Univerza v Mariboru
Fakulteta za elektrotehniko, računalništvo in informatiko

Robert Meolic

Preverjanje pravilnosti obnašanja sistemov s sočasnostjo

Magistrsko delo

Ključne besede: formalne metode verifikacije sistemov, sistemi s sočasnostjo, procesne algebre, opazovalne ekvivalence, testne ekvivalence, simbolično preverjanje modelov, ACTL, BDD

Vsebina:

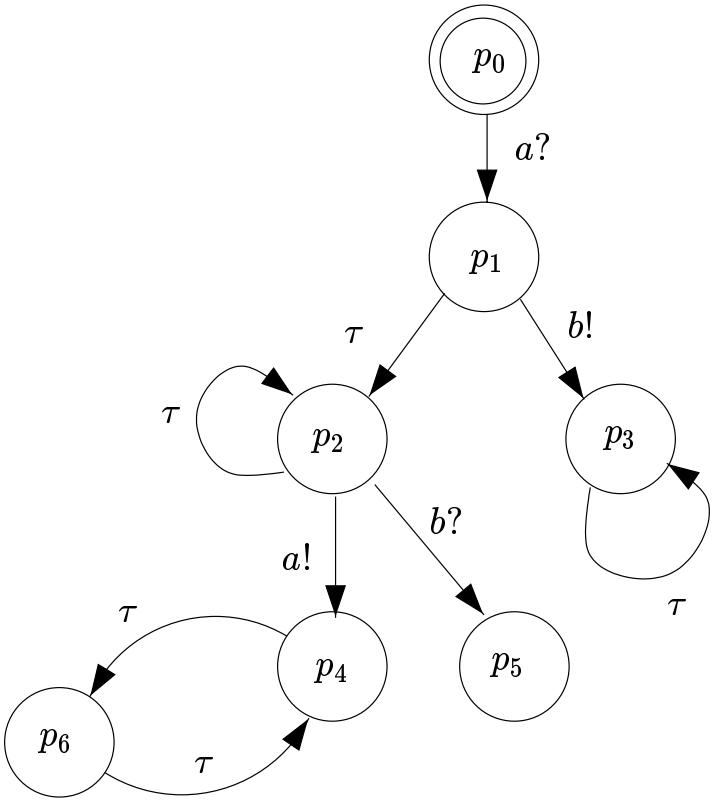
Preverjanje pravilnosti obnašanja sistemov s sočasnostjo

Uvod

- Formalne metode **verifikacije sistemov** so potrebne, ker kompleksnost elektronske in računalniške opreme narašča.
- Prepozno odkrita **napaka v sistemu** se lahko odraža v veliki materialni škodi (primer: Intel Pentium, 1994),
- Bistvena elementa pri snovanju sistemov sta **specifikacija zahtev** in **specifikacija zasnove** sistema.
- **Sistemi s sočasnostjo** so sestavljeni iz množice komponent, ki se izvajajo sočasno in med seboj komunicirajo.
- **Formalne metode** so tiste, ki temeljijo na matematičnih principih in vsebujejo sistem dokazovanja.
- Jedro formalnih metod za snovanje sistemov predstavljajo **formalni jeziki** za podajanje specifikacij.

Procesna algebra

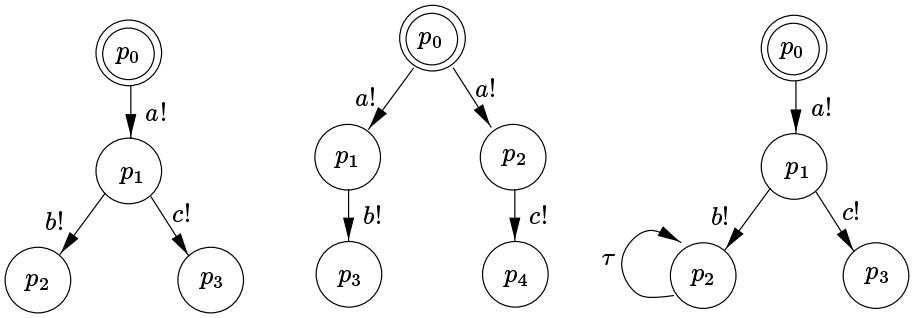
- Sistem s sočasnostjo predstavimo kot **množico procesov**.
- Proces **izvaja dogodke** in ob tem prehaja med svojimi stanji.
- Ločimo **notranji** dogodek τ ter **vhodne** in **izhodne** zunanje dogodke.
- Nad procesi definiramo **številne operacije**:
  - iskanje dosegljivih, zagatnih, divergentnih in zaciklanih stanj,
  - preimenovanje, skrivanje in prepoved dogodkov,
  - sestavljanje procesov z zaporedno, alternativno, paralelno in delta kompozicijo.
- Primer procesa:



