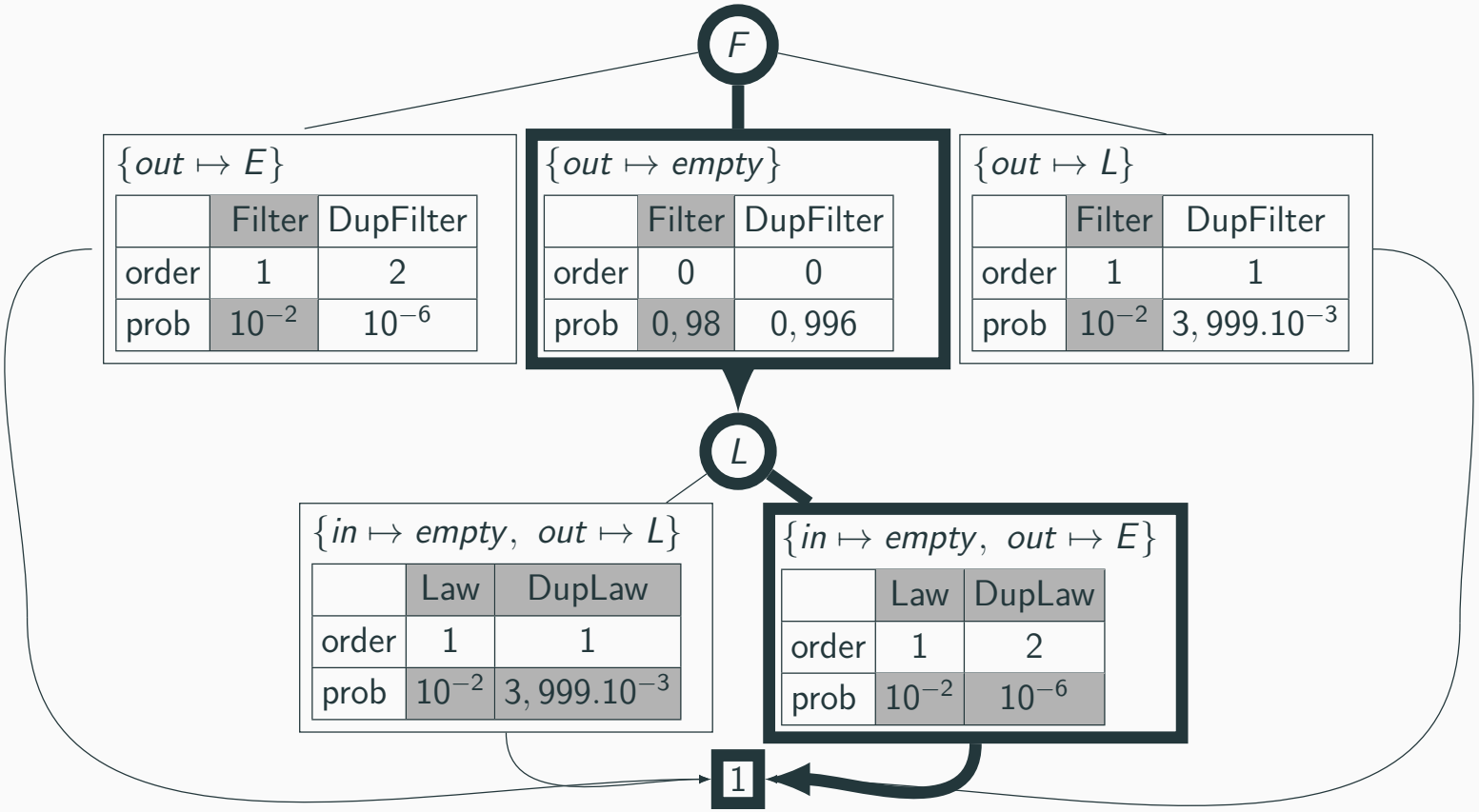
Comment étendre le solveur pour traiter les règles de Décision et Propagation de CDCL ?

Si $F \mapsto \mathit{Filter}$ et $R \geq 0,99$ alors

$$R \leq 1 - (10^{-2} + \qquad\qquad\qquad\qquad) = 0.99$$



Comment étendre le solveur pour traiter les règles de Décision et Propagation de CDCL ?

Si $F \mapsto \mathit{Filter}$ et $R \geq 0,99$ alors

$$R \leq 1 - (10^{-2} + 0,98(\mathit{min}(10^{-2}; 10^{-6})) = 0.9802$$