

CPS - Notes de TD

Jordi Bertran de Balanda

TD 1

Ex1. Communication évènementielle

Q1. Interfaces de service

Service considéré: pouvoir recevoir un évènement.

```
public interface IntEventReceiverService {  
    public void onIntEvent(IntEvent event);  
}
```

Q2. Interfaces de liaison

```
public interface requireIntEventReceiver {  
    public void bindIntEventReceiver(IntEventReceiverService receiver);  
}
```

```
public interface requireActivator {  
    public void bindActivator(ActivatorService activator);  
}
```

Q3. Composant émetteur

cf. feuille Pas de IntEventSenderService, pas réifié (cf Q2).

Q4. Composant récepteur

cf. feuille (diagramme de composant de IntEventReceiverService).

```

public class Printer implements Component, IntEventReceiverService {
    private BigInteger msg;
    public Printer() {
        this.msg = null;
    }

    public void onIntEvent(IntEvent event){
        if (msg != null)
            throw new ReceptionException();
        else
            msg = event.getValue()
    }

    public void activate() {
        System.out.println(msg?msg:".");
        msg = null;
    }
}

```

Q5. Composition

```

public class Composition {
    public static void main (String[] args) {
        GenConst gen = new GenConst(1);
        Printer printer = new Printer();
        gen.bindIntEventReceiverService(printer);
        // Point (1)
        for (int i = 0; i < 10; i++) {
            gen.activate();
            printer.activate();
        }
    }
}

```

Le programme produit une suite de 10 fois le nombre 1 sur sa sortie standard.
cf. feuille pour le diagramme de composants.

Ex2. Dataflow

Q1. Génération des entiers naturels

cf. Feuille.

Le composant add/mul/div/sub attend d'avoir obtenu 2 évènements.

Q2. Composant composite

But: créer un composant *composite* qui envoie des événements de valeurs successives (1, 2...). Ce composant offre ActivatorService, et requiert in IntEventReceiverService.

```
public class GenInt implements Component, requireIntEventReceiver {
    private GenConst gen;
    private Add plus;
    public GenInt (BigInteger value) {
        gen = new GenConst(value);
        plus = new Add();
        gen.bind(plus);
        plus.bind(plus);
        plus.onIntEvent(new IntEvent(value - 1));
    }

    public void bindIntEventReceiver (IntEventReceiverService rec) {
        plus.bind(rec);
    }

    public void activate () {
        gen.activate();
        plus.activate();
    }
}
```

Diagramme de composants: cf. feuille.

TD 2

Spécifications bancaires

Q1. Compte bancaire.

- **Service:** Compte
- **Observateurs:**
 - *const* nom : [Compte] → String
 - *const* numero : [Compte] → int
 - solde : [Compte] → double
 - *const* limite : [Compte] → double
 - decouvert : [Compte] → double

- * **pre:** decouvert(C) **require** aDecouvert(C)
 - aDecouvert : [Compte] \rightarrow bool
 - retraitPossible : [Compte] * double \rightarrow bool
- **Constructeurs:**
 - init : String * int * double \rightarrow [Compte]
 - * **pre:** init(nom, num, dec) **require** (num > 0) \wedge (dec \geq 0)
 - init : Compte \rightarrow [Compte]
- **Opérateurs:**
 - depot : [Compte] * double \rightarrow [Compte]
 - * **pre:** depot(C, s) **require** s > 0
 - retrait : [Compte] * double \rightarrow [Compte]
 - * **pre:** retrait(C, s) **require** retraitPossible(C, s)
- **Observations:**
 - [invariants]
 - * aDecouvert(C, s) (min)= solde < 0
 - * retraitPossible(C, s) (min)= 0 < s \leq solde(C) + limite(C)
 - * decouvert(C) (min)= - solde(C)
 - * solde(C) \geq - limite(C) # PROPRIÉTÉS
 - * 0 \leq decouvert(C) \leq limite(C) # IMPORTANTES
 - [init]
 - * nom(init(n, num, lim)) = n # Const:
 - * numero(init(n, num, lim)) = num # plus besoin de faire
 - * limite(init(n, num, lim)) = lim # d'observations après init
 - * solde(init(n, num, lim)) = 0
 - * nom(init(C)) = Compte::nom(C)
 - * numero(init(C)) = Compte::numero(C)
 - * limite(init(C)) = Compte::limite(C)
 - * solde(init(C)) = 0
 - [retrait]
 - * limite(retrait(C, s)) = limite(C) # Redondant avec const
 - * solde(retrait(C, s)) = solde(C) - s

Q2. Propriétés

Complet: pour tout état, pour tout observateur accessible, il faut pouvoir donner une valeur.

