

Modellek ekvivalenciájának ellenőrzése

Majzik István

Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék

Relációk modellek között

- **Megfelelőség (ekvivalencia) modellek között:**

Referencia modell ↔ Módosított modell

Specifikáció (absztrakt) ↔ Megvalósítás (konkrét, részletes)

Elvárt viselkedés ↔ Nyújtott viselkedés (pl. protokoll)

Ideális rendszer ↔ Hibatűrő rendszer adott hibák esetén

- **Finomítás (rendezés) modellek között:**

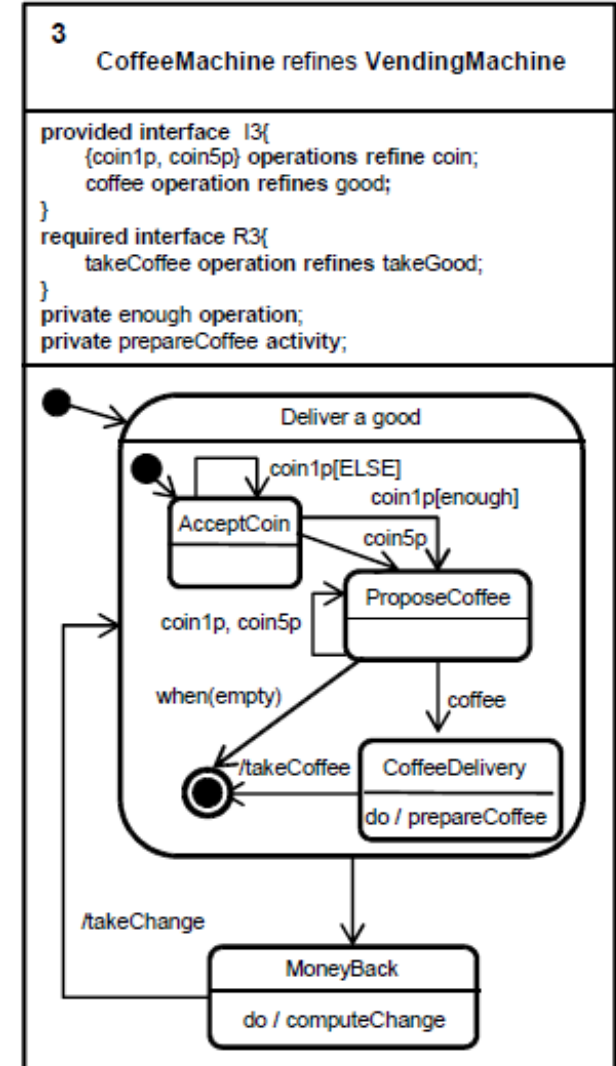
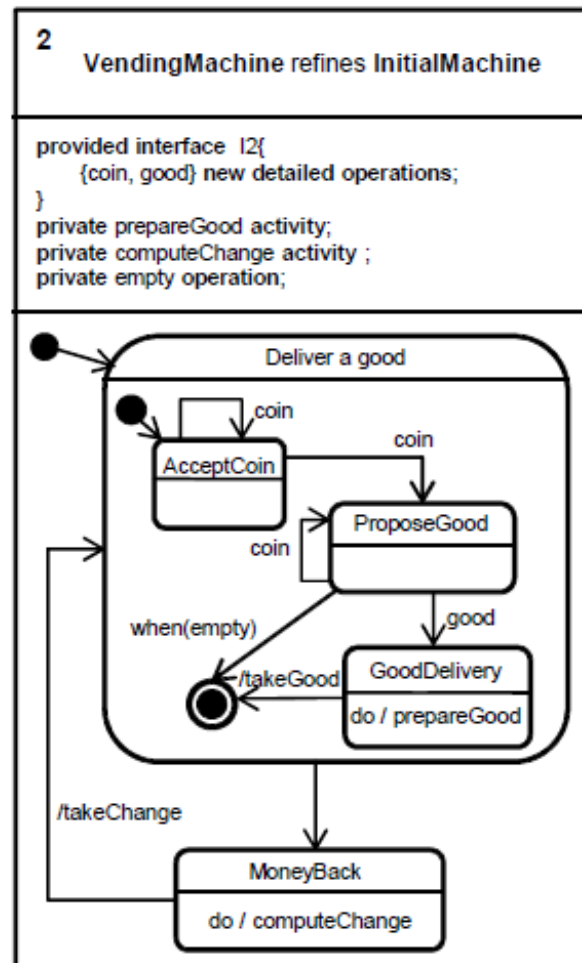
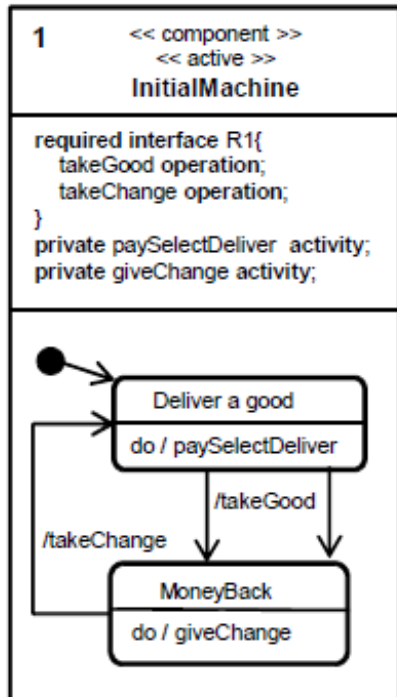
- Referencia viselkedés megtartása, meghatározott bővítésekkel

- Lehetséges nondeterminizmus csökkentése

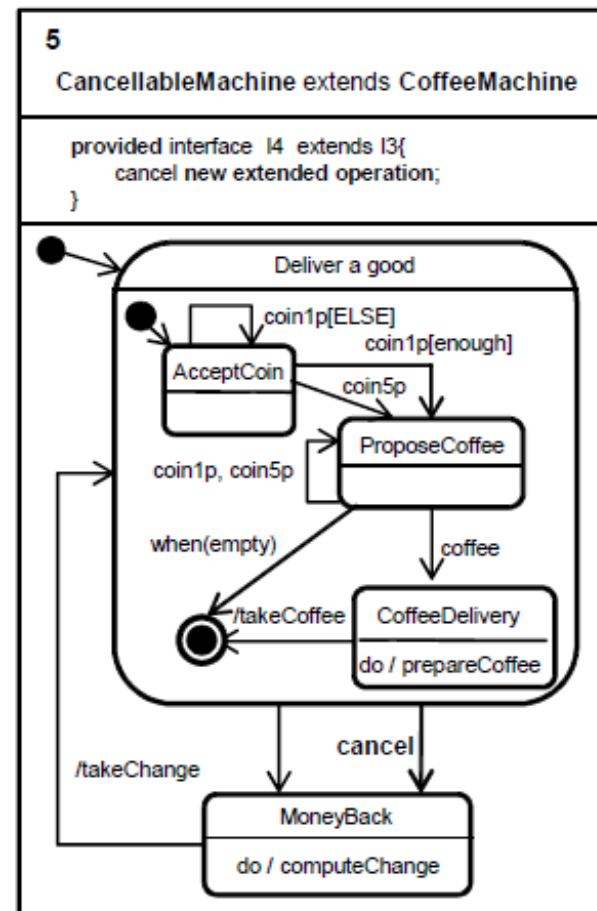
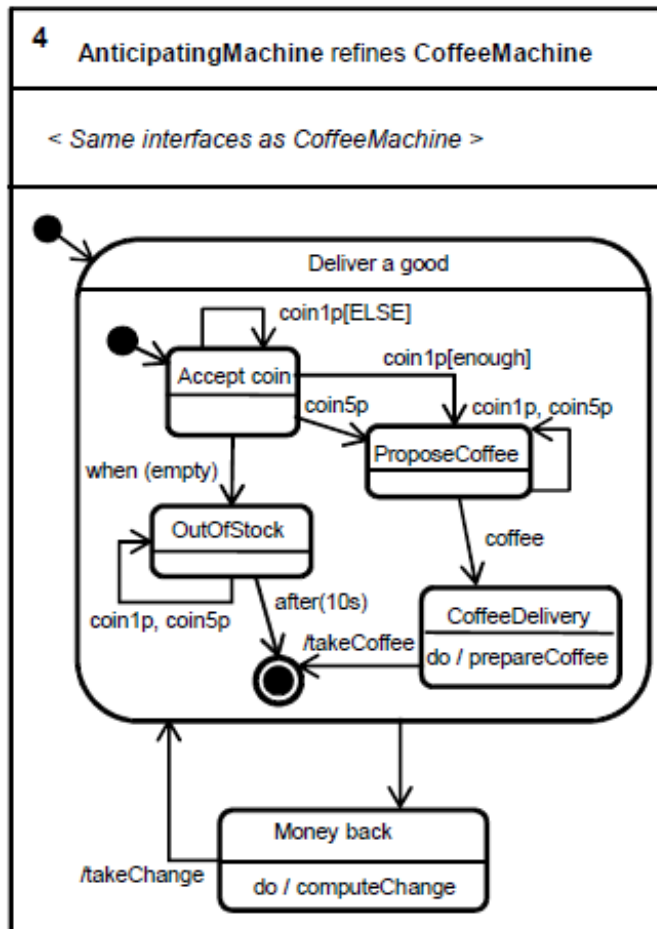
- Lehetséges holtpontok számának csökkentése

