

VERSYDIS

**Formalismes non séquentiels
pour la vérification et la synthèse
de systèmes distribués**

Coordinateur : Paul Gastin

Objectifs

- Développer des techniques spécifiques pour assurer/étudier la sécurité des systèmes distribués.

Objectifs

- Développer des techniques spécifiques pour assurer/étudier la sécurité des systèmes distribués.
- Les applications visées sont principalement la vérification de modèles (model-checking) et la synthèse de contrôleurs.

Objectifs

- Développer des techniques spécifiques pour assurer/étudier la sécurité des systèmes distribués.
- Les applications visées sont principalement la vérification de modèles (model-checking) et la synthèse de contrôleurs.
- Les techniques usuelles ramènent le problème au cadre séquentiel.
Inconvénients :
Explosion combinatoire,
Certains concepts essentiels peuvent être perdus ou difficiles à retrouver : causalité, distinction entre concurrence et choix, ...

Objectifs

- Développer des techniques spécifiques pour assurer/étudier la sécurité des systèmes distribués.
- Les applications visées sont principalement la vérification de modèles (model-checking) et la synthèse de contrôleurs.
- Les techniques usuelles ramènent le problème au cadre séquentiel.
Inconvénients :
Explosion combinatoire,
Certains concepts essentiels peuvent être perdus ou difficiles à retrouver : causalité, distinction entre concurrence et choix, ...
- Au contraire, dans le projet VERSYDIS nous cherchons à exploiter la concurrence.

Exploiter la concurrence

Pour cela, nous devons développer

- les **modèles** : principalement à base d'ordres partiels,
- les formalismes de **spécification** : logiques temporelles distribuées, MSC, μ -calcul, ...
- une **algorithmique** spécifique à ces formalismes

Problème du contrôle

Données :

- M modèle du système ouvert
- S spécification : description des comportements désirables.

Problème : Trouver un contrôleur C tel que

$$(M \otimes C) \parallel Environment \models S$$

.

Il y a en fait deux problèmes : existence et synthèse.

Problème du contrôle revisité

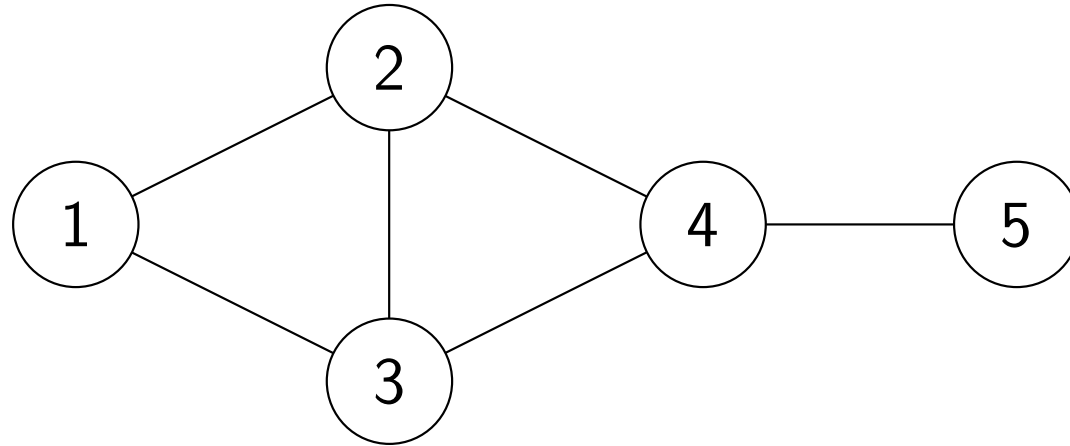
Données :

- M modèle du système fermé (système à contrôler + environnement)
- actions contrôlables Σ_c (système) ou incontrôlables Σ_u
- actions observables ou non
- S spécification.

Problème : Trouver un contrôleur C tel que $M \otimes C \models S$.

Le contrôleur sélectionne une action contrôlable en fonction de ce qu'il a pu observer.

