DD1350 Logik för dataloger

Fö 12 – Modellprovning

Exempel (server)

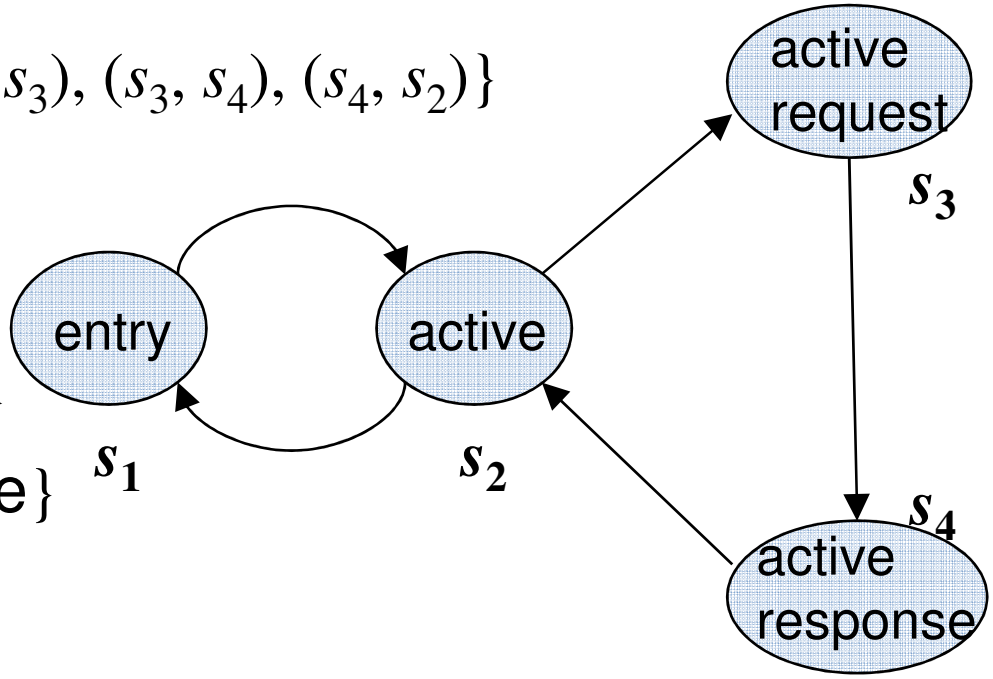
$Atoms$ = {entry, active, request, response}

Modell M = $(S, \rightarrow, L)$ där:

$S = \{s_1, s_2, s_3, s_4\}$

$\rightarrow = \{(s_1, s_2), (s_2, s_1), (s_2, s_3), (s_3, s_4), (s_4, s_2)\}$

$L(s_1)$ = {entry}
$L(s_2)$ = {active}
$L(s_3)$ = {active, request}
$L(s_4)$ = {active, response}



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

- Ges relativt ett tillstånd s i en modell

$$\mathsf{M} = (S, \rightarrow, L)$$

- Definieras induktivt över formelns struktur, som **satisfieringsrelation**

$$\mathsf{M}, s \models \phi$$

- Läses ”ϕ är sann i tillståndet *s*”.

Modellprovning

Vi vill nu definiera ett **bevissystem** med vilket man kan bevisa att en given CTL-formel är sann i ett visst tillstånd i en viss modell.

Ett program som konstruerar sådana bevis kallas **modellprovare** (vilket ska implementeras i labb 2).

Bevissystem

De sekventer vi vill bevisa har formen M, $s \models_U \phi$

Regler, t.ex.:

$$\frac{\mathsf{M}, s_1 \models_{[\,]} \phi \quad \ldots \quad \mathsf{M}, s_n \models_{[\,]} \phi}{\mathsf{M}, s \models_{[\,]} \mathsf{AX}\, \phi}$$

(Se instruktionerna för labb 2 för en fullständig uppsättning regler.)

Bevisen vi kommer konstruera är i form av **träd**, där roten är formeln vi vill bevisa, och löven är axiom i systemet.

Slingdetektion (loop checking)

För att sökandet efter ett bevis ska **terminera**, så uppdaterar vi i varje steg en lista U med tillstånd i vilka vi redan har utvärderat formeln.

Detta garanterar **avgörbarhet**: Modellprovaren kommer alltid att terminera med ett bevis (om formeln är sann i tillståndet), eller med ett ”no” (om formeln är falsk).

Man kan även bevisa **sundhet** och **fullständighet**.

Sundhet och fullständighet

Bevissystemet är **sunt** och **fullständigt** för ändliga modeller **M** :

$$\mathbf{M}, s \vdash_{[]} \phi$$

om och endast om

$$\mathbf{M}, s \models \phi$$