A problémakör bevezetése

Példa: Állapottérkép modellek finomítása

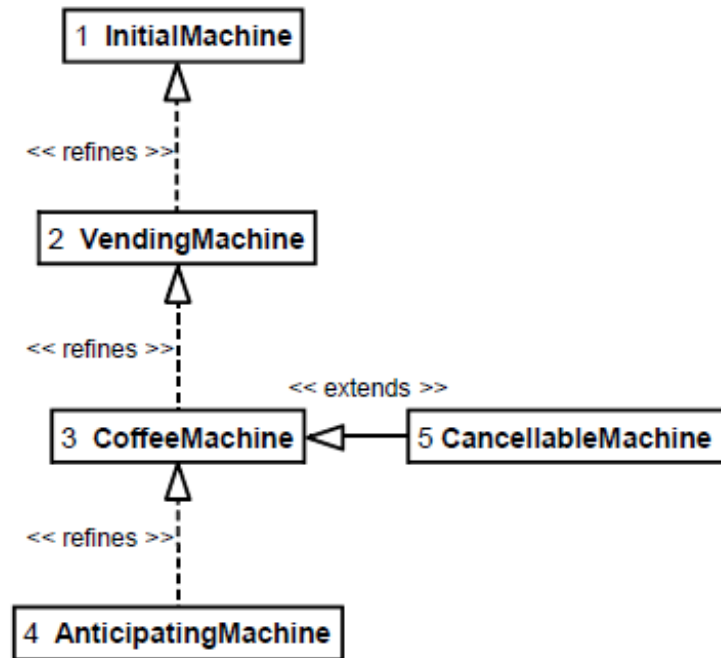


Példa: Állapottérkép modellek finomítása (folytatás)



Mit szeretnénk?

Relációkat ellenőrizni az állapottérkép modelleken



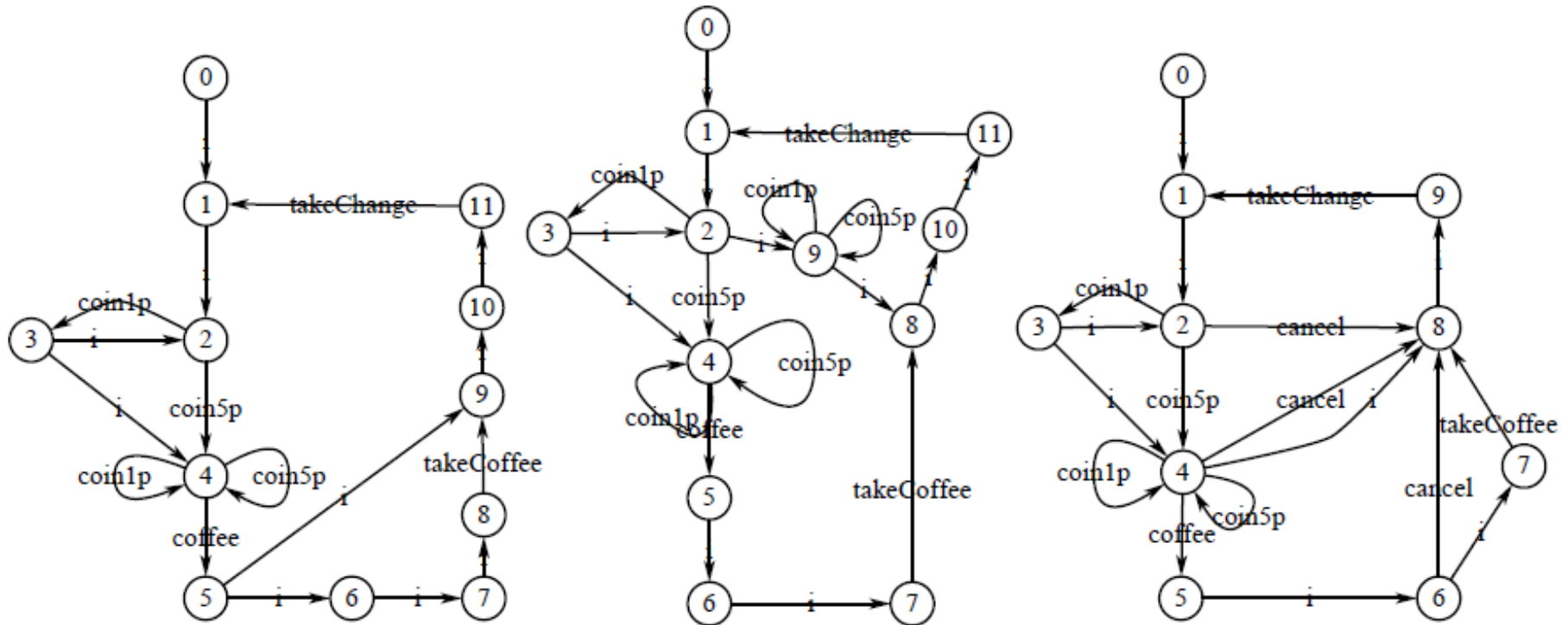
Mit várunk egy finomítás relációtól?

- Reflexív és tranzitív reláció
- Nem szimmetrikus reláció
- Élő tulajdonság megtartása: A finomított modell tudja nyújtani azt az viselkedést, amit az eredeti modellnek is tudnia kellett
 - Méltányosság (fairness) feltételezés: Az élő tulajdonság megtartása méltányos viselkedés mellett történik (azaz választás esetén minden viselkedésnek van esélye)
- Komponálhatóság:
 - Egymás utáni finomítások finomítást eredményeznek
 - Finomítás és kiterjesztés együtt kiterjesztést eredményez
- ...

Pontos definíció szükséges!

A relációk definiálása

- A relációk definiálása alacsony szintű modelleken (tipikusan LTS-eken) történik



a. LTS₃: CoffeeMachine

b. LTS₄: AnticipatingMachine

c. LTS₅: CancellableMachine

Formalizmusok

- Ekvivalencia és finomítási relációk modellje:
LTS (Labeled Transition System)

$$LTS = (S, Act, \rightarrow)$$

S az állapotok halmaza

Act az akciók halmaza

$\rightarrow \subseteq S \times Act \times S$ az állapotátmeneti reláció

- LTS-ek magasabb rendű formalizmusokból (műveleti szemantikával) származhatnak
 - Processz algebra, Petri-háló, állapottérkép, ...

