

Formale objektorientierte Software-Entwicklung

Prof. Dr. Rolf Hennicker

22.04.2004

Operationsspezifikationen, Invarianten und Komponentenspezifikationen

Ziele

- Klassensignaturen kennen
- Operationsspezifikationen, die in der Form von Vor- und Nachbedingungen gegeben sind, schreiben können
- Das Vertragskonzept hinter Operationsspezifikationen verstehen
- Invarianten für Klassen und Komponenten formulieren können
- Komponentenspezifikationen erstellen können
- Implizite Invarianten aus Klassendiagrammen herleiten können
- Die formale Repräsentation einer Komponentenspezifikation kennen

3.1 Klassensignaturen

Definition (Klassensignatur):

Sei Δ ein Klassendiagramm. Die Klassensignatur von Δ ist definiert durch

$\Sigma_{\Delta} = (S_{\Delta}, \leq, OP_{\Delta}, Visibility)$ wobei

1. $S_{\Delta} = S_{\Delta}^{OCL} \cup \{Void\}$
2. \leq ist die partielle Ordnung auf S_{Δ}^{OCL} (vgl. Kapitel 2)
3. $OP_{\Delta} = OP_{\Delta}^{OCL} \cup M_{\Delta} \cup Q_{\Delta} \cup Con_{\Delta}$ wobei

M_{Δ} enthält

- für jede Methode $m(x_1 : T_1, \dots, x_n : T_n)$ einer Klasse C
 $m : C \times T_1 \times \dots \times T_n \rightarrow Void$
- für jede Methode $m(x_1 : T_1, \dots, x_n : T_n) : T$ einer Klasse C
 $m : C \times T_1 \times \dots \times T_n \rightarrow T$

Q_{Δ} enthält

- für jede Query $q(x_1 : T_1, \dots, x_n : T_n) : T \{query\}$ einer Klasse C
 $q : C \times T_1 \times \dots \times T_n \rightarrow T$

Con_{Δ} enthält

- für jeden Konstruktor $C(x_1 : T_1, \dots, x_n : T_n)$ einer Klasse C
 $C : T_1 \times \dots \times T_n \rightarrow C$

4. *Visibility* : $A_\Delta \cup M_\Delta \cup Q_\Delta \cup Con_\Delta \rightarrow \{+, \sim, \#, -\}$ ist eine partielle Funktion wobei

- + steht für komponenten-öffentliche Sichtbarkeit
- \sim steht für komponenten-private Sichtbarkeit
- # steht für geschützte Sichtbarkeit ("protected")
- steht für klassen-private Sichtbarkeit

Annahmen

- Für dieselbe Klasse C gibt es keine zwei Operationen mit demselben Namen und derselben Anzahl von Parametern.
- Beim Überschreiben (Redefinieren) von Operationen in Subklassen wird die Sichtbarkeit erhalten.

Notation

$Opns_\Delta =_{def} M_\Delta \cup Q_\Delta \cup Con_\Delta$ bezeichnet die Operationen aus Δ

Beispiel (Punkte und Formen):

$$\begin{aligned}
 M_{\Delta} = & \{ \text{setColour} : CPoint \times Real \rightarrow Void \\
 & \text{setOwner} : Point \times Shape \rightarrow Void, \\
 & \text{unSetOwner} : Point \rightarrow Void, \\
 & \text{move} : Point \times Real \times Real \rightarrow Void, \\
 & \text{addPoint} : Shape \times Point \rightarrow Void, \\
 & \text{removePoint} : Shape \times Point \rightarrow Void, \\
 & \text{move} : Shape \times Real \times Real \rightarrow Void, \\
 & \text{createPoint} : System \times Real \times Real \rightarrow Point, \dots \}
 \end{aligned}$$

$$Q_{\Delta} = \{ \text{belongsTo} : Shape \times Point \rightarrow Boolean \}$$

$$\begin{aligned}
 Con_{\Delta} = & \{ CPoint : \rightarrow CPoint \\
 & CPoint : Real \times Real \times Real \rightarrow CPoint, \\
 & Point : \rightarrow Point, \\
 & Point : Real \times Real \rightarrow Point, \\
 & Shape : \rightarrow Shape, \\
 & System : \rightarrow System \}
 \end{aligned}$$

$Visibility(op) = +$ für alle Operationen op der Klasse System

$Visibility(op) = \sim$ für alle übrigen Operationen

$Visibility(a) = -$ für alle Attribute und Rollennamen

3.2 Operationsspezifikationen

Sei Δ ein Klassendiagramm.

- Für jede Operation $op \in Ops_{\Delta}$ kann eine Operationsspezifikation angegeben werden, welche das mögliche Verhalten der Operation einschränkt.
- Eine Operationsspezifikation ist in der Form von Vor- und Nachbedingungen gegeben:
 - Die Vorbedingung muss wahr sein, wenn die Operation aufgerufen wird.
 - Die Nachbedingung muss wahr sein, wenn die Operation beendet ist (i.e. nach Ausführung der Operation).