Activable: dans tous les états, au moins une opération est accessible.

Le service est activable.

Convergence:

- depot: opération divergente
- retrait: opération convergente
- retrait : [Compte] * double → [Compte]
 - **pre**: retrait(C, s) require retraitPossible(C, s)
 - * **converge** solde(C)

Q3. Agence

- **Service:** Agence
- **Observateurs:**
 - *const* nom : [Agence] → String
 - numeros : [Agence] → Set
 - nbComptes : [Agence] → int
 - compteExiste : [Agence] * int → bool
 - compte : [Agence] * int → Compte
 - * **pre** getCompte(A, num) require compteExiste(A, num)
- **Constructeurs:**
 - init : String → Agence
- **Opérateurs:**
 - create : [Agence] * String * int * double → [Agence]
 - * **pre** create(A, nom, num, lim) require not(compteExiste(A, num))
 - virement : [Agence] * int * int * double → [Agence]
 - * **pre** virement(A, src, dst, s) require compteExiste(A, src) ∧ compteExiste(A, dst) ∧ Compte::retraitPossible(compte(A, src), s)
- **Observations:**
 - [invariants]
 - * nbComptes(A) (min)= card(numeros(A)) card(E) le cardinal de l'ensemble E
 - * compteExiste(A, num) (min)= num ∈ numeros(A)
 - [init]
 - * nom(init(n)) = n
 - * numeros(init(nom)) = NONE
 - [create]
 - * numero(create(A, nom, num, lim)) = numeros(A) ∪ {num}
 - [compte]
 - * compte(create(A, nom, num, lim)) = Compte::init(nom, num, lim)

```

    *  $\forall \text{ num2, num2} \neq \text{num} \Rightarrow \text{compte}(\text{create}(\text{A}, \text{nom}, \text{num}, \text{lim}),$ 
       $\text{num2}) = \text{compte}(\text{A}, \text{num2})$ 
  - [virement]
    *  $\text{numerous}(\text{virement}(\text{A}, \text{src}, \text{dst}, \text{s})) = \text{numerous}(\text{A})$ 
    *  $\text{compte}(\text{virement}(\text{A}, \text{src}, \text{dst}, \text{s}), \text{src}) = \text{Compte}::\text{retrait}(\text{compte}(\text{A},$ 
       $\text{src}), \text{s})$ 
    *  $\text{compte}(\text{virement}(\text{A}, \text{src}, \text{dst}, \text{s}), \text{dst}) = \text{Compte}::\text{depot}(\text{compte}(\text{A},$ 
       $\text{dst}), \text{s})$ 
    *  $\forall \text{ num, num} \neq \text{src} \wedge \text{num} \neq \text{dst} : \text{compte}(\text{virement}(\text{A}, \text{src}, \text{dst},$ 
       $\text{s}), \text{num}) = \text{compte}(\text{A}, \text{num})$ 

```

TD3 - Conception par contrats

Idée \rightarrow Spec \rightarrow Contrat \rightarrow Impl

Ex1. Compte bancaire

Interface

```

public interface ICompte {

    ***** Observators *****

    String nom();           // Const
    int numero();           // Const
    double solde();
    double limite();        // Const
    // \pre estDecouvert() == true
    double montantDecouvert();
    bool estDecouvert();
    // \pre s > 0
    bool peutPrelever(double s);

    ***** Operators *****

    // \pre somme > 0
    // \post solde() == solde()@pre + somme
    void depot(double somme);
    // \pre peutPrelever(somme) == true
    // \post somme() == somme()@pre + somme
    void retrait(double somme);

    ***** Initializers *****