Contrôle distribué



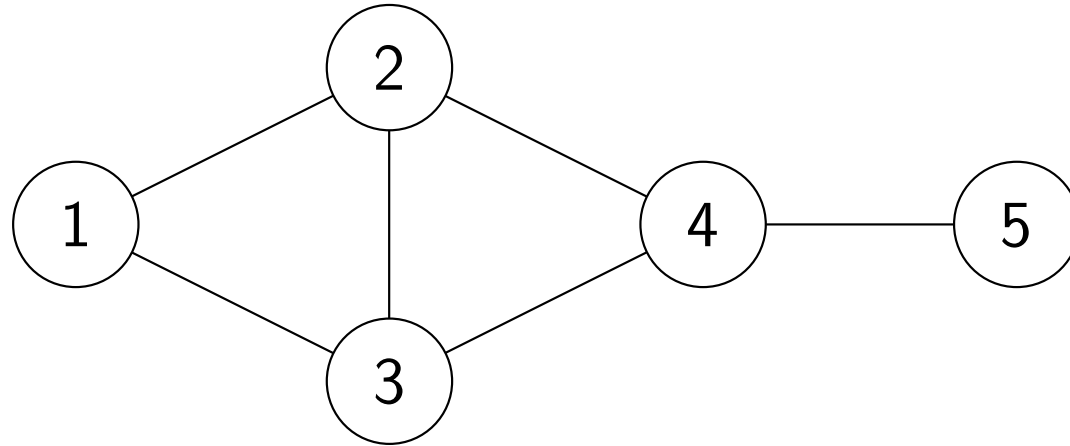
Le système est distribué : $M = M_1 \parallel \dots \parallel M_k$.

Les actions peuvent être locales ou synchronisées.

Communication : l'action a lit les cellules $R(a)$ et écrit dans $W(a)$.

$$R, W : \Sigma \rightarrow 2^{\{1, \dots, k\}}$$

Contrôle distribué



Le système est distribué : $M = M_1 \parallel \dots \parallel M_k$.

Les actions peuvent être locales ou synchronisées.

Communication : l'action a lit les cellules $R(a)$ et écrit dans $W(a)$.

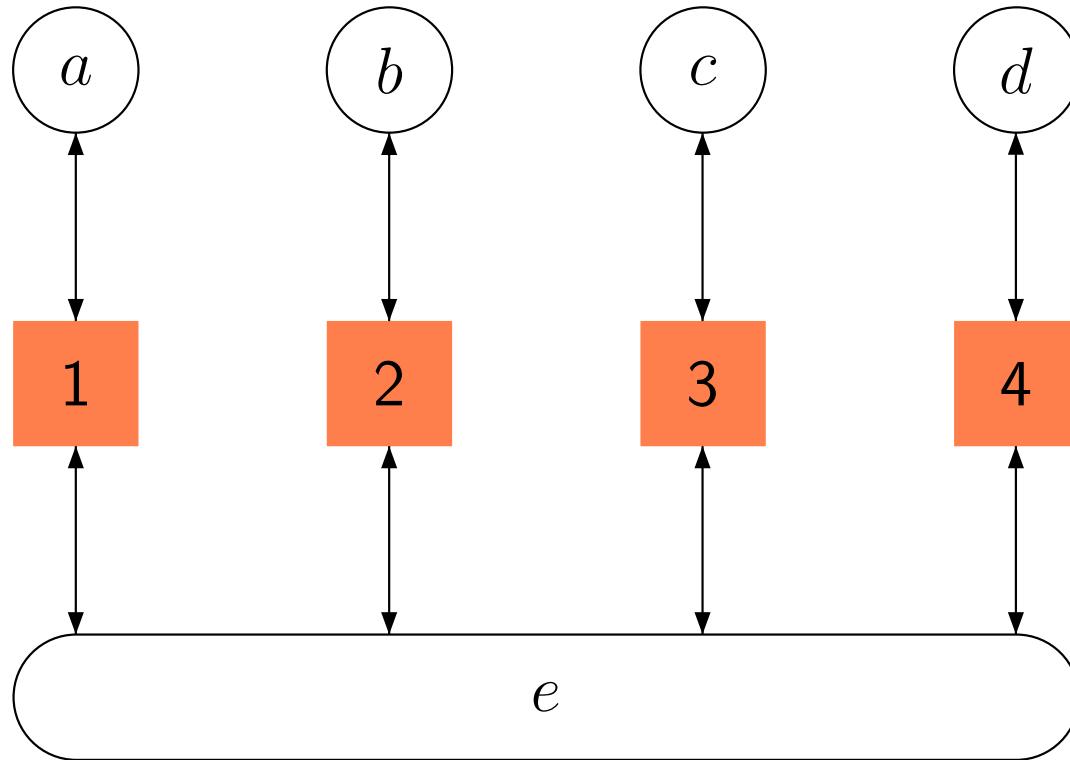
$$R, W : \Sigma \rightarrow 2^{\{1, \dots, k\}}$$

