# LOG 8470

Méthodes formelles en fiabilité et sécurité

# TP1 : MODEL CHECKING - iSPIN

| | |
|---|---|
| Session | Automne 2019 |
| Pondération | 7.5 % de la note finale |
| Taille des équipes | 2 étudiants |
| Date de remise du projet | 28 0ctobre 2019 pour le groupe 2 et 4 Novembre 2019 pour le groupe 1 (23h55 au plus tard) |
| Directives particulières | Soumission du livrable par moodle uniquement (https ://moodle.polymtl.ca). |
| | Toute soumission du livrable en retard est pénalisée à raison de 10% par jour de retard. |

## 1 Connaissances requises

— Notions de modélisation formelle des systèmes concurrents

— Logique Temporelle Linéaire (LTL).

## 2 Protocole d'exclusion mutuelle

On suppose un nombre arbitraire N (pour $N > 0$) de processus identiques (mais d'identité unique) qui s'exécutent en parallèle. Le but de cet exercice est de modéliser, de spécifier et de vérifier un protocole d'exclusion mutuelle de ces N processus. Il y a une variable globale flag, qui est un tableau de longueur N tel que $flag[i]$ est une valeur entre 0 et 4 (pour $0 < i < N$). L'idée est que $flag[i]$ indique le statut du processus i. Le protocole exécuté par le processus i est décrit comme suit :

0 :**while** true **do**
**begin**
1 : section non critique
2 : $flag[i] := 1$;
3 : attendre ($flag[0] < 3$ and $flag[1] < 3$ and ... and $flag[N-1] < 3$);
4 : $flag[i] := 3$;
5 : **if** ($flag[0] = 1$ or $flag[1] = 1$ or ... or $flag[N-1] = 1$) **then**
**begin**
6 :$flag[i] := 2$;
7 : attendre ($flag[0] = 4$ or $flag[1] = 4$ or ... or $flag[N-1] = 4$) ;
**end**
8 : $flag[i] := 4$;
9 : attendre ($flag[0] < 2$ and $flag[1] < 2$ and ... and $flag[i-1] < 2$) ;
10 : section critique
11 : attendre ($flag[i+1]$ $\epsilon \{0, 1, 4\}$ *and...and* flag[N-1] $\epsilon \{0, 1, 4\}$);
12 : $flag[i] := 0$;

**end**,

1. Modélisez ce protocole en Promela. Vous pouvez assumer que tous les tests sur la variable globale flag sont atomiques. Étudiez attentivement les indices de la variable flag utilisée dans les tests. Concevez votre modèle de façon modulaire de sorte que le nombre de processus puisse être modifié facilement.
2. Vérifiez pour plusieurs valeurs de N ($N \geq 2$) que le protocole assure bien l'exclusion mutuelle en utilisant LTL. Rapportez vos résultats pour N = 4.
3. Le code du protocole peut être subdivisé en plusieurs segments. L'énoncé [4] est le seuil, le segment [5], [6] et [7] est la salle d'attente et le segment [8] à [12], la chambre critique. Vérifiez les requis suivants en les spécifiant en LTL. Indiquez pour chacun des cas les modifications effectuées au modèle Promela original et présentez les résultats de la vérification.
   — Dès qu'un processus est dans la chambre critique, le seuil est vérouillé c'est à dire, aucun processus n'est à la ligne [4].
   — Si un processus i est à la ligne [10], [11] ou [12] alors il a le plus petit indice parmi tous les processus qui sont dans la salle d'attente et la chambre critique.
   — Si un processus est à la ligne [12] alors tous les processus dans la salle d'attente et la chambre critique ont la valeur du flag à 4.

