

Vérification et validation

Année 2016-2017

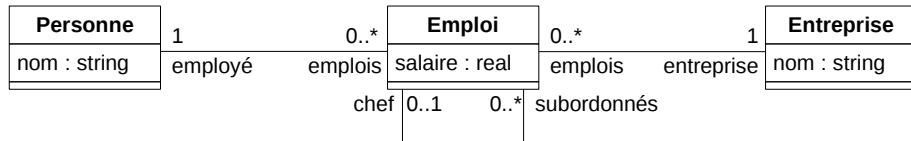
Delphine Longuet, Georges Ouffoué
longuet@lri.fr, ouffoue@lri.fr

TD 2 - Spécification des opérations

22 février 2017

Exercice 1

On considère le diagramme de classes suivant, qui modélise les différents emplois occupés par des personnes dans des entreprises. Un emploi est caractérisé par son salaire et associe de manière unique une personne et une entreprise. Une personne ne peut pas occuper plusieurs emplois dans la même entreprise mais peut par contre travailler dans plusieurs entreprises. Il peut exister une relation de hiérarchie entre les employés d'une même entreprise, modélisée par l'association réflexive sur la classe **Emploi**. Une personne reçoit toujours un salaire strictement inférieur à son supérieur. Pour simplifier, les personnes et les entreprises sont caractérisées de manière unique par leur nom.



On associe à ce diagramme de classes les invariants suivants :

- (a) $\forall p1, p2 \in \text{Personne}, p1 \neq p2 \Rightarrow p1.\text{nom} \neq p2.\text{nom}$
- (b) $\forall p \in \text{Personne}, |p.\text{emplois}| = |p.\text{emplois.entreprise}|$
- (c) $\forall e1, e2 \in \text{Entreprise}, e1 \neq e2 \Rightarrow e1.\text{nom} \neq e2.\text{nom}$
- (d) $\forall e \in \text{Emploi}, e.\text{salaire} > 0$
- (e) $\forall e \in \text{Emploi}, e.\text{chef} \neq \emptyset \Rightarrow e.\text{salaire} < e.\text{chef.salaire}$
- (f) $\forall e \in \text{Emploi}, e.\text{chef} \neq \emptyset \Rightarrow e.\text{entreprise} = e.\text{chef.entreprise}$

On veut spécifier les opérations suivantes :

1. **Emploi :: augmenter(montant : int)** permet d'augmenter le salaire d'un emploi du montant passé en argument. Il faut que les invariants liés à la hiérarchie dans l'entreprise soient toujours vérifiés après l'augmentation.
2. **Emploi :: diriger(emp : Emploi)** permet de devenir le supérieur de l'emploi passé en argument. Il faut que cette personne n'ait pas déjà un supérieur et que la contrainte sur les salaires soit respectée.
3. **Entreprise :: embaucher(nom : string, salaire : int)** permet d'embaucher une personne avec le salaire donné. Il faut que cette personne existe et n'appartienne pas déjà aux employés de l'entreprise. L'emploi doit être créé lors de l'opération.
4. **Personne :: collegues(ent : Entreprise) : P(Personne)** construit l'ensemble des personnes travaillant dans la même entreprise que la personne. Il faut que cette personne ait un emploi dans l'entreprise passée en argument. Une personne ne fait pas partie de l'ensemble de ses collègues.

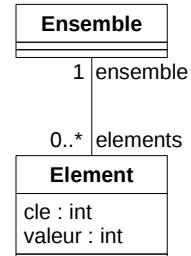
5. `Emploi :: superieurs()` : $\mathcal{P}(\text{Emploi})$ construit l'ensemble des emplois placés hiérarchiquement au-dessus de l'emploi concerné.

Exercice 2

On considère une classe `Ensemble` dont les éléments sont des couples formés d'une clé et d'une valeur. Les clés et les valeurs sont toutes positives strictement et les clés sont deux à deux distinctes. L'opération `chercher` prend un entier en argument, renvoie la valeur correspondant à cette clé si elle existe dans l'ensemble et -1 sinon.

On a écrit une première spécification de l'opération `chercher` :

```
Ensemble :: chercher(clé : int) : int
pre : true
post : (result >= 0 ∧ ∃e ∈ Ensemble, e.clé = clé) ∨ result = -1
```



Cette spécification est-elle correcte ? Est-elle complète ? Quelles implémentations de l'opération `chercher` sont autorisées par cette spécification ? Corriger la spécification en s'assurant que seules les implémentations voulues sont autorisées.

Exercice 3

L'opération `sqrt` calcule la racine carrée entière inférieure de son argument entier. On donne la spécification suivante de cette opération :

```
sqrt(a : int) : int
pre : a > 0
post : result * result = a
```

Cette spécification est-elle correcte ? Est-elle complète ? Quelles implémentations de l'opération `sqrt` sont autorisées par cette spécification ? Corriger la spécification en s'assurant que toutes les implémentations voulues sont autorisées.