Architecture cellulaire : $\forall a \in \Sigma, |W(a)| = 1$ et $W(a) \subseteq R(a)$.

Contrôle distribué

Exemple : système local et synchrone

- $\Sigma_u = \{e\}$ avec $R(e) = W(e) = \{1, \dots, k\}$
- $\forall a \in \Sigma_c, \exists i \in \{1, \dots, k\}, R(a) = W(a) = \{i\}$.



Contrôle distribué

Approche séquentielle : contrôler $M = M_1 \parallel \dots \parallel M_k$.

$$(M_1 \parallel \dots \parallel M_k) \otimes C \models S$$

Problème : comment distribuer le contrôleur ?

Contrôle distribué

Approche séquentielle : contrôler $M = M_1 \parallel \dots \parallel M_k$.

$$(M_1 \parallel \dots \parallel M_k) \otimes C \models S$$

Problème : comment distribuer le contrôleur ?

Approche distribuée : Trouver C_1, \dots, C_k tels que

$$(M_1 \otimes C_1) \parallel \dots \parallel (M_k \otimes C_k) \models S$$

Contrôle distribué : difficultés

Les contrôleurs locaux ne communiquent pas (directement) entre eux.

Le système peut être asynchrone.

Un contrôleur local n'a accès qu'à une information partielle.

- Le contrôleur peut n'observer que la suite des états locaux.
- Le contrôleur peut observer tout ce qui est dans son passé.

La mémoire du contrôleur peut être restreinte (sans mémoire, mémoire bornée, mémoire totale).

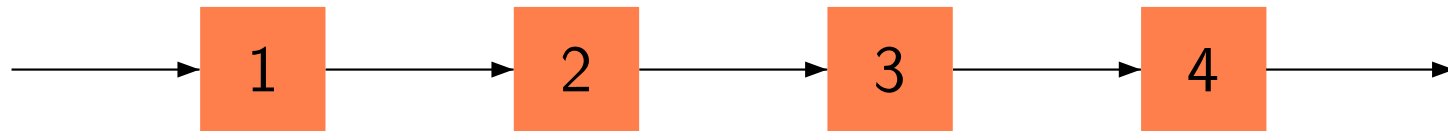
La spécification peut être locale ou globale.

La spécification peut être plus ou moins complexe (FO, régulière, ...)

Travaux existants

Pnueli et Rosner, 1990.

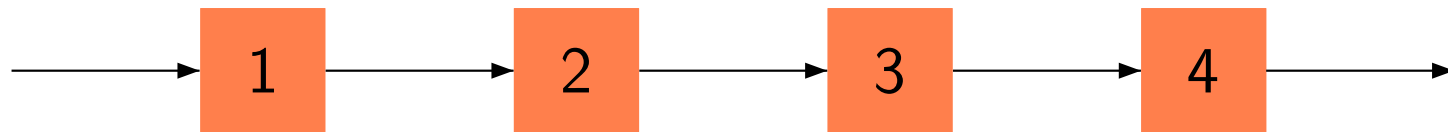
- Système synchrone, communication contrôlée par l'environnement.
- Spécification globale.



