DD1350 Logik för dataloger

Fö 11 – Temporallogik

1

Rigorös systemutveckling

I kursens tio första föreläsningar har vi diskuterat den matematiska logikens teori.

I resten av kursen ska vi titta på tillämpningar, speciellt **rigorös systemutveckling**, där vi använder logik för att skapa **bevisbart korrekta system**.

System och systembeteende

Funktionsbeteende: (fö 13-14)
input $\Rightarrow$ exekvering $\Rightarrow$ output
(t.ex. ett program som beräknar x^y)
Här vill man bevisa att **givet att indata följer specifikationen**, **så kommer också utdata att göra det**.

Interaktionsbeteende: (denna och nästa föreläsning)
begäran $\Rightarrow$ respons $\Rightarrow$ begäran $\Rightarrow$ …
t.ex. servrar, bankomater, säkerhetsprotokoll, …
Här vill man bevisa att **vissa önskvärda egenskaper gäller i alla möjliga interaktionssekvenser**.

Modellbaserad systemutveckling

Väsentliga beteendeegenskaper hos ett system beskrivs med en **specifikation** (som kan vara logiska formler).

Man kan skapa en abstrakt **modell** av systembeteendet (t.ex. med **automater**).

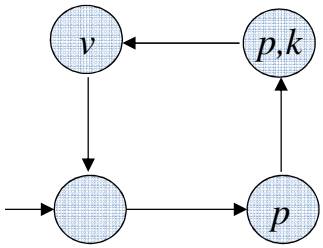
Man kan då **verifiera** att modellen har de specificerade egenskaperna, t.ex. med en **modellprovare**.
Modellen kan sedan ligga till grund för **implementation**.

Interaktionsbeteende

Vilka interaktionssekvenser med/i systemet är möjliga?
Representeras bäst med:

- **tillstånd** (eng: states)
- **övergångar** (eng: transitions)

och kan visualiseras som en graf. T.ex.:



p : rätta pengar är instoppade
k : knappen är intryckt
v : varan är levererad

Beteendeegenskaper

Beteendeegenskaper är **temporala** i sin karaktär: något

- är **alltid** sant (**always**)
- blir sant **så småningom** (**eventually**)
- är sant oändligt ofta
- är sant tills någonting annat blir sant (**until**)

Vad som är sant eller inte i ett givet tillstånd beskriver vi med satslogik (valueringar). Vi introducerar **temporala kvantifierare** för att uttrycka sanning över **sekvenser** av valueringar.

Temporallogiken CTL

CTL (***C**omputation **T**ree **L**ogic*) = satslogik + temporala kvantifierare

- vägkvantifierare
  - över **alla** vägar A
  - över **någon** väg E
- tillståndskvantifierare
  - för **nästa** tillstånd i vägen X
  - för **alla** tillstånd i vägen G
  - för **något** tillstånd i vägen F

Vår ansats i kursen

Specifikationer är formler i CTL.

Vi låter $Atoms = \{ p_1, ..., p_n \}$ vara alla satslogiska variabler vi använder i den aktuella specifikationen.

Modeller är **övergångssystem** (transition systems) som kan åskådliggöras som **grafer**. En modell M består av

- en mängd S av **tillstånd**
- en **övergångsrelation** $\rightarrow \subseteq S \times S$
- en **sanningstilldelning** L (en funktion från S till 2^{Atoms})

CTL: Intuitiv semantik

AX ϕ	i nästa tillstånd ϕ
AG ϕ	alltid ϕ
AF ϕ	så småningom ϕ
EX ϕ	i något nästa tillstånd ϕ
EG ϕ	det finns en väg där alltid ϕ
EF ϕ	det finns en väg där så småningom ϕ

CTL: Formell semantik (1/3)

- M, $s \models p$ om $p \in L(s)$
- M, $s \models \neg\phi$ om ***inte*** M, $s \models \phi$
- M, $s \models \phi \wedge \psi$ om M, $s \models \phi$ *och* M, $s \models \psi$
- … etc. (*cf.* predikatlogik)

CTL: Formell semantik (2/3)

- M, s |= AX ϕ — om M, s' |= ϕ för alla efterföljare s' till s
- M, s |= AG ϕ — om i alla vägar $s_1 \rightarrow s_2 \rightarrow \ldots$ från s M, s_i |= ϕ för alla i
- M, s |= AF ϕ — om i alla vägar $s_1 \rightarrow s_2 \rightarrow \ldots$ från s M, s_i |= ϕ för något i

CTL: Formell semantik (3/3)

- M, s |= EX ϕ — om M, s' |= ϕ för någon efterföljare s' till s
- M, s |= EG ϕ — om i någon väg $s_1 \rightarrow s_2 \rightarrow \ldots$ från s M, s_i |= ϕ för alla i
- M, s |= EF ϕ — om i någon väg $s_1 \rightarrow s_2 \rightarrow \ldots$ från s M, s_i |= ϕ för något i

Specifikationsmönster

AG AF ϕ	oändligt ofta ϕ
AG ($\phi \rightarrow$ AF ψ)	alltid efter ϕ så småningom ψ
AG EF ϕ	alltid nåbar ϕ
AF AG ϕ	så småningom stabilt ϕ