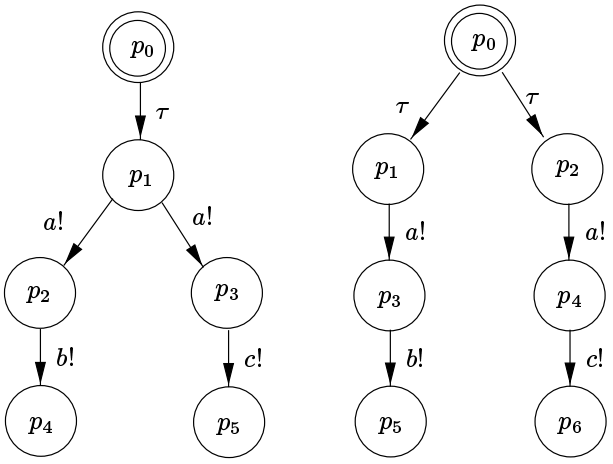
Relacije med procesi

- Obravnavali smo številne **ekvivalenčne relacije**:
  - ekvivalenca sledi,
  - stroga, vejitvena in šibka opazovalna ekvivalenca,
  - MAY-ekvivalenca, MUST-ekvivalenca in testna ekvivalenca.

- Trije procesi, ki imajo **ekvivalentne sledi**:



- Procesa, ki **nista šibko opazovalno** ekvivalentna:



Preverjanje modela z ACTL-jem

- Cilj preverjanja pravilnosti obnašanja sistemov je pokazati, da **specifikacija zasnove** sistema zadosti dani **specifikaciji zahtev** sistema.
- Pri preverjanju modela specifikacijo zahtev sistema podamo v obliki **matematičnih formul**.
- **Akcijska logika drevesa izvajanja (ACTL)** je matematična notacija, ki je zelo primerna za opisovanje lastnosti procesov.
- ACTL je izjavna temporalna logika razvejanega časa. Opisuje, kako proces **s časom** izvaja posamezne dogodke.
- **Značilne lastnosti**, ki jih opisujemo z ACTL-jem, so:
  - proces bo v danem stanju gotovo izvedel dogodek a,
  - proces v danem stanju lahko izvede dogodek a,
  - proces bo nekoč v prihodnosti gotovo izvedel dogodek a,
  - proces ne bo v prihodnosti nikoli izvedel dogodka a.
- **Sintakso** ACTL-ja sestavljajo:
  - Boolovi operatorji $\neg$, $\wedge$ in $\vee$,
  - kvantifikatorja poti **A** in **E**,
  - temporalni operatorji **X**, **F**, **G**, **U**, **$\underline{\mathbf{U}}$**,
  - raznovrstni oklepaji: (), [] in <>.
- Primera dveh ACTL formul sta:
  - $\mathbf{AG}\,[\,\mathbf{semR!}\,]\,\mathbf{A}\,[\,\{\neg\mathbf{vlakS!}\}\,\underline{\mathbf{U}}\,\{\mathbf{semZ!}\}\,]$
  - $\neg\,\mathbf{EF}\,(\mathbf{EX}\,\{\mathbf{vlakS!}\} \wedge \mathbf{EX}\,\{\mathbf{avtoS!}\})$

Izvedba procesne algebre z BDD-ji

- Osnovni gradniki procesov so: **množica stanj**, **množica dogodkov** in **prehajalna relacija**. Vse operacije v procesni algebri temeljijo na operacijah nad množicami in relacijami.

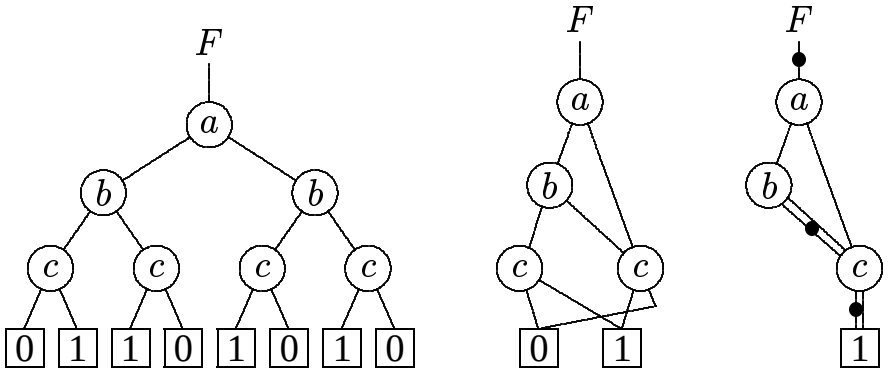
- Množice in relacije lahko predstavimo z logičnimi funkcijami, ki jih imenujemo **karakteristične funkcije**. Operacije nad množicami in relacijami preidejo v Boolove operacije med logičnimi funkcijami.