Travaux existants

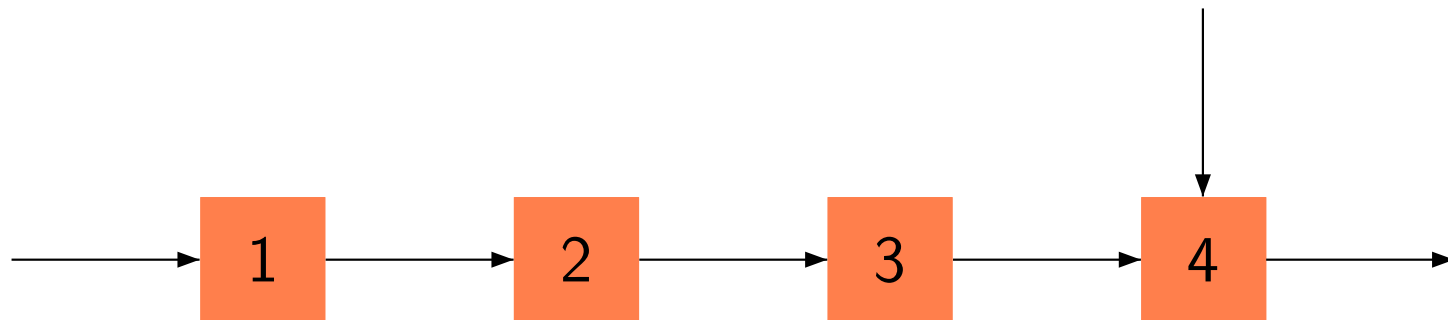
Pnueli et Rosner, 1990.

- Système synchrone, communication contrôlée par l'environnement.
- Spécification globale.



Madhusudan et Thiagarajan, 2001.

- Système synchrone, communication contrôlée par l'environnement.
- Spécification locale.



Approche : jeux distribués

- Graphe du jeux : système à contrôler
- Équipe 1 : actions contrôlables
- Équipe 2 : actions incontrôlables (environnement)
- Condition de gain : spécification
- Stratégie gagnante : contrôleur.

Approche : jeux distribués

- Graphe du jeu : système à contrôler
- Équipe 1 : actions contrôlables
- Équipe 2 : actions incontrôlables (environnement)
- Condition de gain : spécification
- Stratégie gagnante : contrôleur.

Objectif du projet : mettre à jour des classes décidables et développer des algorithmes pour synthétiser des contrôleurs distribués.

Approche : jeux distribués

- Graphe du jeu : système à contrôler
- Équipe 1 : actions contrôlables
- Équipe 2 : actions incontrôlables (environnement)
- Condition de gain : spécification
- Stratégie gagnante : contrôleur.

Objectif du projet : mettre à jour des classes décidables et développer des algorithmes pour synthétiser des contrôleurs distribués.

Premières contributions :

Arnold, Mohalik, Vincent, Walukiewicz : Jeux synchrones.

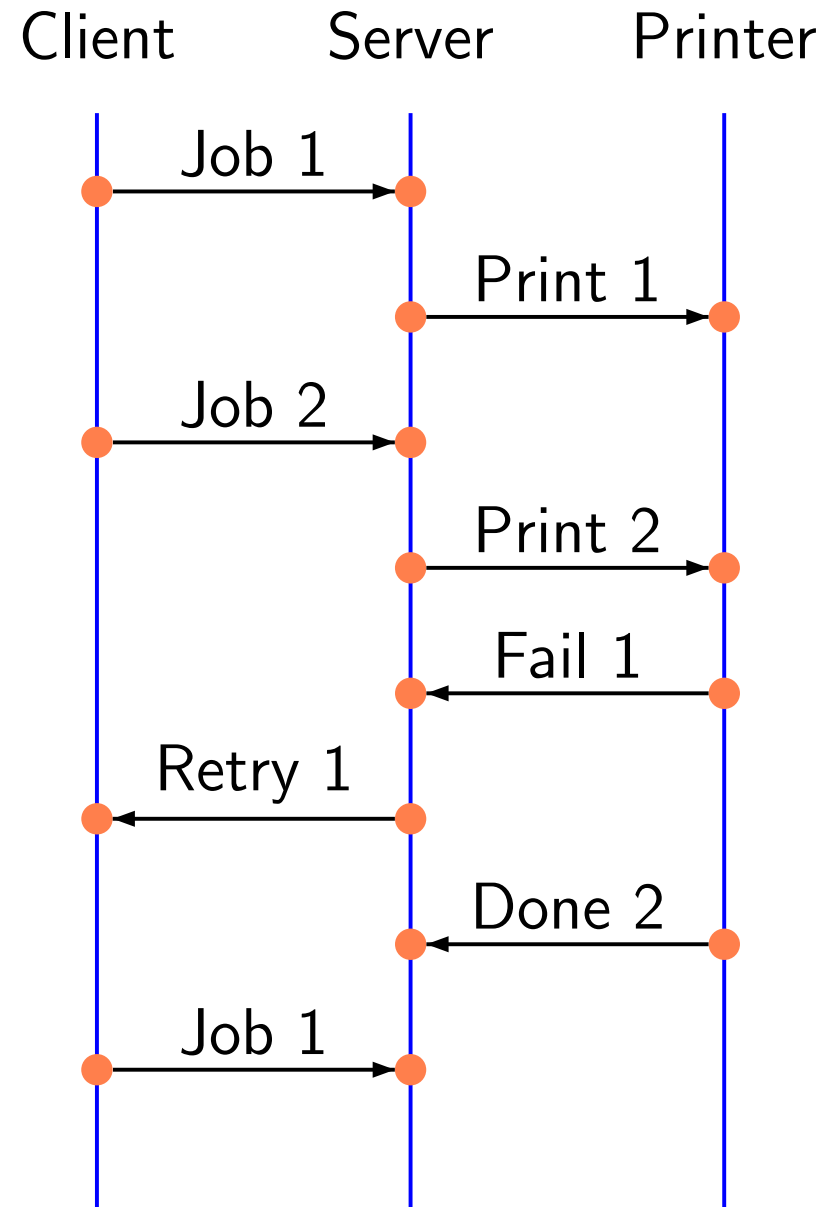
- Réduction du nombre de joueurs.
- Réduction du non déterminisme.