Beispiel (Punkte und Formen):

```
context System::addPointToShape(p:Point, s:Shape)
  pre: pointSet -> includes(p) and
      figures -> includes(s) and
      p.owner = null
  post: s.points = s.points@pre -> including(p) and
       p.owner = s
```

```
context System::createPoint(x:Real, y:Real):Point
  post: result.oclIsNew() and
       pointSet = pointSet@pre -> including(result)
```

```
context Point::move(mx:Real, my:Real)
  post: xx = xx@pre + mx and
       yy = yy@pre + my
```

```
context Shape::belongsTo(p:Point):Boolean
  post: result = points -> includes(p)
```

```
context CPoint::CPoint(x:Real, y:Real, c:Real)
  post: xx = x and yy = y and colour = c
```

Allgemeine Form von Operationsspezifikationen

- Für Methoden $(m : C \times T_1 \times \dots \times T_n \rightarrow Void) \in M_\Delta$ ohne Rückgabewert:

context $C :: m(x_1 : T_1, \dots, x_n : T_n)$

pre : P

post : Q

so dass

- $P \in EXP_{Boolean}^{OCL}$, $Q \in EEXP_{Boolean}^{OCL}$
- $FV(P) \subseteq \{self, x_1, \dots, x_n\}$
- $FV(Q) \subseteq \{self, x_1, \dots, x_n\}$

- Für Methoden $(m : C \times T_1 \times \dots \times T_n \rightarrow T) \in M_\Delta$ mit Rückgabewert:

context $C :: m(x_1 : T_1, \dots, x_n : T_n) : T$

pre : P

post : Q

so dass

- $P \in EXP_{Boolean}^{OCL}$, $Q \in EEXP_{Boolean}^{OCL}$
 - $FV(P) \subseteq \{self, x_1, \dots, x_n\}$
 - $FV(Q) \subseteq \{self, x_1, \dots, x_n, result\}$
- Für Queries $(q : C \times T_1 \times \dots \times T_n \rightarrow T) \in Q_\Delta$ haben Operationsspezifikationen dieselbe Form wie für Methoden mit Rückgabewert.

- Für Konstruktoren $(C : T_1 \times \dots \times T_n \rightarrow C) \in \text{Con}_\Delta$:

context $C :: C(x_1 : T_1, \dots, x_n : T_n)$

pre : P

post : Q

so dass

- $P \in \text{EXP}_{\text{Boolean}}^{\text{OCL}}, Q \in \text{EEXP}_{\text{Boolean}}^{\text{OCL}}$
- $FV(P) \subseteq \{x_1, \dots, x_n\}$
- $FV(Q) \subseteq \{\text{self}, x_1, \dots, x_n\}$

Anmerkung:

Vor- und Nachbedingungen kann ein benutzerdefinierter Name gegeben werden:

context $C :: \text{op}(x_1 : T_1, \dots, x_n : T_n) : T$

pre $\text{prename} : P$

post $\text{postname} : Q$

Operationsspezifikationen als Verträge

Eine Operationsspezifikation kann als ein Vertrag zwischen

- einem Kunden, der die Operation benutzt, und
- einem Programmierer, der die Operation implementiert

betrachtet werden.

Beide einigen sich, dass sie folgende Verpflichtungen erfüllen:

Verpflichtung des Kunden:

Der Kunde ruft die Operation nur auf, wenn die Vorbedingung erfüllt ist.

Verpflichtung des Programmierers:

Unter der Voraussetzung, dass die Operation in einem Zustand aufgerufen wird, in dem die Vorbedingung erfüllt ist, sichert der Programmierer zu:

- Die Operation terminiert fehlerfrei (d.h. ohne einen Laufzeitfehler zu verursachen).
- Nach Ausführung der Operation gilt die Nachbedingung.

Beachte:

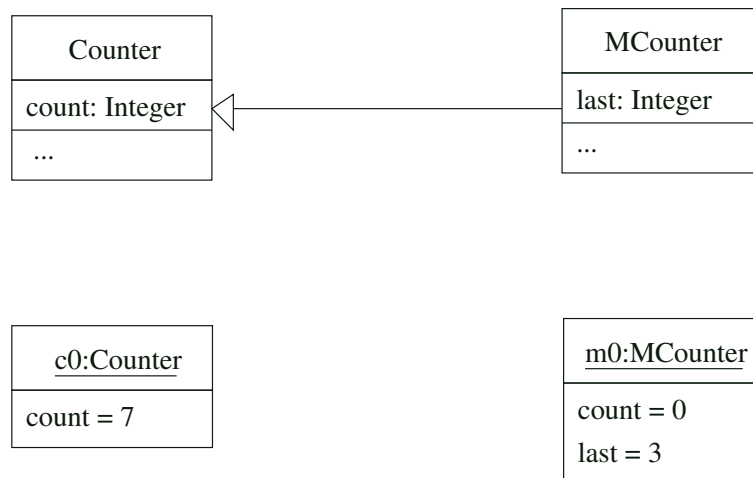
1. Der Vertrag sagt nichts über Situationen aus, in denen die Vorbedingung nicht erfüllt ist.
2. Falls die Operation eine Query ist, dann sichert der Programmierer zusätzlich zu, dass sich der Zustand des Systems während der Ausführung der Operation nicht ändert.
3. Falls die Operation ein Konstruktor ist, dann sichert der Programmierer zusätzlich zu, dass nach Ausführung des Konstruktors ein neues Objekt erzeugt worden ist.