```

```

/*****
 * \pre nom != ""
 * \pre num > 0
 * \pre dec >= 0
 * \post nom().equals(n)
 * \post numero() == num
 * \post limite() == dec
 * \post solde() == 0
 *****/
void init(String nom, int num, double dec);
void init(Compte c);

/***** Invariants *****/
/*****
 * \inv montantDecouvert() == -solde()
 * \inv \forall s:double \with s>0 {peutPrelever(s) == (solde()-s)>=limite()}
 *****/

```

Implem

```

public class CompteImpl implements ICompte {
    private String nom;
    ..
    public CompteImpl() { ... }
    public void init() { ... }
    public String nom() { return nom; }
    ..
}

```

Decorateur

```

public abstract class CompteDecorateur implements ICompte {
    private ICompte delegate;
    protected CompteDecorateur(Compte delegate) {
        this.delegate = delegate;
    }
    public String nom() { return delegate.nom(); }
    ..
}

```

Contrat

```
public class CompteContrat extends CompteDecorateur {
    public CompteContrat(Compte delegate) {
        super(delegate);
    }
    public void checkInvariants() {
        // \inv montantDecouvert() == -solde()
        if (estDecouvert() && montantDecouvert() != -solde())
            throw new InvariantError(err);
        // \inv \forall s:double \with s>0 { peutPrelever(s) == (solde()-s)>=limite() }
        double s1 = solde() + limite();
        if (!(peutPrelever(s1) == true))
            throw new InvariantError("...");
        double s2 = s1 / 2;
        if (!(peutPrelever(s2) == true))
            throw new InvariantError("...");
        double s1 = solde() + limite();
        double s3 = s1;
        if (!(peutPrelever(s3) == true))
            throw new InvariantError("...");
    }
    public void retrait(double s) {
        // (1) Préconditions
        // \pre peutPrelever(s)
        if (!(peutPrelever(s) == true))
            throw new PreconditionException("...");
        // (2) Invariants
        checkInvariants();
        // (3) Capture
        String nom_pre = nom();
        int solde_pre = solde();
        // (4) Métier
        super.retrait(s);
        // (5) Invariant
        checkInvariant();
        // (6) Postconditions
        // \post solde() == solde(@pre - s
        if (!(solde() == solde_pre - s))
            throw new PostconditionException("...");
    }
}
```


Links

```
Compte compte = new Compte();
CompteContrat contrat = new CompteContrat();
contrat.init( .. );
compte.init( .. );
```

Ex2. Agence bancaire

```
public interface ...
```

TD 5 - Tests MBT

Service Commandes (non spécifié) suit 2 listes:

- uplist triée en ordre croissant les commandes pour monter
- downlist triée en ordre décroissant les commands pour descendre

Ex1. Couverture des préconditions

11 objectifs de précondition.

1. **init**

1. Test *positif*:

- *Conditions initiales*: aucune
- *Opération*: $L_{11} = \text{init}(2, 5)$
- *Oracle*: **pas** d'exception levée

2. Test *négatif*:

- *Conditions initiales*: aucune
- *Opération*: $L_{12} = \text{init}(-2, 5)$
- *Oracle*: Exception levée

2. **beginMoveUp**: non atteignable. Le service commande n'est pas spécifié.

3. **stepMoveUp**: non atteignable.

4. **endMoveUp**: non atteignable.

5. **beginMoveDown**: non atteignable.

6. **stepMoveDown**: non atteignable.

7. **endMoveDown**: non atteignable.