- Za hranjenje in obdelovanje logičnih funkcij z računalnikom uporabljamo podatkovno strukturo **binarni odločitveni graf** (BDD). Operacije med logični funkcijami izvedemo kot operacije nad grafi.

- BDD-ji temeljijo na rekurzivni razčlenitvi logične funkcije po **Shannonovi formuli**:

$$F \;=\; x_i \cdot F|_{x_i=1} + \overline{x_i} \cdot F|_{x_i=0} \;=\; \mathsf{ITE}(x_i,\; F|_{x_i=1},\; F|_{x_i=0}) \;.$$

- Tri vrste BDD-jev za logično funkcijo $a \cdot \overline{c} + \overline{a} \cdot \overline{b} \cdot c + b \cdot \overline{c}$:



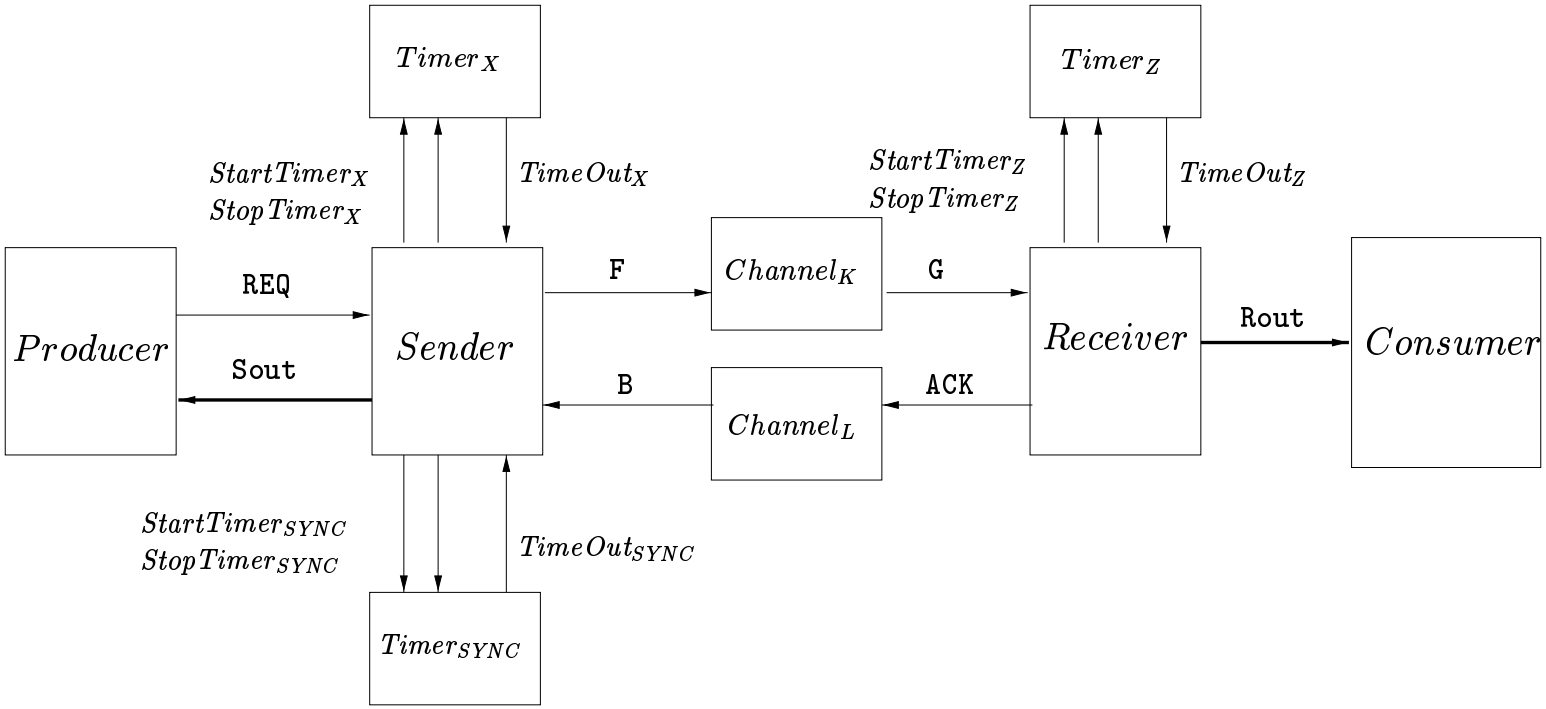
Rezultati

- V sklopu magistrskega dela je nastalo **orodje EST**, ki zmore učinkovito formalno verifikacijo sistemov s procesno algebro.