Relációk csoportosítása

- **Ekvivalencia reláció (equivalence) =**

- Reflexív, tranzitív, szimmetrikus

Kongruencia reláció (congruence)

- Ha $T1=T2$, akkor minden $C[]$ környezetre $C[T1]=C[T2]$
- Azonos kiterjesztés megőrzi az ekvivalenciát
- Nyelvfüggő: $C[]$ beillesztés hogyan történik

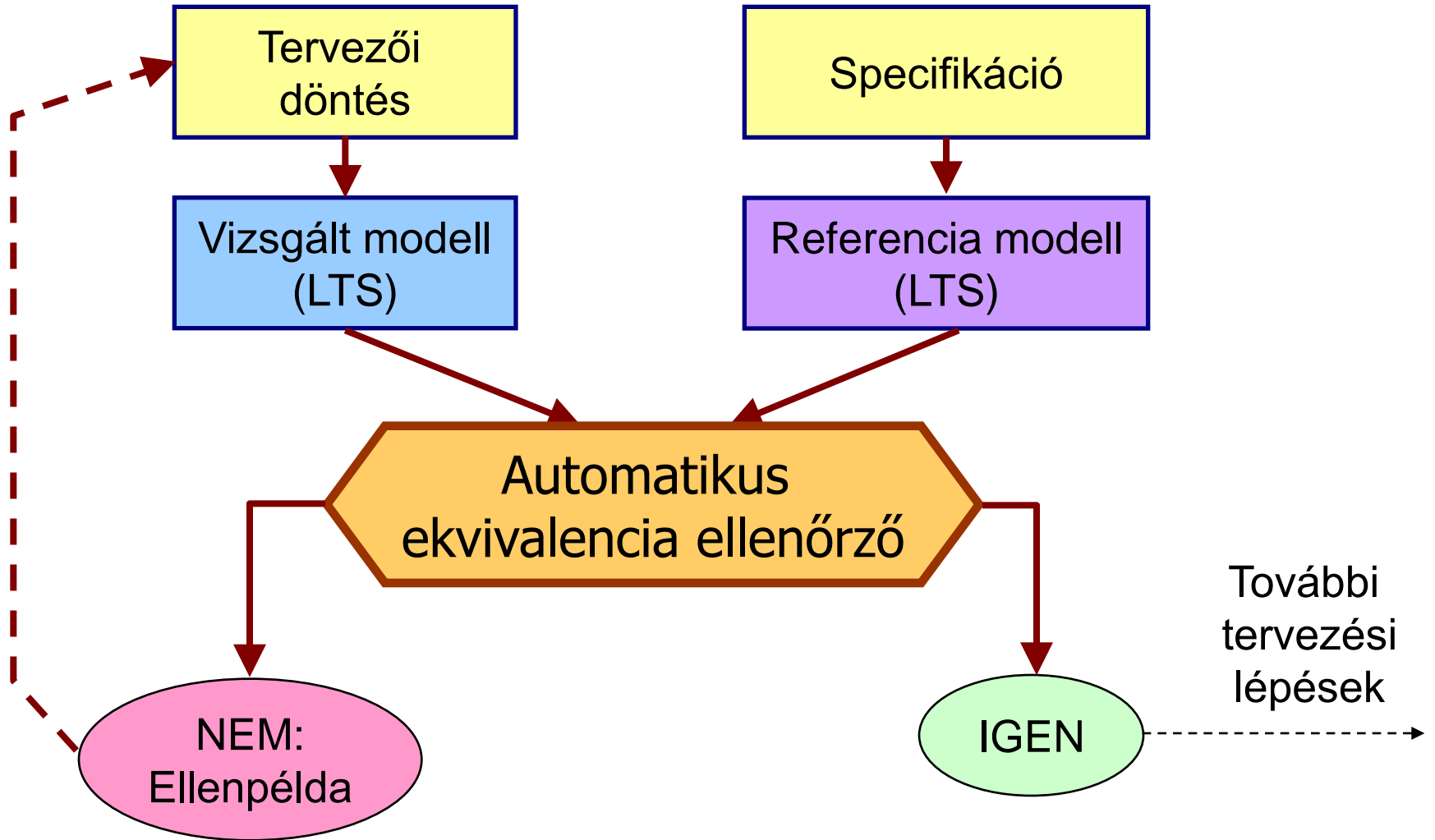
- **Finomítási (rendezési) reláció (preorder) \leq**

- Reflexív, tranzitív, antiszimmetrikus

Prekongruencia reláció (precongruence) \leq

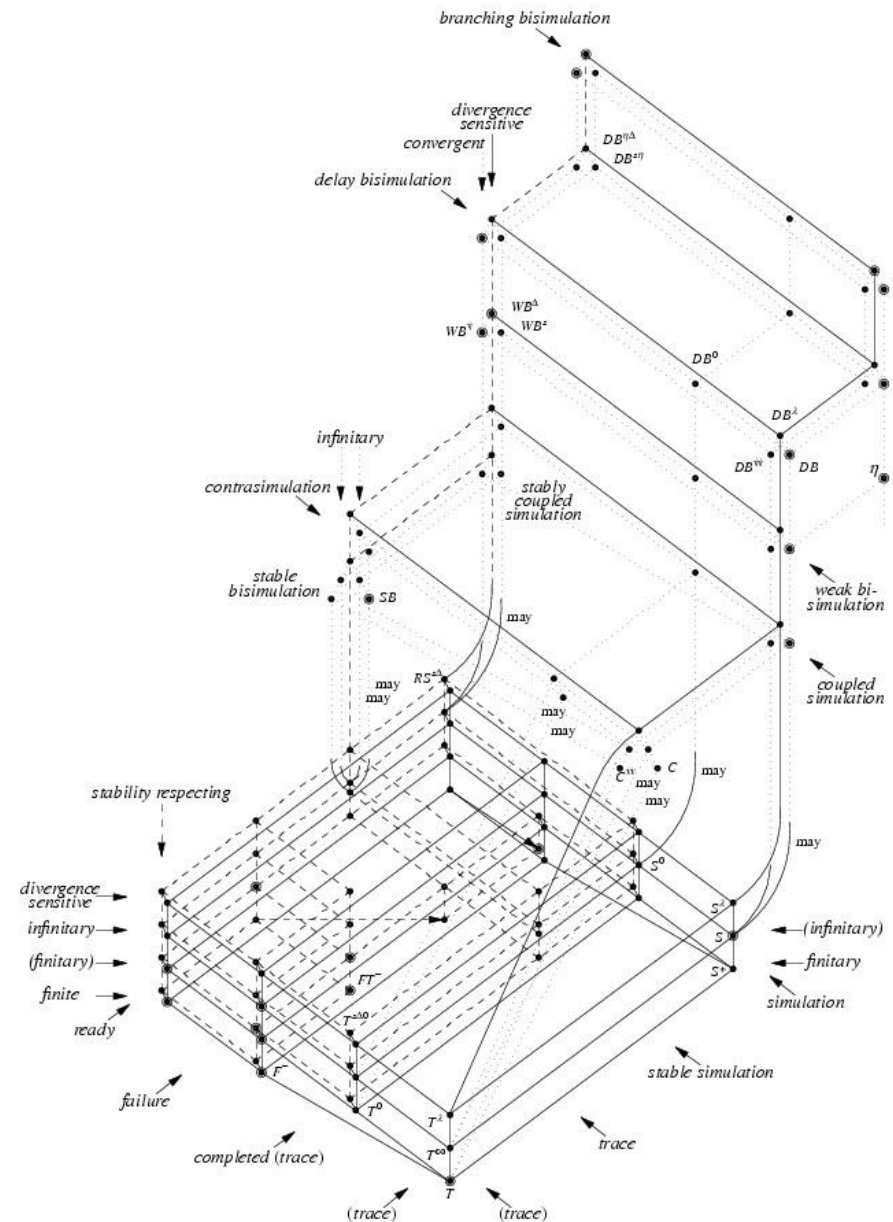
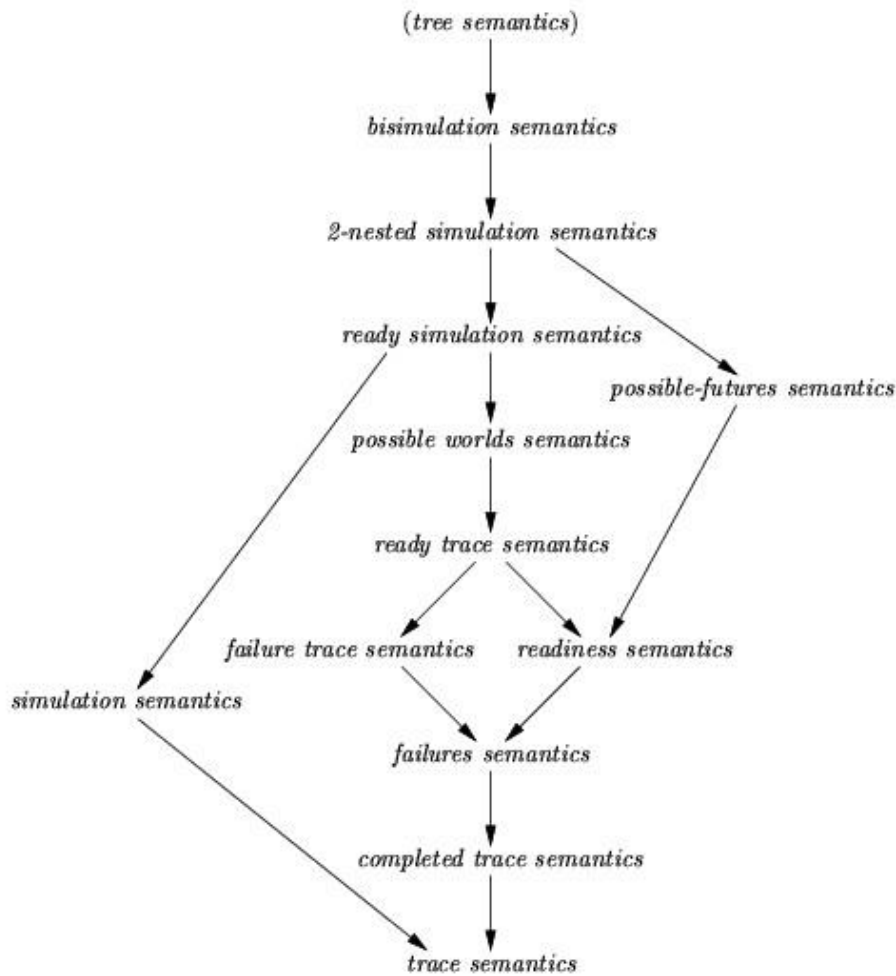
- Ha $T1 \leq T2$, akkor minden $C[]$ környezetre $C[T1] \leq C[T2]$
- Azonos kiterjesztés megőrzi a finomítási relációt

