

***Sur quelques approches de la
sémantique en Object-Z des
diagrammes dynamiques en
UML***

COUZINIER Marjorie

Université Paul Sabatier, TOULOUSE III

Plan

- Motivation
- Object-Z
- Formalismes de transformation: Araújo & Moreira, OZRose (Miao, Liu, Li) et TCOZ (Mahony et Dong)
- Conclusion
- Perspectives

Motivation

- UML: modèle standard des langages OO
- Sémantique en langage naturel

But

Vérification inter et intra diagrammes :
ambiguïté, inconsistance et erreurs de formalisation

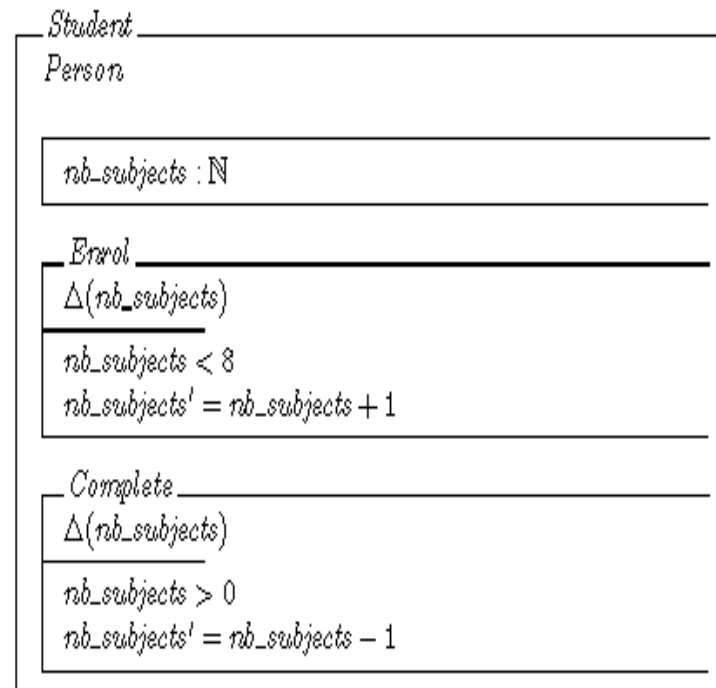
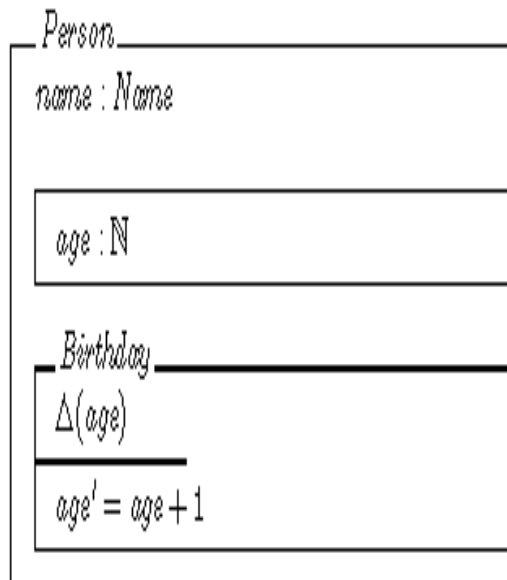
Conséquence

Sémantique formelle pour les diagrammes dynamiques en UML

Object-Z (Smith)

- Extension vers les objets du langage Z
- Langage de spécification formel
- Concepts mathématiques: logique du premier ordre et théorie des ensembles
- **Simple et puissants**
- Logique temporelle linéaire: propriétés d'équité, de vivacité et de sécurité

