Vérification de réseaux de Petri avec états sous une sémantique d'ordres partiels

Florent Avellaneda, Rémi Morin

Vérification de réseaux de Petri avec états sous une sémantique d'ordres partiels

Florent AVELLANEDA [1], **Rémi MORIN** [2]

Aix-Marseille Université, CNRS, LIF UMR 7279, 13000, Marseille, France
florent.avellaneda,remi.morin@lif.univ-mrs.fr

RÉSUMÉ. *Afin de munir le formalisme des MSG de compteurs, de timers et d'autres aspects, nous introduisons le modèle des réseaux de Petri avec états et une sémantique de processus non-branchants. Ce modèle est non seulement plus expressif que les MSG, mais il permet également des spécifications plus concises. Nous nous intéressons à trois problèmes de vérification classiques sur l'ensemble des marquages accessibles par les préfixes des processus : le caractère borné, la couverture et l'accessibilité. Nous montrons comment réduire ces problèmes au cas particulier des réseaux de Petri de telle sorte que tous les résultats de complexité et de décidabilité s'étendent des réseaux de Petri aux réseaux avec états sous la sémantique des processus. Nous introduisons aussi la notion de borne semi-structurelle afin de considérer des systèmes paramétrés. Cela consiste à fixer le marquage initial d'un sous-ensemble approprié de places, puis à vérifier que le système est borné quel que soit les valeurs des paramètres. Nous montrons comment un dépliage conduit à un problème plus simple à vérifier à l'aide de la Programmation Linéaire.*

ABSTRACT. *In order to study MSC specifications with counters, timers and other features, we introduce the model of Petri nets with states together with a non-branching non-sequential process semantics. We obtain a framework that is more expressive and more concise than MSGs. We consider then three classical verification problems for the set of markings reached by prefixes of processes: boundedness, covering and reachability. We show that each of these problems boils down to the equivalent problem for Petri nets. We consider also the notion of semi-structural property in order to study parametrized systems. In this way, only part of the places are provided with an initial marking. Unfolding such a system leads to a simpler problem in the form of a linear programme.*

MOTS-CLÉS : *Réseaux de Petri, diagramme de séquence, caractère borné.*

KEYWORDS: *Petri nets, Message sequence charts, Divergence.*

1. Introduction

Un MSC ou « Messages Sequence Chart » donne une description graphique d'un scenario de communication entre des processus sous la forme d'un ordre partiel. Ce modèle est souvent utilisé pour la documentation des protocoles de télécommunication et a fait l'objet de nombreux travaux ces dernières années (Reniers, 1998 ; Hélouët, 2000 ; Genest, 2004 ; Bollig, 2005). Ils bénéficient d'une présentation visuelle et textuelle normalisée par l'ITU (recommandation Z.120) et sont proches d'autres formalismes tels que les diagrammes de séquence de UML.

Les MSG (pour « Message sequence graphs ») sont utilisés pour décrire des ensembles de scénarios. Ils se représentent simplement sous la forme d'un graphe orienté avec des noeuds étiquetés par des MSC. De nombreux outils ont déjà été développés afin de spécifier les protocoles sous forme de MSG. Certains d'entre eux mettent en oeuvre également des techniques de vérification formelle (Ben-Abdallah, Leue, 1998 ; Hélouët, 2012 ; Holzmann *et al.*, 1997 ; Bezdeka *et al.*, 2012).

Bien que les MSG aient été souvent étudiés, on peut noter qu'ils souffrent d'une certaine rigidité. En effet, les notions de variables ou de compteurs sont le plus souvent exclues. Nous introduisons un modèle qui généralise à la fois les réseaux de Petri et les MSG et qui permet ainsi l'utilisation de compteurs dans des MSG étendus; il est non seulement plus expressif que les MSG, mais permet également de proposer des spécifications plus concises.

2. Réseaux de Petri avec états

Considérons un ensemble de réactions qui ont lieu au sein d'une collection de particules telles que chaque réaction consomme un multi-ensemble de particules disponibles et produit une combinaison linéaire d'autres types de particules. Considérons de plus un état de contrôle qui détermine si une règle peut se produire ou non et tel que l'exécution de cette règle conduit à un nouvel état de contrôle. Ce modèle correspond aux réseaux de Petri avec états, ou PNS pour « Petri Net with States », semblables à des systèmes d'addition de vecteurs avec états (Hopcroft, Pansiot, 1979), sans leur restriction aux règles pures.

Nous adoptons une sémantique d'ordres partiels pour les PNS qui étend la sémantique habituelle des processus pour les réseaux de Petri. L'approche est simple et naturelle. D'abord, nous considérons l'ensemble des séquences de calculs franchissables d'un PNS, ensuite nous définissons les processus qui représentent une séquence donnée. Ainsi, chaque processus décrit des dépendances causales entre les événements qui ne sont plus totalement ordonnés. Cela signifie que deux règles qui apparaissent l'une après l'autre dans une séquence de règles d'un PNS peuvent se produire simultanément dans un processus.

Ce phénomène est bien connu dans les systèmes asynchrones et correspond précisément à la façon dont les MSC d'un MSG sont obtenus. Ainsi, les états de contrôle représentent des étapes abstraites de calculs utilisées pour spécifier des ensembles par-

ticuliers de séquences de règles : ils n'apparaissent pas formellement dans la sémantique des processus. De cette façon, les MSG sont inclus dans le cadre des PNS. Néanmoins une caractéristique de la sémantique adoptée est qu'une séquence de règles peut donner lieu à plusieurs processus non isomorphes en fonction de l'ordre de consommation de particules identiques alors que les MSC sont en général FIFO.