Ekvivalencia ellenőrzés



Relációk: Miért van ennyiféle?

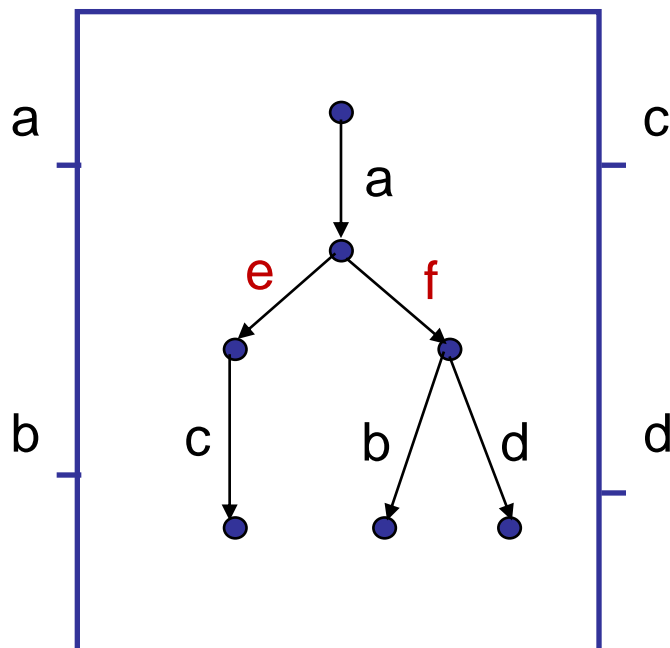
Relációk hierarchiája:



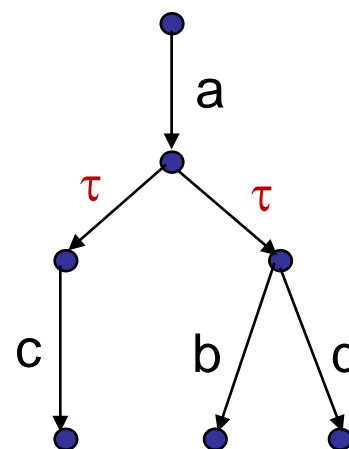
Befolyásoló tulajdonságok

- Az akciók megfigyelhetősége:
 - **Megfigyelhető akciók:** A vizsgált komponens (modul) interfészen megjelenő, a környezet számára **releváns** interakció
 - Pl. metódus hívása, hívás kiszolgálása; üzenet küldése, fogadása
 - **Nem megfigyelhető (belső) akciók:** Az interfészen nem megjelenő, vagy a környezet számára közvetlenül nem releváns viselkedés
 - Pl. belső vagy figyelmen kívül hagyható hívások, üzenetek
 - *Hatása* észlelhető a rákövetkező akciókon keresztül
 - Jelölése: i , vagy τ
- Nemdeterminizmus:
 - Egy állapotból több, azonosan címkézett átmenet
 - „Image finite system”: ezek száma véges
 - Absztrakt modellekben szokásos, finomítás során eltűnik
- Konkurens modellek szemantikája:
 - Átlapolódás (interleaving)
 - Valódi konkurencia (true concurrency)

Belső akciók (példa)



Komponens
belső viselkedés



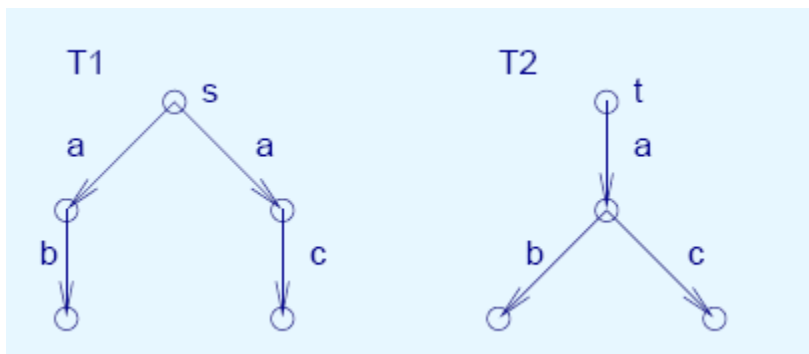
Megfigyelhető
viselkedés

„Tesztelés” és „holtpont” (deadlock) értelmezése

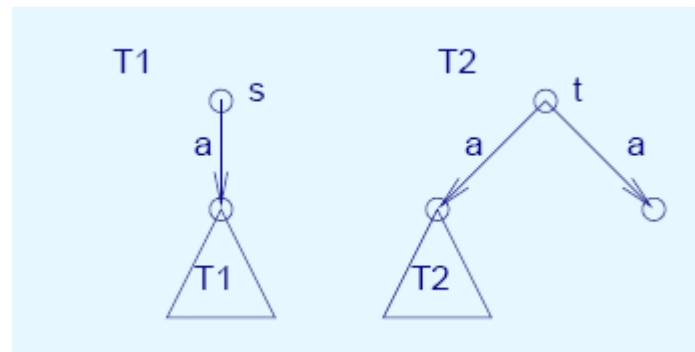
- „Tesztelés” értelmezése LTS-eken:
 - Rendszer mint fekete doboz, interfésszel (portok)
 - **Teszt lefutás:** Interakció a környezettel:
Szinkronizáció sorozat a portokon keresztül
 - Üzenet küldése és fogadása
 - Esemény kiváltása és annak feldolgozása
- „Holtpont” (deadlock) értelmezése:
 - A környezet egy interakciót indít,
de arra a rendszer **nem reagál** (interakció nem jön létre)
 - Üzenet küldése és fogadása nem történik meg
 - Esemény feldolgozása nem történik meg
 - **Teszt „hibázik”:** A kívánt interakció nem lehetséges
 - **Analógia:** Zongora reteszkelhető billentyűkkel
 - Sikeres teszt: Lejátszható dallam