Exemple: classe en Object-Z



Diagrammes dynamiques: critères

Diagrammes de séquence et collaboration

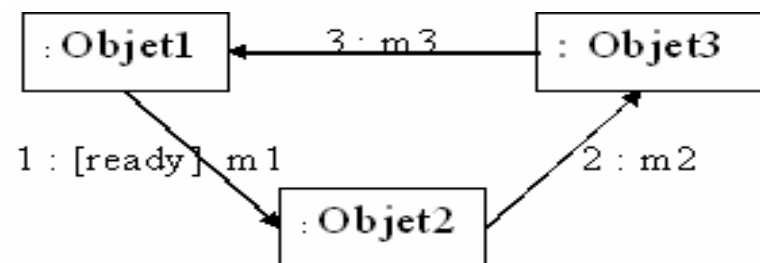
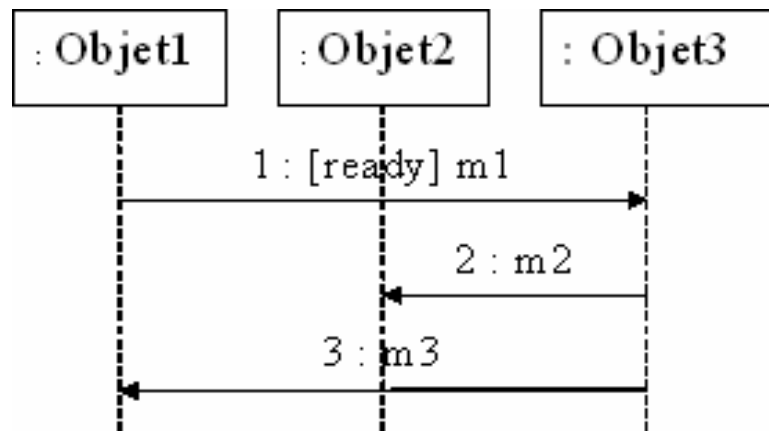
- Messages: types, gardes...
- Envois: parallèles, cycles, ordre de séquençement...

Diagramme états/transitions

- États: entrées, sorties, composites, inaccessibles...
- Transitions: temporisées, événements, gardes, actions...

Araújo et Moreira

Diagrammes séquence et collaboration



Exemple

```

o1 : Objet1
o2 : Objet2
o3 : Objet3
ready : Boolean
    
```

Invt

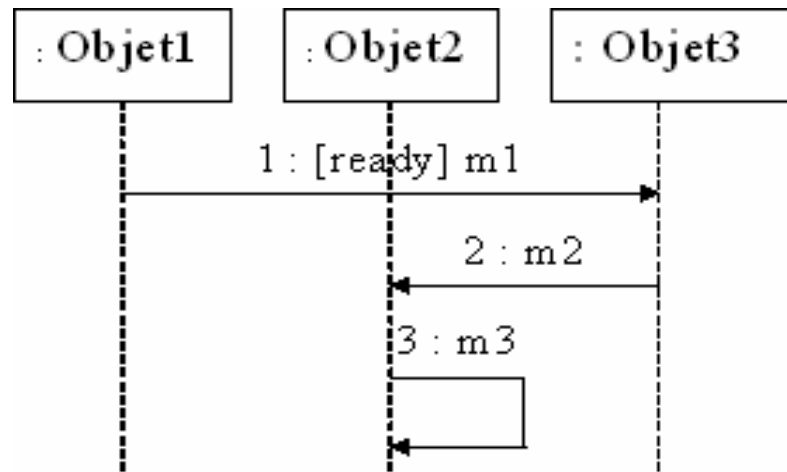
```

o1.invit ∧ o2.invit ∧ o3.invit
    
```

```

□(op = ready ∧ o3.m1 →
  ◇(op = o2.m2 →
    ◇(op = o1.m3)))
    
```

OZRose: Diagramme de séquence



SeqExemple

m1 : m11

m2 : m22

m3 : m33

m1.order < m2.order

m2.order < m3.order

m11

sender : Objet1

receiver : Objet3

ready? : Boolean

msgtype : MESSAGE TYPE

msgtype = Simple

ready? => receiver.m1()

order = 1

m22

sender : Objet3

receiver : Objet2

msgtype : MESSAGE TYPE

msgtype = Simple

receiver.m2()

order = 2

m33

sender : Objet2

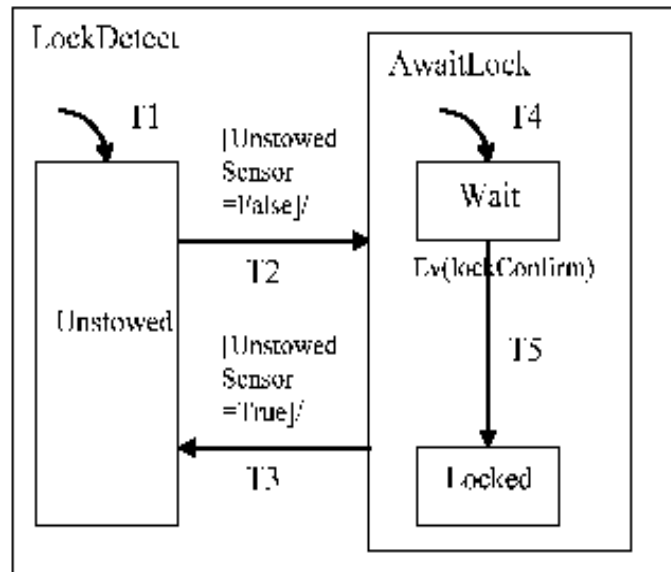
msgtype : MESSAGE TYPE

msgtype = Simple

sender.m3()