# 3 Système triplement redondant

Un système triplement redondant comprend quatre composantes $P_1, P_2, P_3$, V . Les composantes redondantes $P_i, for\ i = 1, 2, 3$, exécutent la même tâche et produisent de manière continue les valeurs de sortie $p_1, p_2$, et $p_3$ , respectivement. Pour tout i = 1, 2, 3, $p_i\ \epsilon\{0, 1\}$. La composante élective V prends tous les $p_i$ en entrée (un par un) et calcule en sortie $v(p_1, p_2, p_3)$ tel que s'il y a majorité d'une valeur des entrées $p_i$, alors cette valeur est choisie comme sortie $v$. Par exemple, considérons $p_1 = 1, p_2 = 0, p_3 = 1$, alors $v(p_1, p_2, p_3) = 1$. Pour $p_1 = 0, p_2 = 0, p_3 = 1$ ,la sortie $v(p_1, p_2, p_3)$ vaut 0.

1. Écrivez un modèle PROMELA de ce système. Modélisez les trois composantes redondantes et la composante élective par des processus différents. Faites communiquer les processus par canaux.
2. Effectuez une première vérification de cohérence de votre modèle en le simulant avec SPIN.
3. Étendez votre modèle PROMELA de telle sorte que vous puissiez vérifier que la composante élective choisit réellement la bonne valeur. Spécifiez ce requis en LTL.
4. Effectuez la vérification de cette propriété avec SPIN.
5. Supposez maintenant que les Pi génèrent les sorties $p_i\ \{0, 1, ..., n\}$ pour $n \geq 2$ fixé. Exécutez le simulateur et observez ce qui arrive. Ce qui arrive dépends de votre implémentation donc décrivez et expliquez.
6. Modifiez la composante élective de façon à ce qu'une sortie ne soit produite que lorsqu'une majorité des valeurs d'entrée existe.
7. Spécifiez cette propriété en LTL et vérifiez qu'elle est bien satisfaite par votre modèle.

# 4 Livrable

Le livrable attendu est constitué des sources et du rapport de laboratoire. Le livrable est une archive (ZIP ou RAR) dont le nom est formé des numéros de matricule des membres de l'équipe, séparés par un trait de soulignement (_). L'archive contiendra les fichiers suivants :

— le rapport au format PDF ;

— tout autre fichier source ou sortie créé par iSpin, jugé pertinent, et correctement référencé dans le rapport.

### 4.1 Rapport

Un rapport de laboratoire rédigé avec soin est requis à la soumission (format .pdf,). Sinon, votre travail ne sera pas corrigé (aussi bien le code source que l'exécutable). Le rapport doit obligatoirement inclure les éléments ou sections suivantes :

1. Page présentation : elle doit contenir le libellé du cours, le numéro et l'identification du TP, la date de remise, les matricules et noms des membres de l'équipe.
2. Introduction avec vos propres mots pour mettre en évidence le contexte et les objectifs du TP.
3. Présentation de vos travaux : une explication de votre solution.
4. Difficultés rencontrées lors de l'élaboration du TP et les éventuelles solutions apportées.
5. Conclusion : expliquez en quoi ce laboratoire vous a été utile, ce que vous avez appris, vos attentes par rapport au prochain laboratoire, etc.

**Notez que vous ne devez pas mettre le code source dans le rapport.**

### 4.2 Soumission du livrable

La soumission doit se faire uniquement par Moodle.

## 5 Évaluation

| **Éléments évalués** | Points |
|---|---|
| **Qualité du rapport** : respect des exigences du rapport, qualité de la présentation des solutions | 10% |
| **Qualité du programme** : commentaires, documentation, clarté, etc. | 10% |
| **Composants implémentés :** respect des requis, logique de développement, etc. | |
| Q1.1 | 10% |
| Q1.2 | 10% |
| Q1.3.a | 5% |
| Q1.3.b | 5% |
| Q1.3.c | 5% |
| Q2.1 | 10% |
| Q2.2 | 5% |
| Q2.3 | 5% |
| Q2.4 | 5% |
| Q2.5 | 10% |
| Q2.6 | 5% |
| Q2.7 | 5% |
| Total de points | 100% |

## 6 Documentation

— Tutoriel de Promela, par Laure Petrucci.

— Site officiel de Spin : http ://spinroot.com/spin/whatispin.html.

— Les notes de cours.