3.3 Klassen- und Komponenteninvarianten

Sei Δ ein Klassendiagramm.

- Für jede Klasse in Δ kann eine Klasseninvariante angegeben werden.
- Eine Klasseninvariante ist ein OCL-Ausdruck vom Typ Boolean, der die möglichen Zustände, unter denen Objekte der betreffenden Klasse von anderen Objekten aus gesehen werden können, einschränkt.

Beispiel (Zähler):



```
(InvCounter) context Counter
inv : count >= 0
```

```
(InvMCounter) context MCounter
inv : last >= 0
```

Ein Zustand, in dem die Klasseninvariante erfüllt ist.

Allgemeine Form von Klasseninvarianten

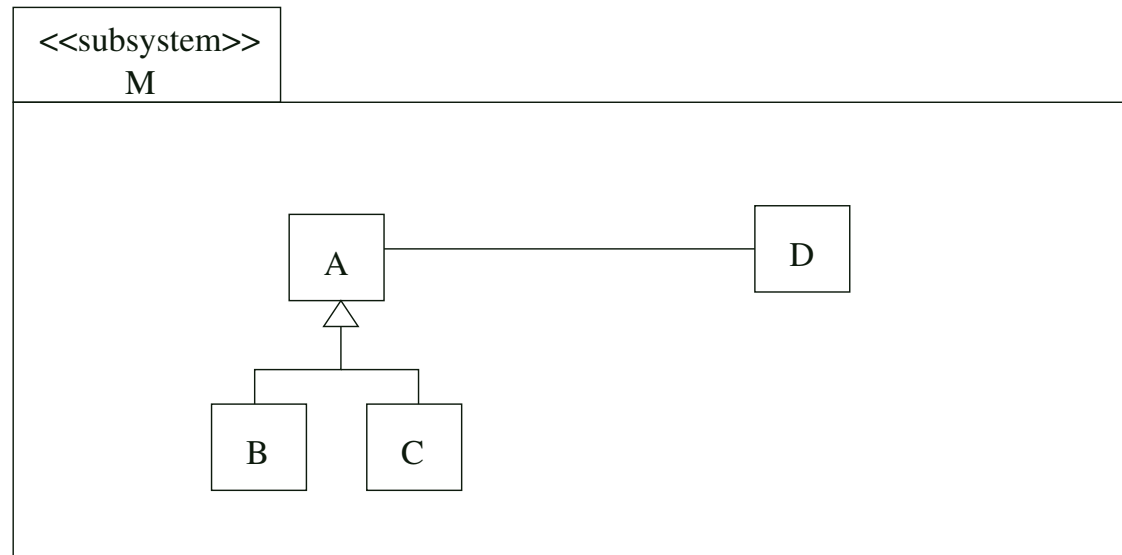
Eine Invariante für eine Klasse C in Δ wird spezifiziert durch

context C oder **context** C
inv : Inv durch **inv** $invname$: Inv

wobei $Inv \in EXP_{Boolean}^{OCL}$ mit $FV(Inv) \subseteq \{self\}$.

