Université Bordeaux I
U.F.R. Mathématiques et Informatique

D.E.S.S. de Génie Logiciel
Année 1998-1999

Spécifications et vérifications formelles
Examen de janvier 1999.
(Alain Griffault)

1 Introduction

Cet exercice est inspiré de la vie de tous les jours.

Il consiste, en partant d'une spécification informelle d'un distributeur de boissons chaudes, d'une part à modéliser le fonctionnement de la spécification en terme d'un système de transition synchronisé validé ; d'autre part de faire les choix nécessaires afin que des propriétés d'honnêteté soient satisfaites.

2 Un distributeur de boissons chaudes

Un constructeur désire construire un distributeur de café et de chocolat chauds. Voici une liste de contraintes auxquelles il a pensé.

1. le client pourra choisir parmi les boissons suivantes :
   - café non sucré,
   - café sucré,
   - chocolat non sucré,
   - chocolat sucré.
2. le prix des consommables sera (dans une unité quelconque) :
   - café : 2,
   - chocolat : 3,
   - sucre : 1,
   - eau et gobelet : gratuits.
3. la machine acceptera les pièces de 1,2 et 5 unités.
4. la machine rendra la monnaie.
5. le client pourra au choix : choisir une boisson puis mettre l'argent en quantité suffisante, ou bien mettre l'argent puis choisir.
6. le client pourra à tout instant annuler ses choix, la machine reviendra alors dans son état initial, et rendra notamment les pièces déjà introduites.
7. un opérateur pourra "de temps en temps" effectuer les actions suivantes :
   - vider le monayeur,
   - ajouter du café,
   - ajouter du chocolat,
   - ajouter du sucre,
   - ajouter des gobelets.
8. la machine sera raccordée directement au service de distribution en eau, que l'on supposera toujours opérationnel.

3 Les spécifications

Le constructeur est un homme honnête, mais pas philanthrope. Il désire donc que sa machine vérifie les propriétés suivantes :

1. La machine ne délivre pas de boissons si l'argent correspondant n'a pas été introduit.
2. La machine ne garde pas plus d'argent que le prix de la boisson servie.
3. La machine ne remplace pas une boisson par une autre sans l'accord du client.
4. La machine est opérationnelle tant qu'elle peut rendre au moins un des services.

4 Travail demandé

Vous devez :

1. construire un modèle du distributeur,
2. convaincre le constructeur qu'il s'agit bien d'un distributeur de boissons,
3. montrer que les quatres propriétés souhaitées sont satisfaites,
4. exhiber éventuellement d'autres propriétés susceptibles de plaire au constructeur.

5 Modalités

Un rapport papier, contenant pour votre dernier modèle :

1. les systèmes de transition (dessin ou texte au format Mec) avec la sémantique des noms des états et des étiquettes des transitions,
2. le système de synchronisation,
3. les hypothèses et choix effectues,
4. les expressions des propriétés vérifiées servant a convaincre de la validité du modèle, les résultats et vos interprétations,
5. les expressions des quatres propriétés de la spécification, les résultats et vos interprétations,
6. pour les propriétés supplémentaires, leur sens, leur expression, les résultats et vos interprétations.

- Date limite de remise des rapports : Jeudi 14 janvier à 9 heures du matin.
- Les binômes sont acceptés.