Példák a holtpont értelmezésére

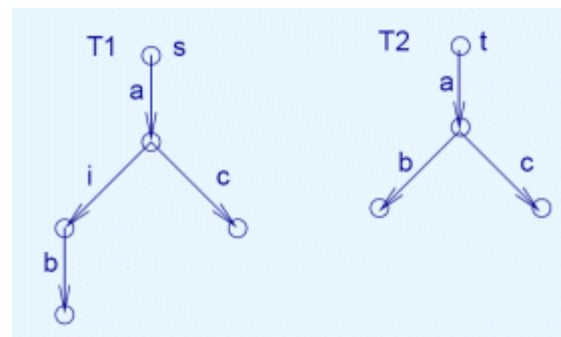
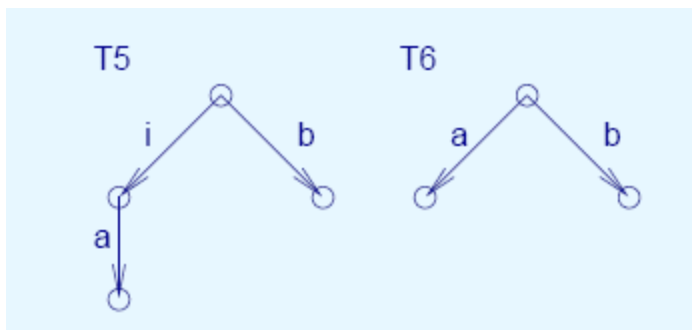
- T1 és T2 ekvivalenciája:



„Rekurzív” modell:



- Belső akció szerepe:



Ekvivalencia relációk

I. Trace ekvivalencia: Jelölések

- Minta: Automaták

$$A_1 = A_2 \text{ ha } L(A_1) = L(A_2)$$

- LTS-ek esetén:

- Minden állapot elfogadó állapot
- „Nyelv”: Minden lehetséges akciószekvencia (trace)

- Jelölések:

$\alpha = a_1 a_2 a_3 a_4 \dots a_n \in Act^*$ véges akciószekvencia (ε az üres)

$s \xrightarrow{\alpha} s'$ ha $\exists s_0 s_1 \dots s_n$ állapotsorozat ahol $s_0 = s$, $s_n = s'$, $s_i \xrightarrow{a_{i+1}} s_{i+1}$

$\alpha(s)$ egy erős trace s-ből, ha $\exists s' : s \xrightarrow{\alpha} s'$

$\Lambda(s)$ legyen s erős trace-einek halmaza: $\Lambda(s) = \left\{ \alpha \mid \exists s' : s \xrightarrow{\alpha} s' \right\}$

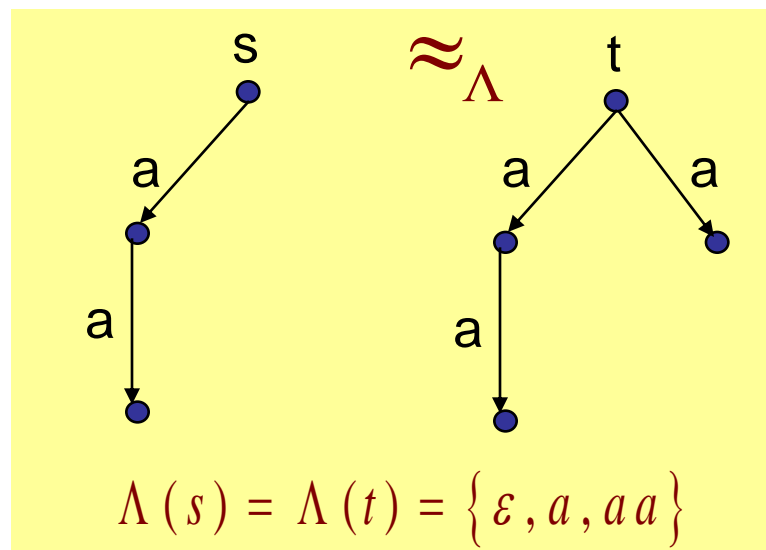
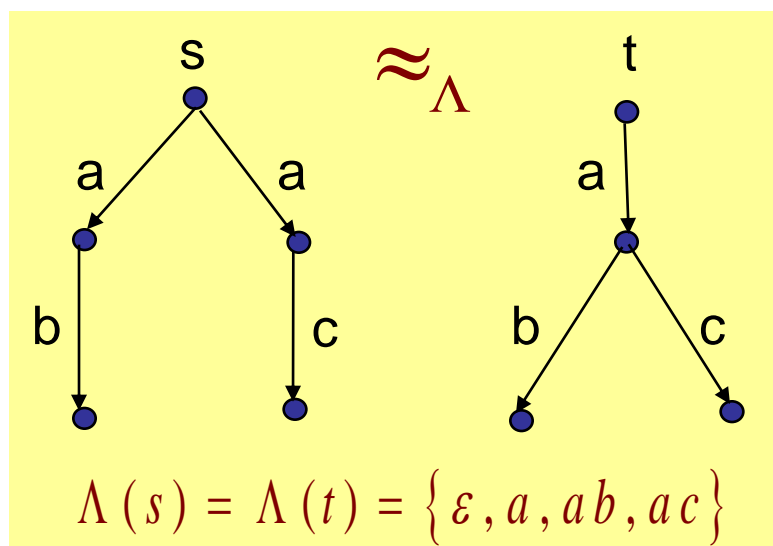
I. Trace ekvivalencia: Definíció és példák

- Legyen T_1 és T_2 két LTS, s_1 és s_2 kezdőállapottal

- Definíció:

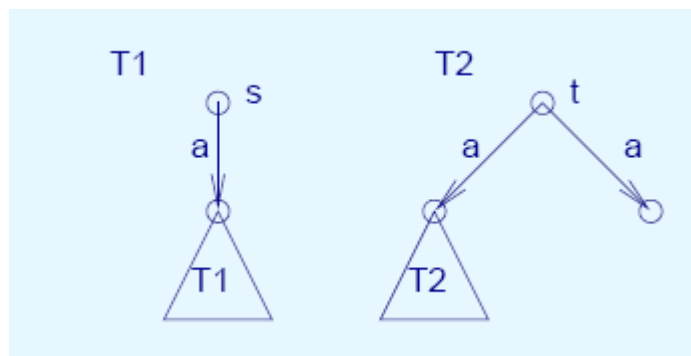
$$T_1 \approx_{\Lambda} T_2 \text{ a.c.s.a. } \Lambda(s_1) = \Lambda(s_2)$$

- Példák:



I. Trace ekvivalencia: Problémák

- Érzékenység a deadlock-ra
 - Ekvivalens LTS-ekre más-más deadlock viselkedés
 - Oka pl. a nemdeterminizmus
 - Azonos trace-ek, de különböző állapotokon keresztül



