Eseményalapú rendszertervezés helyességbizonyítással

Majzik István
Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék
majzik@mit.bme.hu

2004

Vizuális modellezés és a B kapcsolata

- A B-módszer integrálható az UML alapú szoftverfejlesztési folyamattal: verifikációs lépéseket tudunk a B segítségével elvégezni.

- A B által használt absztrakt állapotgép formalizmus: UML diagramokból transzformációval előállítható.

Strukturális diagramok

Az osztálydiagramok használhatók fel:

- A B állapotgépeket az UML osztályai azonosítják.
- Az attribútumok kezdeti értéke: a B specifikáció inicializáló részében (INITIALISATION).
- OCL kifejezések és a társításokhoz rendelt számosság: invariánsok (INVARIANTS).
- A metódusokhoz rendelt elő-és utófeltételek: B műveletekben (OPERATIONS).
- Állapotgépek összekapcsolása:
  az osztályok közötti kapcsolatok csak fa struktúrájúak lehetnek.

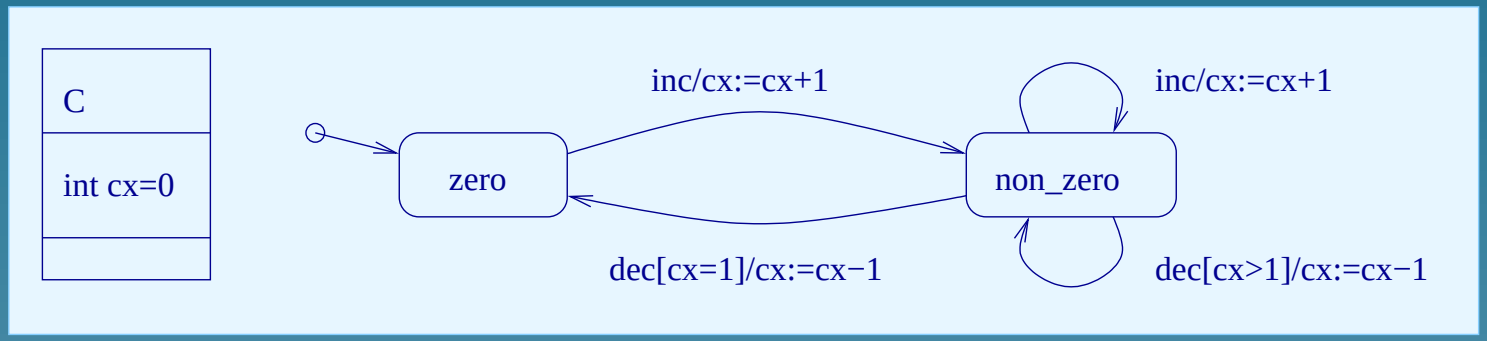
Viselkedési diagramok

Az osztályokhoz rendelt viselkedési diagramok: műveletek (OPERATIONS).

- Az állapottérkép állapotai: felsorolás típusú állapotváltozó.
- Események: szintén állapotváltozók.
- Állapotátmenetek: egy-egy műveletet azonosítanak
  - ⋆ az állapotváltozókon értelmezettek,
  - ⋆ az átmenet kiindulási állapota: előfeltétel,
  - ⋆ trigger és őrfeltétel: ugyancsak előfeltétel,
  - ⋆ akció és célállapot: értékadás.

Példa UML diagram

Példaként tekintsük a C nevű osztályt, aminek állapottérkép diagramja az alábbi:



A B specifikáció elemei

A B specifikáció állapotváltozói:

- A C osztály példányainak azonosítói ($Cinstances$).
  - ⋆ A lehetséges példányokat egy halmaz reprezentálja ($CSET$)
  - ⋆ Egy példány kijelölése ($thisC$ "index").
- Az állapot-azonosító (C_state)
  - ⋆ Az állapotok halmaza (C_STATE).
- Az osztály attribútuma (cx).
  - ⋆ Típus hozzárendelése itt is.

Az invariánsok megkötik az állapotváltozókat.

A B specifikáció

MACHINE C
SETS $CSET; C\_STATE = \{zero, non\_zero\}$
VARIABLES $Cinstances, c\_state, cx$
INVARIANT
$Cinstances \subseteq CSET$ &
$c\_state : Cinstances \rightarrow C\_STATE$ &
$cx : Cinstances \rightarrow NAT$
INITIALISATION $Cinstances := \{\} \parallel c\_state := \{\} \parallel cx := 0$

Műveletek

A dec művelet:

$dec(thisC) =$
PRE $thisC : Cinstances$ THEN
SELECT $c\_state(thisC) = non\_zero \,\&\, cx(thisC) = 1$
THEN $c\_state(thisC) := zero$ END
|| SELECT $c\_state(thisC) = non\_zero \,\&\, cx(thisC) > 1$
THEN $skip$ END
|| $cx(thisC) := cx(thisC) - 1$ END
END

- Az UML profile használatával az UML diagramjaiból B specifikáció generálható.
- Így az UML modell konzisztenciája és a finomítási lépések helyessége a B eszközök segítségével vizsgálható.