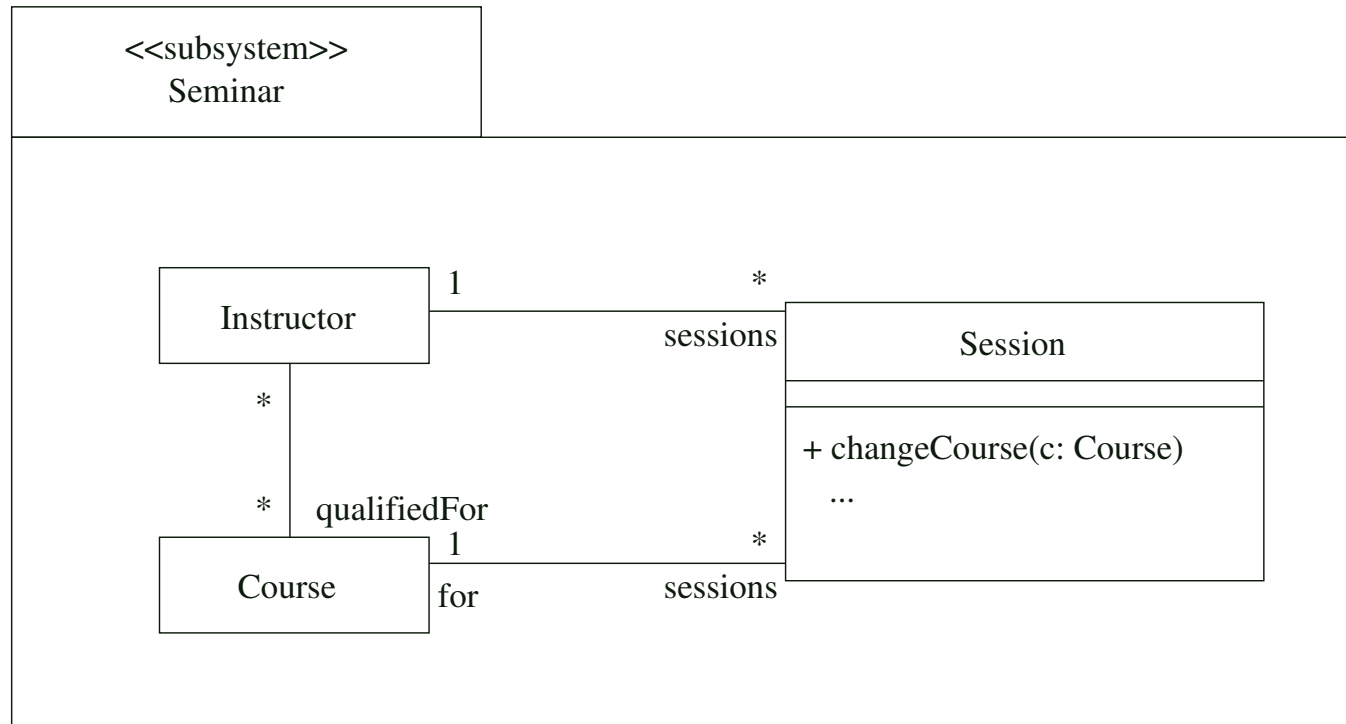
Komponenteninvarianten

Eine Komponente ist ein Subsystem, das ein Klassendiagramm enthält.



- Für jede Komponente M mit Klassendiagramm Δ kann eine Komponenteninvariante angegeben werden.
- Eine Komponenteninvariante ist ein OCL-Ausdruck vom Typ Boolean, der die möglichen Objektkonfigurationen einschränkt, die von außerhalb der Komponente gesehen werden können.

Beispiel (Seminar):

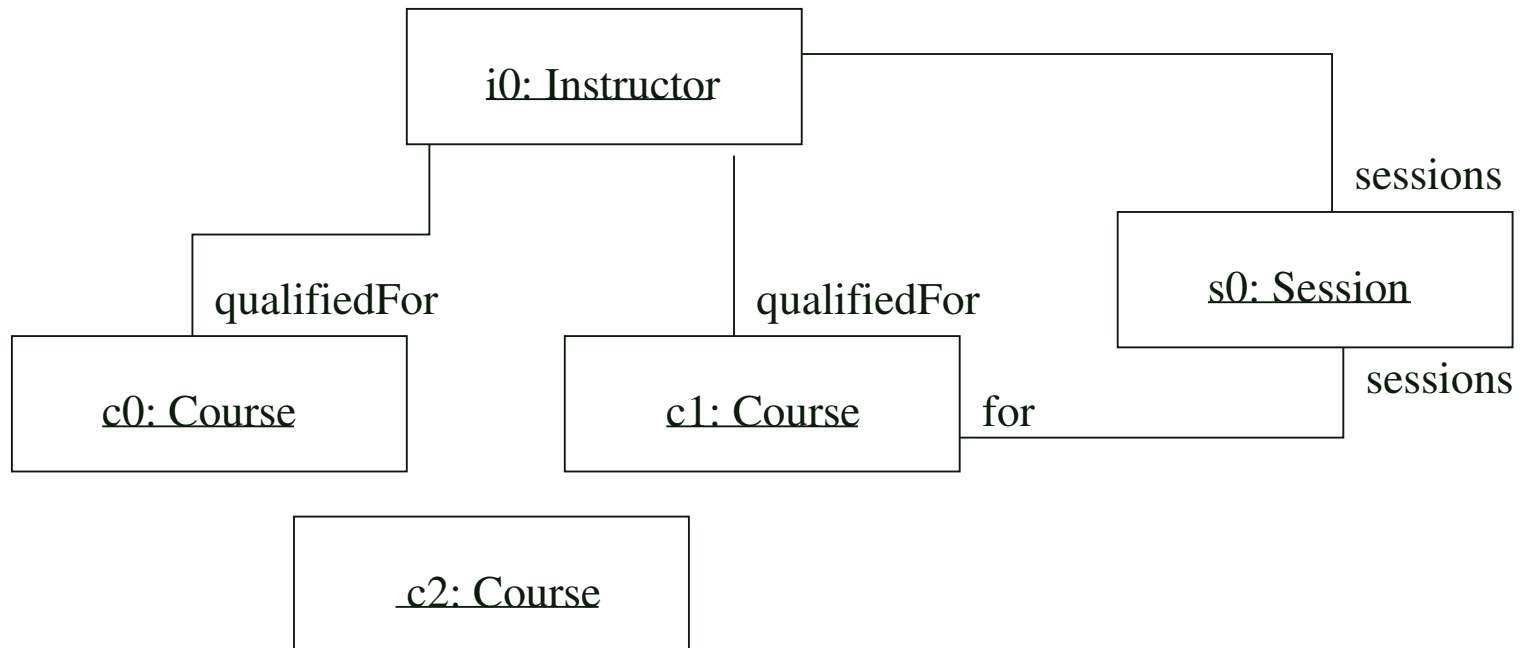


```

(InvSeminar)    context Seminar
                 inv : Instructor.allInstances()->forall(i |
                   i.qualifiedFor->
                     includesAll(i.sessions.for))
  