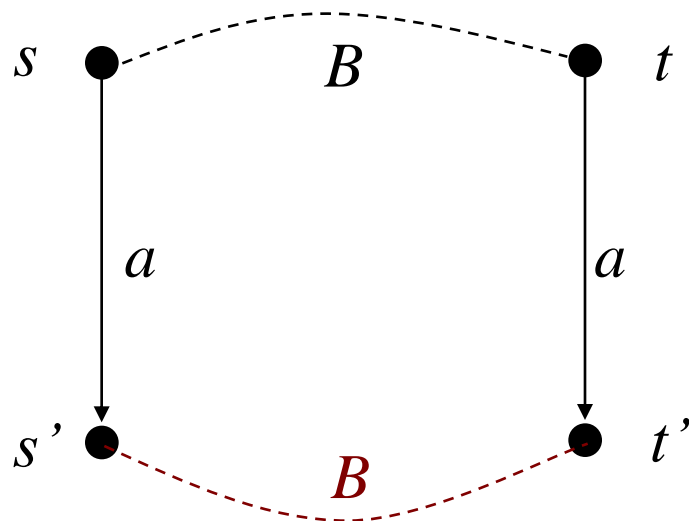
- Megoldás:
 - Ekvivalencia relációk, amelyek előírják **ekvivalens állapotok** bejárását

II. Erős biszimuláció ekvivalencia: Definíció

- Definíció:

$B \subseteq S \times S$ biszimuláció, ha minden $(s, t) \in B$ és bármely $a \in Act$, $s' \in S$ esetén fennáll:

- ha $s \xrightarrow{a} s'$ akkor $\exists t' : t \xrightarrow{a} t'$ és $(s', t') \in B$
- ha $t \xrightarrow{a} t'$ akkor $\exists s' : s \xrightarrow{a} s'$ és $(s', t') \in B$



II. Erős biszimuláció ekvivalencia: Tulajdonságok

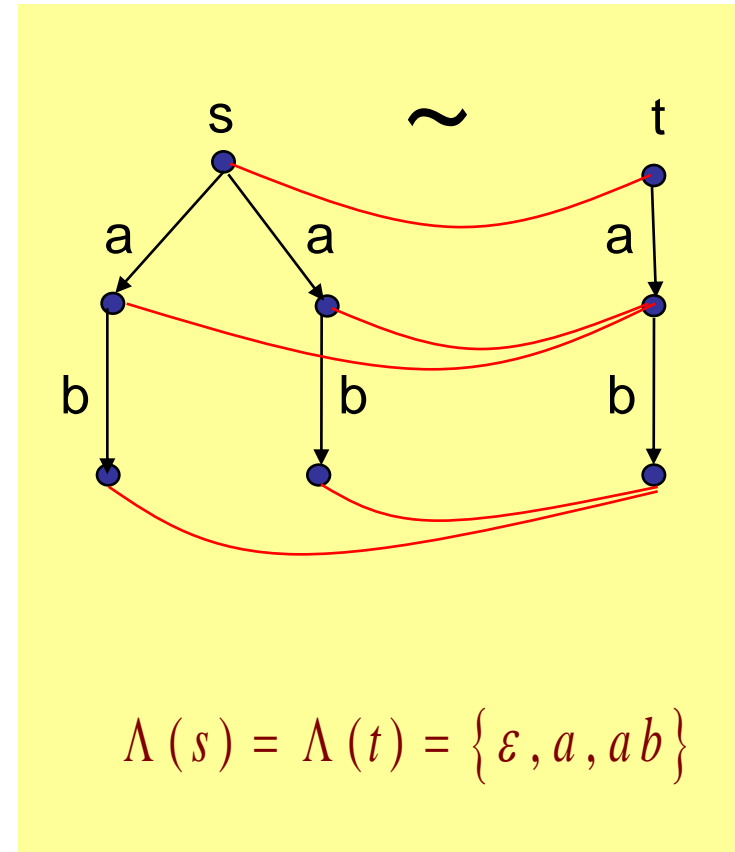
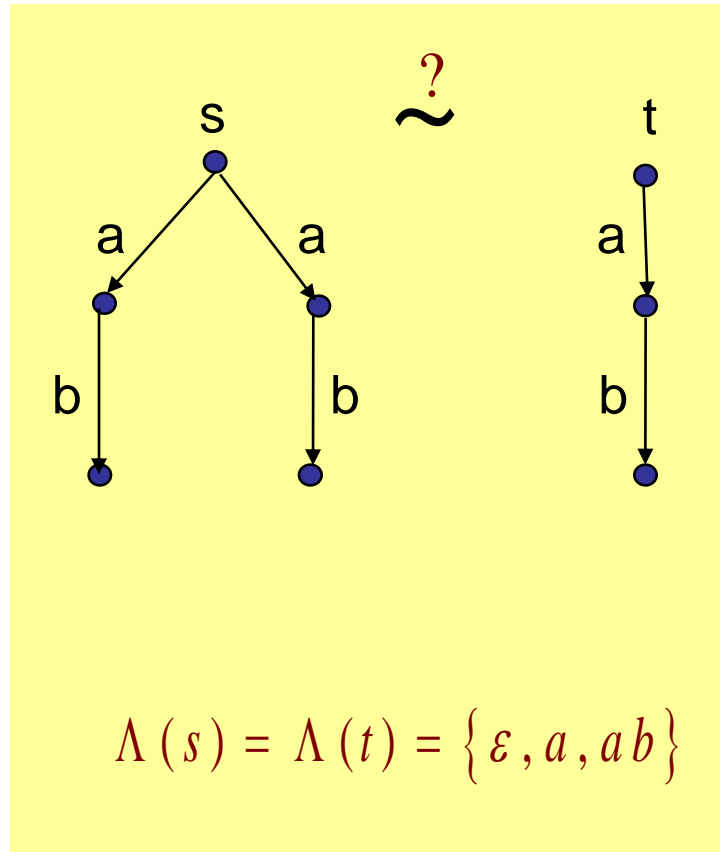
- Erős biszimuláció ekvivalencia:

$$T_1 \sim T_2 \text{ a.c.s.a. } s_1 \sim s_2 \text{ azaz } \exists B : (s_1, s_2) \in B$$

- Intuitív: Egymás viselkedését „szimulálják”
 - Ekvivalens állapotokban illeszkedő átmenetek
 - Azonos akciószekvenciák ekvivalens állapotokon át
- Kedvező tulajdonságok:
 - Erős biszimuláció következménye a trace ekvivalencia (determinisztikus LTS-re egybeesnek)
 - **Kongruencia** CCS LTS-ekre (fa, csúcsokhoz csatlakozás)
 - Erős biszimuláció ekvivalens rendszerek deadlock szempontjából azonosak (ha ez egyikben deadlock lehet, akkor a másikban is)

