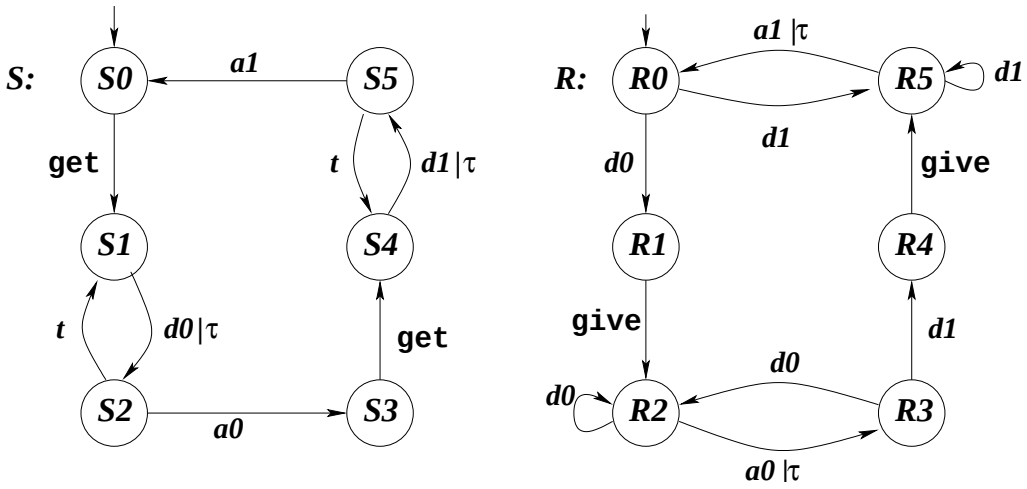
Spesifioinnin ja verifioinnin perusteet

Harjoitus 6, 22.2.2008

HUOM! Ke 20.2 ei ole luentoa. Viimeinen luento pe 22.2 klo 12-14.

1. Spesifioi Lotoksella AB-protokollan toimintaa kuvaava systeemi $S|[d0, d1, a0, a1]|R$, kun S ja R ovat seuraavat siirtymäsysteemit:



2. Muodosta edellisen tehtävän yhteistilaverkko CADP-ohjelmistoa käyttäen. Toteuttaako tämä AB-protokollan versio halutun monisteessa esitetyn palvelun ympäristölleen?

3. Edellisissä harjoituksissa spesifioit Lotoksella Hymanin poissulkemisprotokolan kahden prosessin tapauksessa ja muodostit yhteistilaverkon CADP-ohjelmistoa käyttäen. Piilota yhteistilaverkossa kaikki tapahtumat lukuunottamatta kriittistä aluetta mallintavia. Minimoi nyt yhteistilaverkko heikon bisimulaation suhteen ja tutki tulosta. Ovatko prosessit koskaan yhtäaikaa kriittisellä alueella?

4. Ominaisuuksien testaus voidaan tehdä spesifioimalla haluttu ominaisuus Lotos-testiprosessina (joka päättyy testin onnistumisesta kertovaan tapahtumaan `testok`) ja sykronoimalla testiprosessi spesifikaation kanssa. Tällöin sykronointilistassa ovat kaikki testiprosessin tapahtumat paitsi tapahtuma `testok`.

   Jos esimerkiksi prosessi S voi suorittaa joko tapahtumajonon `ev1;ev2;ev3;exit` tai tapahtumajonon `ev1;ev2;ev4;exit` ja haluttaisiin tietää voiko tapahtuma `ev4` seurata tapahtumaa `ev2`, muodostetaan testausta varten seuraavat prosessit ja käyttäytymislauseke:

   process T[ev2, ev4,testok] : **exit** :=
   ev2;ev4;testok;**exit**
   endproc

process S[ev1,ev2,ev3,ev4] : **exit** :=
  ev1;ev2;ev3;**exit** [] ev1;ev2;ev4;**exit**
endproc

S[ev1,ev2,ev3,ev4] |[ev2, ev4]| T[ev2,ev4,testok]

Prosessit T ja S siis sykronoidaan taphtumien `ev2` ja `ev4` avulla. Tämän jälkeen tutkitaan kaikki mahdolliset yhdistetyn prosessin jäljet ja jos testitapahtuma löydetään on testi mennyt läpi.

Miten voit käyttää yllä olevaa menetelmää selvittääksesi voivatko prosessit olla yhtäaikaa kriittisellä alueella? Kokeile Hymanin algoritmia ja monisteessa esitettyä Dekkerin algoritmia (sivu 97-99).

5. Olkoon $P \approx_{wbis} Q$. Tutki päteekö kaikilla prosesseilla R $R[> P \approx_{wbis} R[> Q$. (HUOM! Jos väite ei päde, niin riittää antaa vastaesimerkki.)

6. (a) Prosessin kutsu ei ole tarkalleen sama, kuin prosessin vartalo, jossa muodolliset parametrit on korvattu kutsuparametreilla. Tarkastele alla olevaa prosessia ja kerro miten voit havainnollistaa asiaa prosessilla.

```
process koe [a,b] :=
  apu[a,a]
 []
  apu[a,b]
where
  process apu[x,y] :=
   x; exit || y; exit
  endproc
endproc
```

   (b) Tarkastellaan seuraavia täyden Lotoksen prosesseja:

```
P[a,b,c] (n:Nat): noexit :=
 a!n; b?m:Nat !3; c?n:Nat; P[a,b,c](n)

Q[a,b,c]: noexit :=
 a?x:Nat; b!x !3; c!x+1; Q[a,b,c]
  []
 a!1; i; Q[a,b,c]
```

   Muodosta yhteistilaverkkoa

```
P[a,b,c](0) || Q[a,b,c]
```

   sen verran, että kokonaisrakenne tulee selville.