order = 3

OZRose: Diagramme E-T

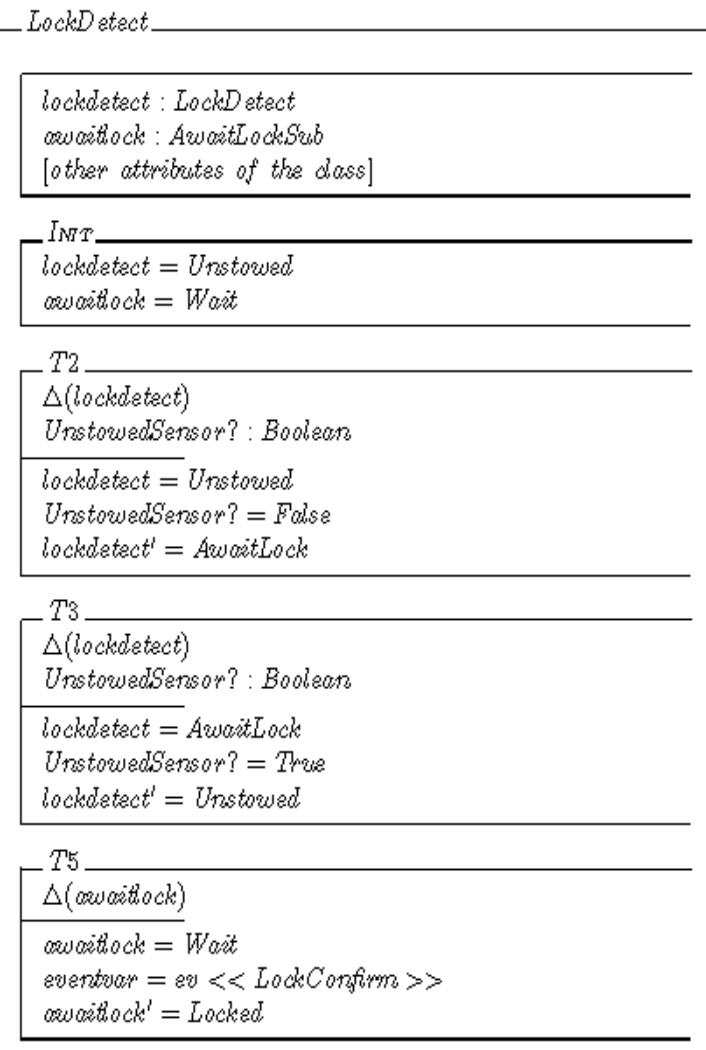


LockDetect ::= Unstowed | AwaitLock

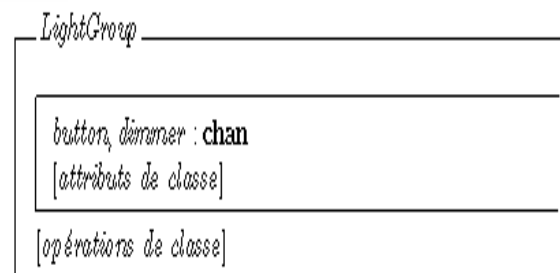
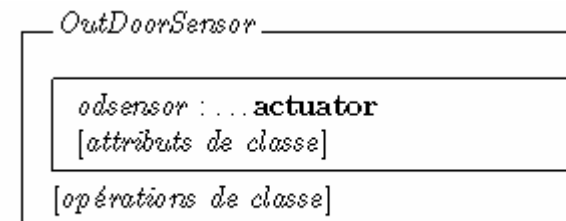
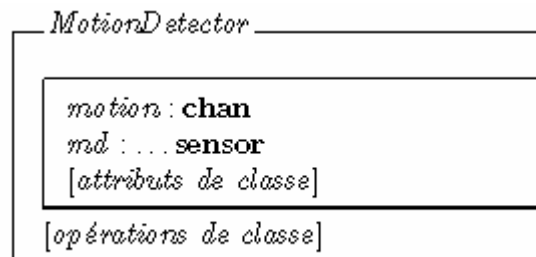
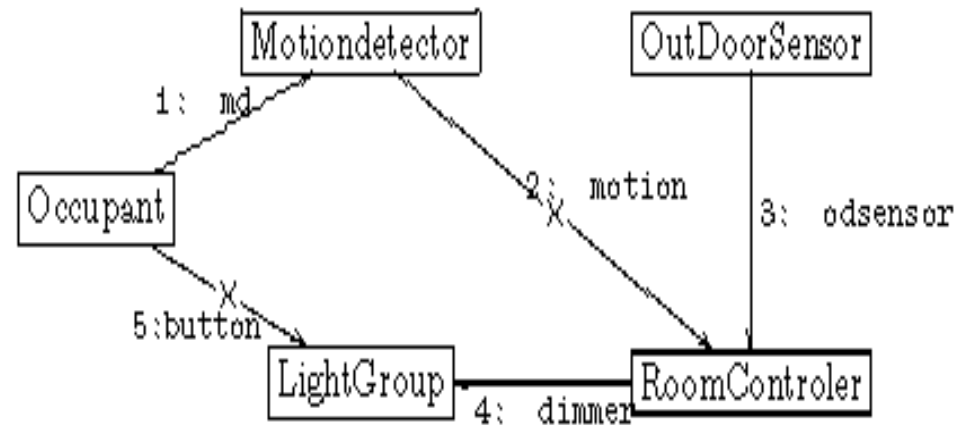
AwaitLockSub ::= Wait | Locked