- Orodje EST je napisano v C-ju, uporabljeni pa so tudi `bison`, `flex` in `Tcl/Tk`.

- **Zmogljivosti** orodja EST:
  - zna včitati tekstovne datoteke z opisi procesov,
  - zna kodirati procese in jih predstaviti z BDD-ji,
  - zna sestavljati procese s paralelno in delta kompozicijo,
  - zna ugotavljati strogo in šibko opazovalno ekvivalenco med procesi,
  - zna ugotavljati testno ekvivalenco med procesi,
  - zna simbolično preverjati modele z ACTL-jem.

Protokol z omejenim številom ponovnih oddaj (BRP)



Enota *Producer* želi zaporedoma prenesti več večjih podatkovnih paketov do enote *Consumer* skozi nezanesljiv kanal, ki izgublja podatke.

Rezultati

proces	število stanj	število prehodov	število prehodov z zunanjim dogodkom	število vozlišč v BDD-ju
S	48	66	66	221
R	27	40	40	152
K	7	10	6	54
L	4	5	3	27
T	8	10	8	66
BRP	1726	3907	396	3460
BRP_{trace}	6	11	11	64
BRP_{weak}	15	20	10	101
Obs_{BRP}	1726	282186	192462	28786
$Obs_{BRP_{weak}}$	15	68	41	117
BRP_{test}	14	19	10	99
Acc_{BRP}	45	69	69	254
$Acc_{BRP_{test}}$	6	11	11	64

operacija	novih vozlišč v BDD-jih	čas izvajanja [s]
1. kodiranje procesov S, R, K, L in T	4197	0.12
2. paralelna kompozicija	84969	3.38
3. kodiranje procesov BRP_{trace}, BRP_{weak} in BRP_{test}	1328	0.07
4. tvorjenje Obs_{BRP}	376247	22.67
5. tvorjenje $Obs_{BRP_{weak}}$	398	0.04
6. preverjanje bisimulacije med Obs_{BRP} in $Obs_{BRP_{weak}}$	51883	4.97
7. tvorjenje Acc_{BRP}	53308	6.75
8. tvorjenje $Acc_{BRP_{test}}$	1345	0.14
9. preverjanje bisimulacije med Acc_{BRP} in $Acc_{BRP_{test}}$	6200	0.27
10. preverjanje modelov z ACTL-jem	135305*	3.78

Zaključek

- Magistrsko delo obravnava metode preverjanja pravilnosti obnašanja sistemov s sočasnostjo, ki temeljijo na opisu sistema s **procesno algebro**.
- Pravilnost obnašanja sistemov lahko preverimo
  - z **ugotavljanjem ekvivalence** med danima specifikacijama,
  - s **preverjanjem modela**.
- Magistrsko delo nazorno prikazuje teorijo in izvedbo. Vsebuje **39 definicij** in **89 slik**, od tega je **26 algoritmov**.
- Magistrsko delo je podprto z **zmogljivim orodjem** EST, s katerim smo verificirali realni komunikacijski protokol.
- Magistrsko delo vsebuje več **originalnih prispevkov**:
  - učinkovita rekurzivna algoritma za **kodiranje** in **dekodiranje** procesov,
  - učinkovito izvedbo **paralelne kompozicije** n procesov,
  - učinkovito izvedbo algoritma za ugotavljanje **testne ekvivalence**,
  - vpeljavo številnih **vzorcev CTL formul** za podajanje lastnosti sistemov,
  - **originalno definicijo** ACTL-ja ter vpeljavo uporabnih okrajšav itd.
- Obstoječe orodje EST nudi velike možnosti za nadgradnjo:
  - **generiranje izvršne kode** iz opisa procesa ter **simulacija** hkratnega izvajanja procesov,
  - **abstrakcija** (minimizacija) procesov glede na dano ekvivalenčno relacijo oz. množico ACTL formul,
  - vpeljava **poštenih poti** ter iskanje **prič in protiprimerov** pri preverjanju modelov z ACTL-jem itd.