Gastin, Lerman, Zeitoun : Jeux asynchrones.

MSC : Diagrammes de séquences

- Formalisme visuel pour la description d'exécutions de systèmes distribués
- Utilisé pour décrire les comportements souhaités ou interdits
- Standard de l'ITU Z120 (1996, 2000), intégré dans UML

Difficultés : communication asynchrone et canaux non bornés.



MSC : Diagrammes de séquences

Travaux récents et en cours :

- Classes de HMSCs pour lesquelles on peut faire du Model Checking.
- Classes de HMSCs que l'on peut réaliser par des automates communicants.
- Spécifications à l'aide de MSCs à trous.

Travaux futurs :

- Spécification de problèmes de contrôle à l'aide de MSCs.
- Décision et synthèse de contrôleurs.

Spécifications pour les systèmes distribués

Actuellement :

- le modèle est un système distribué.
- le langage de spécification porte sur les exécutions séquentielles.

Inconvénients :

- Nécessité de séquentialiser le modèle pour l'étudier (explosion combinatoire).
- On peut distinguer des linéarisations d'un même comportement distribué.

Objectif : Logiques temporelles pour les ordres partiels.

Logiques temporelles distribuées

- **Expressivité** : les logiques temporelles locales ont le pouvoir d'expression de FO, donc peuvent exprimer les propriétés globales.
- **Complexité** : les logiques temporelles locales sont décidables en PSPACE (comme les logiques temporelles séquentielles).

Logiques temporelles distribuées

- **Expressivité** : les logiques temporelles locales ont le pouvoir d'expression de FO, donc peuvent exprimer les propriétés globales.
- **Complexité** : les logiques temporelles locales sont décidables en PSPACE (comme les logiques temporelles séquentielles).
- **Distribution d'une spécification globale**

$$\varphi = \bigvee_i \bigwedge_j \varphi_{i,j}$$

où $\varphi_{i,j}$ est une propriété locale du composant j du système.

Projet : model checking modulaire pour les systèmes séries-parallèles.

Partenaires

	LaBRI, Bordeaux	LIAFA, Paris
Permanents	Janin David, MCF Ly Olivier, MCF Walukiewicz Igor, CR Weil Pascal, DR	Gastin Paul, Prof. Muscholl Anca, Prof. Zeitoun Marc, MCF Zielonka Wieslaw, Prof.
Doctorants	Bernet Julien Bouquet Alexis Nguena-Timo Omer	Genest Blaise Gimbert Hugo Lerman Benjamin