Université de Sherbrooke, Département d'informatique

IGL510-IGL710: Méthodes formelles en génie logiciel

Modélisation en Alloy du cas des coffres

Spécifiez en Alloy un système de coffres de sécurité. Voici sa description.

Une banque possède une salle des coffres. Pour ouvrir un coffre, il faut deux clés: la clé de la banque, et la clé propre au coffre. Pour ouvrir un coffre, il faut que la clé de la banque et la clé du coffre soient insérées. La porte du coffre comporte un verrou. Le système doit déverrouiller le verrou lorsque les deux clés sont insérées, sinon, le verrou doit être verrouillé. Quand le verrou est déverrouillé, la porte peut s'ouvrir; sinon, la porte ne peut être ouverte. On peut fermer la porte peu importe l'état du verrou.

1. Ajouter un `fact` qui assure que:
   (a) chaque clé est associée à un coffre distinct de ceux des autres clés.
   (b) chaque coffre a une clé
2. Utilisez Alloy pour déterminer si les énoncés suivants sont équivalents. Analysez chaque paire d'énoncés (ie, i) et ii), i) et iii), ii) et iii).
   (a) `all k1,k2 : CleClient | k1 != k2 => k1.coffre != k2.coffre`
   (b) `all c : Coffre | one coffre.c`
   (c) `CleClient.coffre = Coffre`
3. Spécifiez les actions suivantes

```
pred insererCle[s,s' : State, c : Coffre, k : Cle]
pred enleverCle[s,s' : State, c : Coffre, k : Cle]
pred ouvrirPorte[s,s' : State, c : Coffre]
pred fermerPorte[s,s' : State, c : Coffre]
```

4. Spécifiez le prédicat `Init[s:State]` qui retourne vrai ssi toutes les portes sont fermées et verrouillées, et qu'aucune clé n'est insérée.
5. Donnez les `assert` et `pred` nécessaires pour montrer la propriété d'invariance suivante: Le verrou d'une porte est déverrouillé ssi les deux clés (banque et celle propre au coffre) sont insérées dans la porte.
6. Donnez un énoncé `run` qui vérifie que la spécification comprend un modèle avec une trace de longueur 4.
7. Utilisez une trace (module util/ordering[State]) pour écrire des `check` ou des `run` pour vérifier les propriétés suivantes.
   (a) Si le verrou est déverrouillé, alors la clé de la banque est insérée.
   (b) On peut ouvrir la porte d'un coffre à partir de l'état initial en insérant la clé de la banque et la clé du coffre.
   (c) Si on ouvre la porte, alors les deux clés ont été insérées.