EVPARAMETER ::= LockConfirm

EVENTTYPE ::= ev<<EVPARAMETER>>

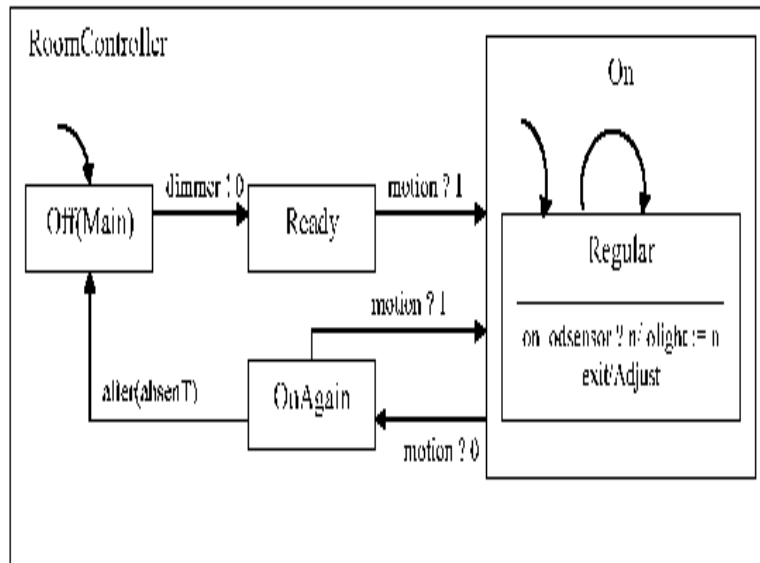


TCOZ: Diagramme de collaboration



TCOZ: Diagramme E-T

satisfy : Percent ↔ Illumination



RoomController

dimmer, motion : chan
odsensor : Illumination sensor
adsentT : T
olight : Illumination

Adjust

dim! : Percent on dimmer
dim! satisfy olight

Ready ≅ motion?1 → On

Regular ≅ μ R ♦ [n : Illumination] ♦ odsensor?n → olight := n; Adjust; R

On ≅ Regular ∇ motion?0 → OnAgain

OnAgain ≅ (motion?1 → On) ▷ { AbsentT } Off

Off ≅ dimmer!0 → Ready

MAIN ≅ Off

Critères de comparaison

- Diagrammes de séquence et collaboration: caractéristiques des messages
- Diagramme états/transitions: caractéristiques des états et des transitions
- Cohérence inter diagrammes: types des diagrammes traités
- Vérification inter et intra diagrammes: présence d'un environnement permettant d'effectuer des preuves

Tableau

		Aratijo Moreira	OZRose	TCOZ
Type des diagrammes		Collaboration Séquence	Séquence État-Transition	Collaboration État-Transition
Messages	Types	synchrone	synchrone asynchrone réflexif	synchrone asynchrone réflexif
	Parallèles	non	non précisé	non précisé
	Cycles	non	non précisé	non précisé
	Ordre	total	total	non précisé
	Gardes	oui	oui	non précisé
États	Composites	-	oui	oui
	Entrée	-	oui	oui
	Sortie	-	non	non
	Inaccessibles	-	non	non
Transitions	Événement	-	oui	oui
	Garde	-	oui	oui
	Action	-	oui	oui
	Temps	-	non	oui
Vérification inter-diagrammes		oui	non	non
Environnement de développement		non	non	oui

Conclusion

- Problèmes ouverts: traitement des messages, états inaccessibles...
- Séquencement supposé totalement ordonné
- Object-Z ne possède pas d'environnement pour la preuve
- TCOZ ne fournit pas un outil de preuves automatiques

Perspectives: TLA+ de Lamport

- Formalisme de plus bas niveau : exprimer des propriétés plus fines sur les messages
- Expression des propriétés temporelles
- Assistance pour effectuer des preuves automatiques (TLC)