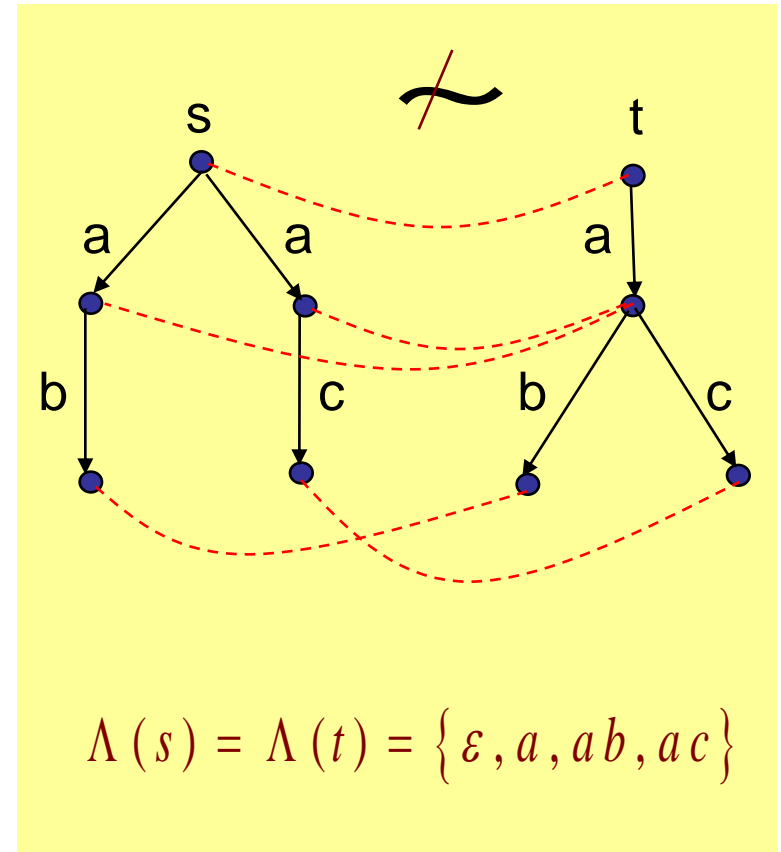
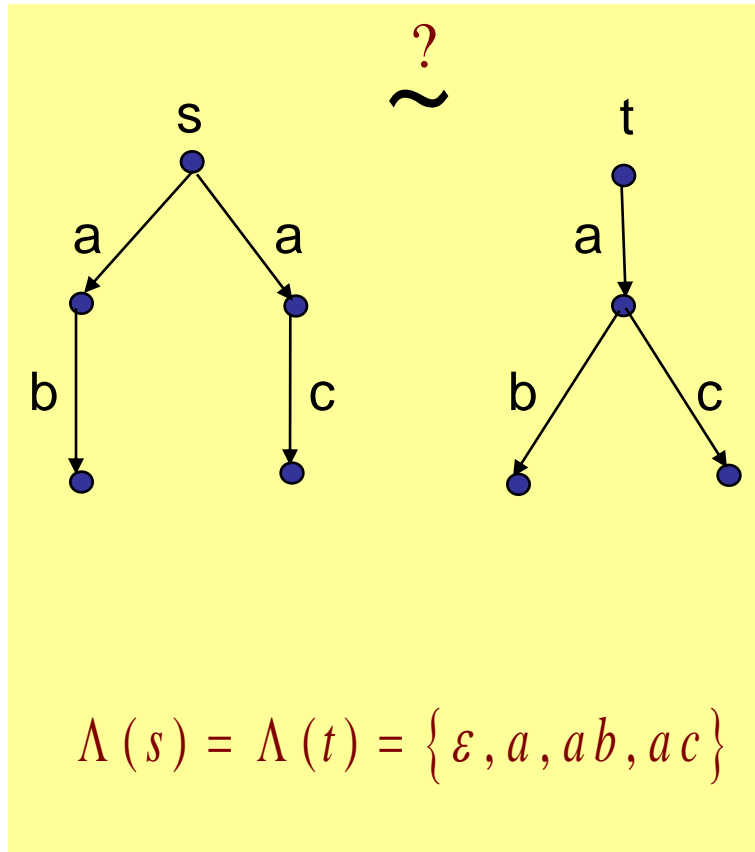
II. Erős biszimuláció ekvivalencia: Példák

- Példa:



II. Erős biszimuláció ekvivalencia: Példák

- Példa:

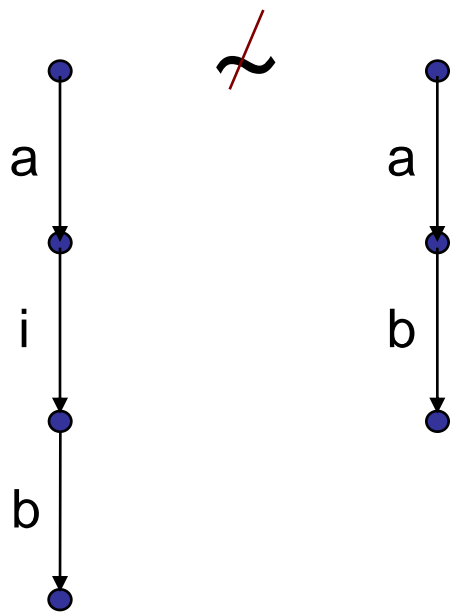


II. Erős biszimuláció: Deadlock formalizálása

- Deadlock lehetőség kifejezése a Hennessy-Milner logika segítségével:
 - Az a akcióra: $[a]\text{false}$
 - Ez csak akkor lehet igaz, ha nincs a -val címkézett átmenet, azaz a -ra deadlock van!
 - Egy akcióhalmazra: $\{[a_1]\text{false} \wedge [a_2]\text{false} \wedge \dots \wedge [a_n]\text{false}\}$
 - Egy elért állapotban: $\langle b_1 \rangle \dots \langle b_n \rangle \{[a_1]\text{false} \wedge \dots \wedge [a_2]\text{false}\}$
- Tétel: LTS-ekben $T_1 \sim T_2$ a.cs.a., ha minden p HML kifejezésre
 - vagy $T_1, s_1 \models p$ és $T_2, s_2 \models p$,
 - vagy $T_1, s_1 \not\models p$ és $T_2, s_2 \not\models p$

II. Erős biszimuláció ekvivalencia: Problémák

- Érzékenység a megfigyelhető hatás nélküli belső átmenetekre:
 - Nincs megfigyelhető hatás, ha a végrehajtás nem befolyásolja a további viselkedést (deadlock-ot)
 - Egyszerű példa:



III. Gyenge biszimuláció ekvivalencia: Jelölések

- Az erős biszimuláció „gyenge” változata
 - Nem érzékeny a megfigyelhető hatás nélküli belső átmenetekre
 - Lényege: Azonos megfigyelhető akciószekvenciák ekvivalens állapotokon keresztül
- Jelölések:

$\alpha \in Act^*$ véges akciószekvencia (ε az üres)

$\hat{\alpha} \in (Act - \tau)^*$ megfigyelhető akciószekvencia (τ törlése)

itt $\hat{\alpha} = \varepsilon$ ha $\alpha = \tau$

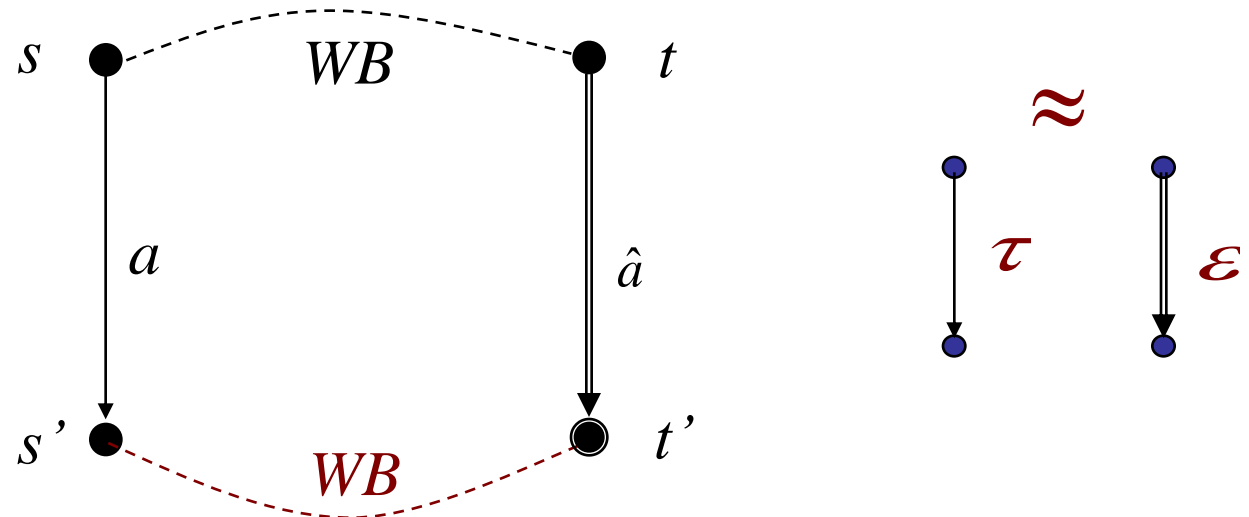
$s \xRightarrow{\beta} s'$ ha $\exists \alpha: s \xrightarrow{\alpha} s'$ és $\beta = \hat{\alpha}$