8. **openDoor**

1. Test *positif*:

- *Conditions initiales*: $L_{01} = \text{doorAck}(\text{closeDoor}(\text{init}(2, 5)))$
 - *Opération*: $L_{81} = \text{openDoor}(L_0)$
 - *Oracle*: Pas d'exception levée
2. Test *négatif*:
 - *Conditions initiales*: $L_{02} = \text{init}(2, 5)$
 - *Opération*: $L_{82} = \text{openDoor}(L)$
 - *Oracle*: Exception levée
 3. Test *négatif*: Impossible d'atteindre un statut différent de IDLE sans avoir la spécification de Commandes
 4. Test *négatif*: Idem que 8.3
9. **closeDoor**
1. Test *positif*:
 - *Conditions initiales*: $L_{01} = \text{init}(2, 5)$
 - *Opération*: $L_{91} = \text{openDoor}(L_{01})$
 - *Oracle*: Pas d'exception levée
 2. Test *négatif*:
 - *Conditions initiales*: $L_{02} = \text{doorAck}(\text{closeDoor}(\text{init}(2, 5)))$
 - *Opération*: $L_{92} = \text{closeDoor}(L)$
 - *Oracle*: Exception levée
 3. Test *négatif*: Impossible d'atteindre un statut différent de IDLE sans avoir la spécification de Commandes
 4. Test *négatif*: Idem que 9.3
10. **doorAck**
1. Test *positif*:
 - *Conditions initiales*: $L_{01} = \text{closeDoor}(\text{init}(2, 5))$
 - *Opération*: $L_{101} = \text{doorAck}(L_{01})$
 - *Oracle*: Pas d'exception levée
 2. Test *positif*:
 - *Conditions initiales*: $L_{02} = \text{openDoor}(\text{doorAck}(\text{closeDoor}(\text{init}(2, 5))))$
 - *Opération*: $L_{101} = \text{doorAck}(L_{02})$
 - *Oracle*: Pas d'exception levée
 3. Test *négatif*:
 - *Conditions initiales*: $L_{03} = \text{init}(2, 5)$
 - *Opération*: $L_{101} = \text{doorAck}(L_{03})$
 - *Oracle*: Exception levée
11. **selectLevel**

Couverture des tests de préconditions, en l'absence de la spécification de Commandes: 27,2%.

Ex2. Couverture en termes d'automates

Q1. Couverture des transitions

1. **init**

- *Conditions initiales*: aucune
- *Opération*: $L_{11} = \text{init}(2, 5)$
- *Oracle (Post)*: $\text{minLevel}(L_{11}) = 2, \text{maxLevel}(L_{11}) = 5 \dots$
- *Oracle (Inv)*: $\text{minLevel}(L_{11}) \leq \text{level}(L_{11}) \leq \text{maxLevel}(L_{11})$

2. **beginMoveUp**: non atteignable. Le service commande n'est pas spécifié.

3. **stepMoveUp**: non atteignable.

4. **endMoveUp**: non atteignable.

5. **beginMoveDown**: non atteignable.

6. **stepMoveDown**: non atteignable.

7. **endMoveDown**: non atteignable.

8. **openDoor**

- *Conditions initiales*: $L_0 = \text{doorAck}(\text{closeDoor}(\text{init}(2, 5)))$
- *Opération*: $L_8 = \text{openDoor}(L_0)$
- *Oracle (Post)*: $\text{doorStatus}(L_8) = \text{OPENING}$
- *Oracle (Inv)*: $\text{minLevel}(L_8) \leq \text{level}(L_8) \leq \text{maxLevel}(L_8) \dots$

Couverture de transitions: 18%.

Q2. Couverture des états remarquables

1. **STANDBY_UP**

- *Conditions initiales*: aucune
- *Opération*: $L_{331} = \text{selectLevel}(\text{doorAck}(\text{closeDoor}(\text{init}(2, 5))), 3))$
- *Oracle(Inv)*: $\text{minLevel}(L_{331}) \leq \text{level}(L_{331}) \leq \text{maxLevel}(L_{331}) \dots$

Q3. Couverture de paires de transitions

1. **doorAck; openDoor**

- *Conditions initiales*: $L_{41} = \text{closeDoor}(\text{init}(2, 5))$
- *Opération*: $L_{42} = \text{openDoor}(\text{doorAck}(L_{41}))$
- *Oracle(P) 1*: ..
- *Oracle(I) 1*: ..
- *Oracle(P) 2*: ..
- *Oracle(I) 2*: ..

Q4. Couverture des use case

Raconter des histoires (cf. IL)

Ex3. Couverture des données

Gestion des plages de valeurs.

1. **selectLevel:** tester `selectLevel(L, m)`, avec par ex. `init(0, 5)`
 - Un cas dans les bornes - `selectLevel(L, 2)`
 - Trois cas aux bornes - `selectLevel(0)`, `selectLevel(5)`, `selectLevel(2)`
 - Deux cas hors bornes - `selectLevel(-1)`, `selectLevel(6)`