```

Beispiel (Seminar):

Ein Zustand, in dem die Komponenteninvariante erfüllt ist:



Allgemeine Form von Komponenteninvarianten

Eine Komponenteninvariante für eine Komponente M mit Klassendiagramm Δ wird spezifiziert durch

context M oder **context** M
inv : Inv durch **inv** $invname$: Inv

wobei $Inv \in EXP_{Boolean}^{OCL}$ mit $FV(Inv) = \emptyset$.

3.4 Komponentenspezifikationen

Eine Komponentenspezifikation

$$CompSpec = (\langle M, \Delta \rangle, OpSpecs, Invs^e)$$

besteht aus

- einer Komponente M mit Klassendiagramm Δ
so dass für jedes $op \in Opns_{\Delta}$ gilt $Visibility(op) \in \{+, \sim, -\}$,
- einer Menge $OpSpecs$ von Operationsspezifikationen
für die Operationen aus $Opns_{\Delta}$,
- einer Menge $Invs^e = ClassInvs^e \cup CompInvs^e$ von (expliziten)
Klasseninvarianten und (expliziten) Komponenteninvarianten.

Annahme:

$OpSpecs$ enthält für jede Operation $op \in Opns_{\Delta}$ genau eine Operationsspezifikation.
(Default: context $C :: op(x_1 : T_1, \dots, x_n : T_n)$ pre: true post: true)

Komposition von Operationsspezifikationen

Gegeben seien zwei Operationsspezifikationen für dieselbe Operation:

(*Spec1*) **context** $C :: op(x_1 : T_1, \dots, x_n : T_n) : T$
 pre : P_1
 post : Q_1

(*Spec2*) **context** $C :: op(x_1 : T_1, \dots, x_n : T_n) : T$
 pre : P_2
 post : Q_2

1. Join-Operator

$Join(Spec1, Spec2)$ ist definiert durch

context $C :: op(x_1 : T_1, \dots, x_n : T_n) : T$
pre : P_1 and P_2
post : Q_1 and Q_2

Beispiel (Join)

Counter1
count: Integer last: Ingeger
dec() ...

(Spec1)

```
context Counter1::dec()
  pre: count > 0
  post: count = count@pre - 1
```

(Spec2)

```
context Counter1::dec()
  pre: true
  post: last = count@pre
```

Join(Spec1, Spec2)

```
context Counter1::dec()
  pre: count > 0
  post: count = count@pre - 1 and
        last = count@pre
```

2. Combine-Operator

$Combine(Spec1, Spec2)$ ist definiert durch

context $C :: op(x_1 : T_1, \dots, x_n : T_n) : T$
pre : P_1 or P_2
post : $(P_1@pre$ implies $Q_1)$ and
 $(P_2@pre$ implies $Q_2)$

wobei $P_i@pre$ (für $i = 1, 2$) den OCL-Ausdruck bezeichnet, der aus P_i entsteht, wenn man

- alle Vorkommen von Symbolen a mit $(_ . a) \in A_\Delta$ ersetzt durch $a@pre$ und
- alle Vorkommen von Symbolen $D.allInstances()$ ersetzt durch $D.allInstances@pre()$.

Beispiel (Combine)

Counter2
count: Integer
dec() ...