3. Vérification

Nous nous intéressons à trois problèmes de vérification classiques sur l'ensemble des marquages accessibles par les préfixes des processus : le caractère borné, la couverture et l'accessibilité. Nous montrons comment réduire ces problèmes au cas particulier des réseaux de Petri de telle sorte que tous les résultats de complexité et de décidabilité s'étendent des réseaux de Petri aux PNS sous la sémantique des processus. La notion de non-divergence (aussi appelée borne universelle) pour un MSG coïncide avec le caractère borné par préfixe pour les PNS. Cependant, l'expressivité des PNS est plus grande que celle des MSG. Alors que la divergence d'un MSG est NP-complet, le caractère borné par préfixe d'un PNS requiert un espace exponentiel.

Pour contourner ce problème, nous proposons d'abstraire les propriétés à vérifier, de sorte que si l'abstraction de cette propriété est vraie, alors cette propriété est vraie. L'abstraction que nous proposons est de vérifier les propriétés de manière structurelle, c'est-à-dire indépendamment du marquage initial. Nous pouvons citer par exemple le caractère structurellement borné qui assure que, quel que soit le marquage initial, le nombre de particules est borné au cours des exécutions. Cette abstraction est intéressante, car vérifier le caractère borné d'un réseau de Petri muni d'une configuration initiale nécessite un espace exponentiel (Lipton, 1976) alors que vérifier le caractère structurellement borné est polynomial (Memmi, Roucairol, 1980).

Il est alors intéressant de pouvoir définir le degré d'abstraction souhaité. En effet, si une propriété n'est pas vraie structurellement, nous ne pouvons rien dire sur la véracité de cette propriété pour un marquage initial donné. Ceci est d'autant plus vrai pour les MSG étendus. Une instance I étant vue comme un jeton dans une place I, la vérification de propriété structurelle abstrait également les instances en omettant le fait que chaque instance est unique. Cette abstraction étant trop forte, beaucoup de propriétés vraies risquent d'être fausses structurellement.

Afin de pouvoir définir un degré d'abstraction souhaité, nous introduisons la notion de propriété semi-structurelle. Cela consiste à fixer le marquage initial d'un sous-ensemble approprié de places, puis de vérifier les propriétés structurelles sur les places restantes. Pour cela, nous déplions le PNS afin de faire disparaître les places dont nous conservons le marquage. Les propriétés structurelles sur le PNS ainsi obtenu déterminent les propriétés semi-structurelles du PNS d'origine. Nous pouvons ainsi vérifier une propriété sans fixer la valeur initiale de certaines variables vue comme des paramètres du système.

4. Conclusion

Afin d'ajouter des notions de variables et de compteurs au MSG, nous avons introduit le modèle des Réseaux de Petri avec états (ou PNS pour « Petri Net withs States ») sous une sémantique de processus. Ce modèle est non seulement plus expressif que les MSG, mais permet également des spécifications plus concises.

Nous nous sommes intéressés à trois problèmes de vérification classiques sur l'ensemble des marquages accessibles par les préfixes des processus : le caractère borné, la couverture et l'accessibilité. Nous avons montré comment réduire ces problèmes au cas particulier des réseaux de Petri. Ainsi, tous les résultats de complexité et de décidabilité s'étendent des réseaux de Petri aux PNS sous la sémantique des processus.

Les PNS pouvant décrire une infinité de MSG en fonction de la valeur de ses variables, nous avons introduit la notion de propriété semi-structurelle. Cela consiste à fixer le marquage initial d'un sous-ensemble approprié de places, puis de vérifier les propriétés structurelles sur les places restantes. Nous pouvons ainsi vérifier une propriété sans fixer la valeur initiale de certaines variables.

Bibliographie

Ben-Abdallah H., Leue S. (1998). MESA: Support for scenario-based design of concurrent systems. In B. Steffen (Ed.), *Tacas*, vol. 1384, p. 118-135. Springer.

Bezdeka M., Bouda O., Korenciak L., Madzin M., Rehák V. (2012). Sequence chart studio. In J. Brandt, K. Heljanko (Eds.), *Acsd*, p. 148-153. IEEE.

Bollig B. (2005). *Automata and logics for message sequence charts*. Thèse de doctorat, Department of Computer Science, RWTH Aachen, Germany. Consulté sur http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/Bollig-phd.pdf

Genest B. (2004). *The odyssey of msc-graphs*. Thèse de doctorat, Université Paris 7.

Hélouët L. (2000). *Analyse des exigences des systèmes répartis exprimées par des langages de scénarios*. Thèse de doctorat, Rennes.

Hélouët L. (2012). *A Scenario Oracle and Formal Analysis Toolbox (SOFAT).* http://www.irisa.fr/distribcom/Prototypes/SOFAT. ([Online; accessed 7-Oct-2012])

Holzmann G. J., Peled D. A., Redberg M. H. (1997). Design tools for requirements engineering. *Bell Labs Technical Journal*, vol. 2, p. 86–95.

Hopcroft J., Pansiot J.-J. (1979). On the reachability problem for 5-dimensional vector addition systems. *Theoretical Computer Science*, vol. 8, p. 135-159.

Lipton R. (1976). *The reachability problem requires exponential space*. Rapport technique n° 63. Yale University.

Memmi G., Roucairol G. (1980). Linear algebra in net theory. In W. Brauer (Ed.), *Advanced course: Net theory and applications*, vol. 84, p. 213-223. Springer.

Reniers M. (1998). *Message sequence chart: Syntax and semantics*. Phd thesis, Eindhoven University of Technology.