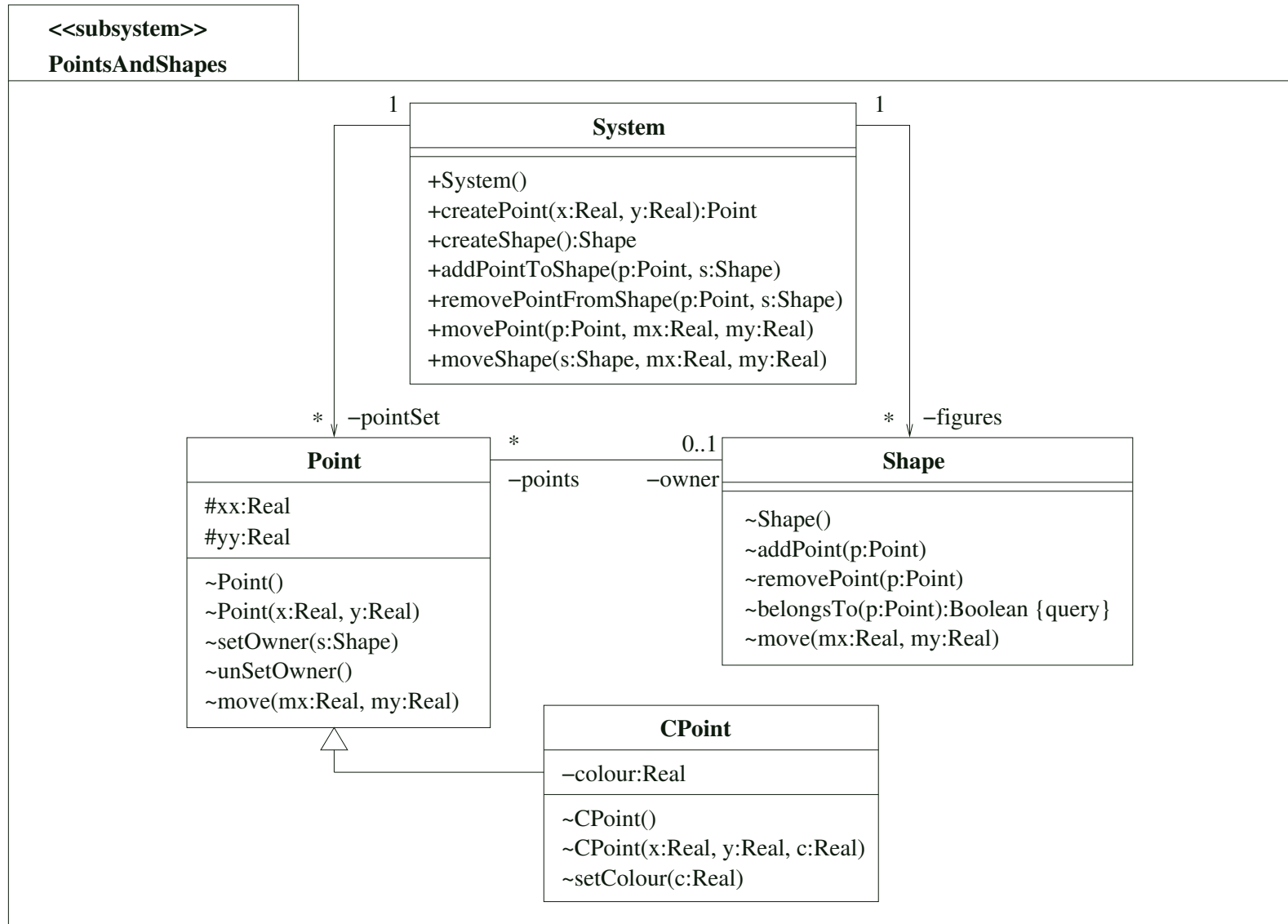
```
(Spec1)      context Counter2::dec()
              pre: count > 0
              post: count = count@pre - 1
```

```
(Spec2)      context Counter2::dec()
              pre: count = 0
              post: count = 0
```

```
Combine(Spec1, Spec2)
```

```
context Counter2::dec()
pre: count >= 0
post: (count@pre > 0 implies count = count@pre - 1) and
      (count@pre = 0 implies count = 0)
```

Komponentenspezifikation für Punkte und Formen



- Als Operationsspezifikationen werden die in Abschnitt 3.2 angegebenen Vor- und Nachbedingungen verwendet, ergänzt um geeignete Spezifikationen für die restlichen Operationen.
- Es werden keine expliziten Klasseninvarianten verwendet.
- Es wird die folgende explizite Komponenteninvariante verwendet, die verlangt, dass assoziierte Punkte und Formen zum selben System gehören:

```
context PointsAndShapes
  inv  invSameSystem:
    System.allInstances() -> forall(sys |
      sys.pointSet -> forall(p |
        p.owner <> null implies
          sys.figures -> includes(p.owner)) and
      sys.figures -> forall(s |
        s.points -> forall(p |
          sys.pointSet -> includes(p))))
```

3.5 Formale Repräsentation von Komponentenspezifikationen

Motivation

- Ein Klassendiagramm Δ drückt Bedingungen für Assoziationen durch Multiplizitäten und Bidirektionalitäts-Anforderungen aus.
- Solche Bedingungen führen zu "impliziten" Klassen- und Komponenteninvarianten, die berücksichtigt werden müssen, wenn man eine präzise Semantik von Komponentenspezifikationen angeben will.

Definition:

Sei $CompSpec = (\langle M, \Delta \rangle, OpSpecs, Invs^e)$ eine Komponentenspezifikation.
Die formale Repräsentation von $CompSpec$ ist gegeben durch

$$FRep(CompSpec) = (\langle M, \Sigma_{\Delta} \rangle, OpSpecs, Invs)$$

wobei

- Σ_{Δ} die Klassensignatur von Δ ist und
- $Invs = Invs^e \cup Invs^i$ die Menge aller expliziten und impliziten Invarianten ist.

Im Folgenden wird beschrieben, wie implizite Klassen- und Komponenteninvarianten hergeleitet werden.

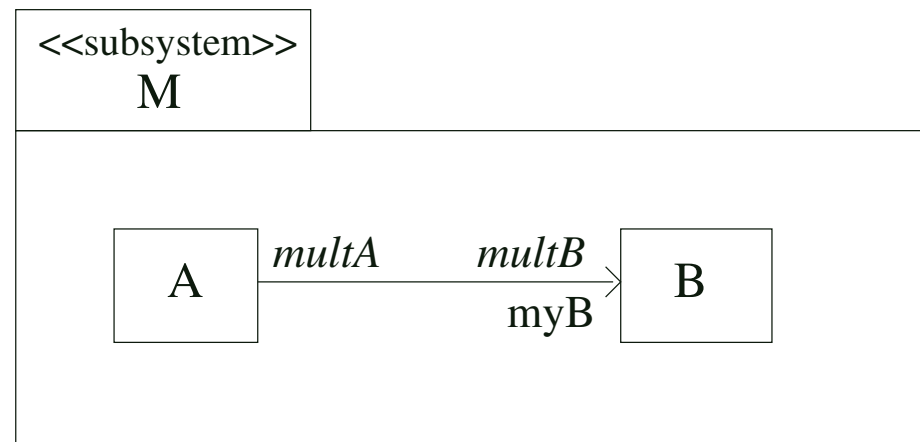
Anmerkung:

$\langle M, \Delta \rangle$ enthält dieselbe Information wie $\langle M, \Sigma_{\Delta} \rangle$ zusammen mit $Invs^i$.

Implizite Klassen- und Komponenteninvarianten

Unidirektionale und bidirektionale Assoziationen induzieren Bedingungen für Objektzustände und Objektkonfigurationen, die durch implizite Klassen- und Komponenteninvarianten formalisiert werden.

Unidirektionale Assoziationen



1. Klasseninvarianten, die durch navigierbare Assoziationsenden induziert werden

Fall 1.1: $multB = 0..1$

ist bereits vollständig formalisiert durch das Symbol $..myB : A \rightarrow B$

Fall 1.2: $multB = 1$

induziert die Klasseninvariante

context A

inv : $myB \langle \rangle null$

Fall 1.3: $multB = *$

ist bereits vollständig formalisiert durch das Symbol $..myB : A \rightarrow Set(B)$

Fall 1.4: $multB = 1..*$

induziert die Klasseninvariante

context A

inv : $myB \rightarrow exists(b \mid b \langle \rangle null)$

2. Komponenteninvarianten, die durch nicht-navigierbare Assoziationsenden induziert werden

Fall 2.1: $multA = 0..1$, $multB \leq 1$ induziert die Komponenteninvariante

```
context M
  inv : B.allInstances() → forAll(b |
        A.allInstances() → select(a |
        a.myB = b) → size() <= 1)
```

Fall 2.2: $multA = 1$, $multB \leq 1$ induziert

```
context M
  inv : B.allInstances() → forAll(b |
        A.allInstances() → one(a | a.myB = b))
```

Fall 2.3: $multA = *$ induziert keine Einschränkung

Fall 2.4: $multA = 1..*$, $multB \leq 1$ induziert

context M

inv : $B.allInstances() \rightarrow forAll(b |$
 $A.allInstances() \rightarrow exists(a |$
 $a.myB = b))$

Fall 2.6: Falls $multB > 1$ dann ersetze in den obigen Fällen
 $a.myB = b$ durch $a.myB \rightarrow includes(b)$

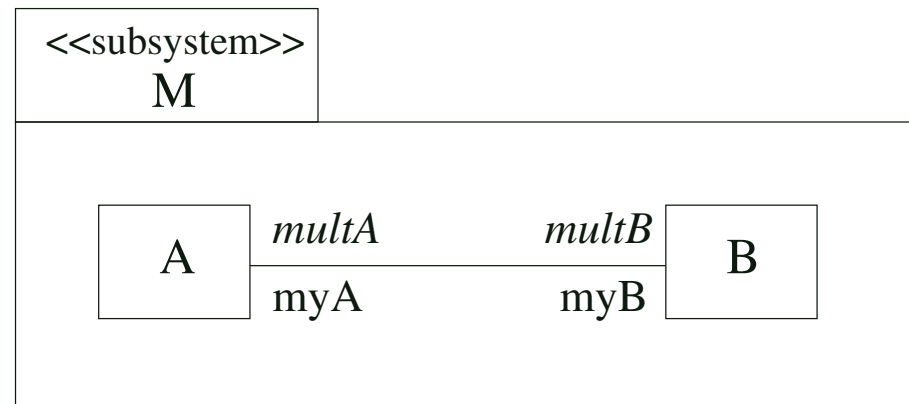
Beispiel (Punkte und Formen):



induziert die folgende Komponenteninvariante:

```
context PointsAndShapes
  inv invOneSystem:
    Point.allInstances() -> forall(p |
      System.allInstances() -> one(sys |
        sys.pointSet -> includes(p))) and
    Shape.allInstances() -> forall(s |
      System.allInstances() -> one(sys |
        sys.figures -> includes(s)))
```

Bidirektionale Assoziationen



induzieren die folgenden impliziten Invarianten:

1. Klasseninvarianten für A induziert durch das navigierbare Assoziationsende mit Rollennamen myB (wie im unidirektionalen Fall).
2. Klasseninvarianten für B induziert durch das navigierbare Assoziationsende mit Rollennamen myA (wie im unidirektionalen Fall).
3. **Komponenteninvarianten** für M induziert durch die Anforderung der Bidirektionalität.

Fall 3.1: $multA = multB = 0..1$

induziert die Komponenteninvariante

context M

inv : $A.allInstances() \rightarrow forAll(a \mid$
 $a.myB \langle \rangle null \text{ implies } a.myB.myA = a) \text{ and}$
 $B.allInstances() \rightarrow forAll(b \mid$
 $b.myA \langle \rangle null \text{ implies } b.myA.myB = b)$

Fall 3.2: $multA = multB = 1$

induziert die Komponenteninvariante

context M

inv : $A.allInstances() \rightarrow forAll(a \mid a.myB.myA = a) \text{ and}$
 $B.allInstances() \rightarrow forAll(b \mid b.myA.myB = b)$

Fall 3.3: $multA = 0..1, multB = 1$ or $multA = 1, multB = 0..1$

ist ähnlich zu den Fällen 3.1 und 3.2

Fall 3.4: $multA = *$ und $multB = *$
induziert die Komponenteninvariante

context M
inv : $A.allInstances() \rightarrow forAll(a \mid$
 $a.myB \rightarrow forAll(b \mid b \langle \rangle null \text{ implies } b.myA \rightarrow includes(a)) \text{ and}$
 $B.allInstances() \rightarrow forAll(b \mid$
 $b.myA \rightarrow forAll(a \mid a \langle \rangle null \text{ implies } a.myB \rightarrow includes(b))$

Alle übrigen Fälle sind geeignete Mischformen der oben betrachteten Fälle.

Beispiel (Punkte und Formen):



induziert die folgende Komponenteninvariante:

```
context PointsAndShapes
  inv invBidirect:
    Point.allInstances() -> forAll(p |
      p.owner <> null implies
        p.owner.points -> includes(p)) and
    Shape.allInstances() -> forAll(s |
      s.points -> forAll(p |
        p <> null implies p.owner = s))
```

3.6 Zusammenfassung

- Jedem Klassendiagramm Δ kann eine Klassensignatur $\Sigma_{\Delta} = (S_{\Delta}, \leq, OP_{\Delta}, Visibility)$ zugeordnet werden, die eine Erweiterung der OCL-Signatur Σ_{Δ}^{OCL} ist.
- Für alle Operationen $op \in Opns_{\Delta} = M_{\Delta} \cup Q_{\Delta} \cup Con_{\Delta}$ können Operationsspezifikationen in der Form von Vor- und Nachbedingungen angegeben werden.
- Eine Operationsspezifikation kann als Vertrag zwischen dem Benutzer der Operation (Kunde) und dem Programmierer der Operation angesehen werden.
- Eine Klasseninvariante spezifiziert eine Eigenschaft, die von allen Objekten der Klasse "von außen" betrachtet erfüllt sein muss.
- Eine Komponenteninvariante spezifiziert eine Eigenschaft, die von allen Objektkonfigurationen erfüllt sein muss, wenn man die Komponente "von außen" betrachtet.

- Eine Komponentenspezifikation $CompSpec = (\langle M, \Delta \rangle, OpSpecs, Invs^e)$ besteht aus einer Komponente mit Klassendiagramm, einer Menge von Operationsspezifikationen und einer Menge von expliziten Klassen- und Komponenteninvarianten.
- Jede Komponentenspezifikation hat eine formale Repräsentation $FRep(CompSpec) = (\langle M, \Sigma_{\Delta} \rangle, OpSpecs, Invs)$ wobei $Invs$ die expliziten Invarianten um implizite Invarianten ergänzt, die sich aus den Multiplizitäten und bidirektionalen Assoziationen von Δ ergeben.