III. Gyenge biszimuláció ekvivalencia: Definíció

- Definíció:

$WB \subseteq S \times S$ gyenge biszimuláció, ha minden $(s, t) \in WB$ és bármely $a \in Act$, $s', t' \in S$ esetén fennáll:

- ha $s \xrightarrow{a} s'$ akkor $\exists t' : t \xRightarrow{\hat{a}} t'$ és $(s', t') \in WB$
- ha $t \xrightarrow{a} t'$ akkor $\exists s' : s \xRightarrow{\hat{a}} s'$ és $(s', t') \in WB$

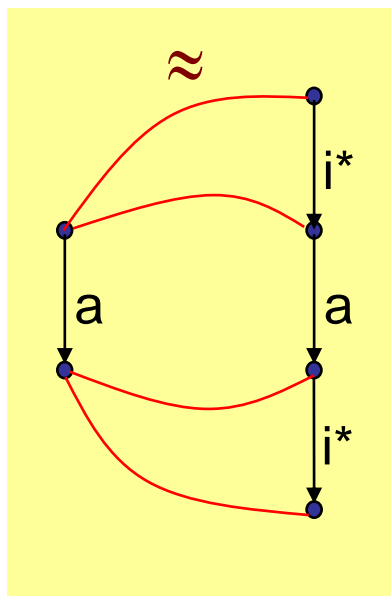
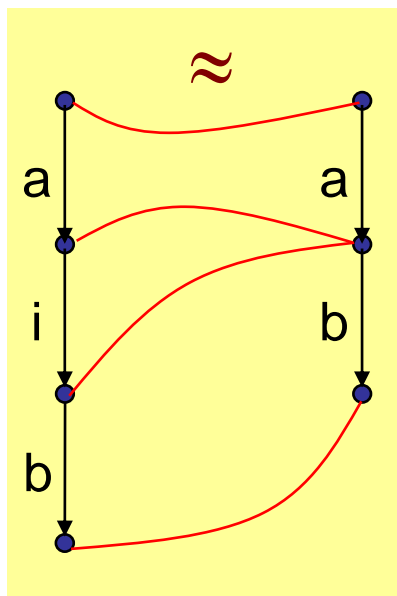


III. Gyenge biszimuláció ekvivalencia: Példák

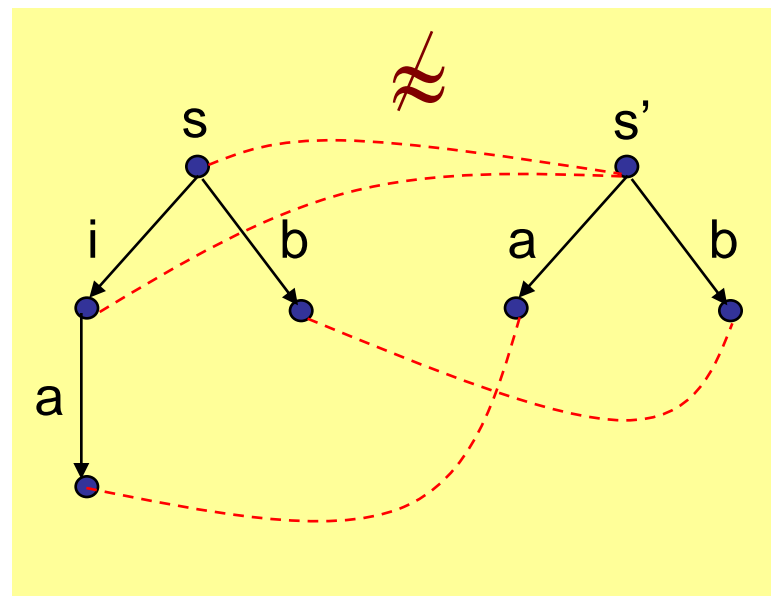
- Gyenge biszimuláció ekvivalencia
= Megfigyelési ekvivalencia (observation equiv.)

$$T_1 \approx T_2 \text{ a.c.s.a. } s_1 \approx s_2 \text{ azaz } \exists WB : (s_1, s_2) \in WB$$

- Példák:



Hatással járó belső tranzíció:



III. Gyenge biszimuláció: Deadlock formalizálás

- HML variáns megfigyelhető akciókra:

$HML^* ::= true \mid false \mid p \wedge q \mid p \vee q \mid [[a]]p \mid \langle\langle a \rangle\rangle p$

- Szemantika:

– **H3***: $T, s \models [[a]]p \quad \text{a.cs.a.} \quad \forall s' \text{ ahol } s \Rightarrow^a s': s' \models p$

– **H4***: $T, s \models \langle\langle a \rangle\rangle p \quad \text{a.cs.a.} \quad \exists s': s \Rightarrow^a s' \text{ és } s' \models p$

- Tétel: LTS-ekben $T_1 \approx T_2$ a.cs.a.

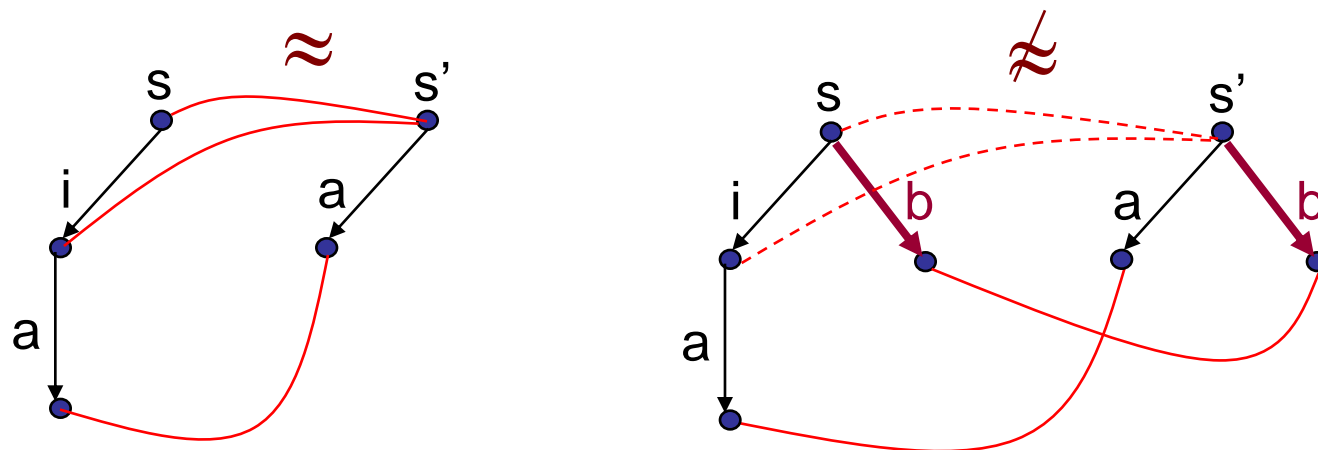
ha minden p HML^* kifejezésre

– vagy $T_1, s_1 \models p$ és $T_2, s_2 \models p$

– vagy $T_1, s_1 \not\models p$ és $T_2, s_2 \not\models p$

III. Gyenge biszimuláció ekvivalencia: Tulajdonságok

- Nem kongruencia CCS LTS-re (ellenpélda van)



- Érdekesség: Legmegengedőbb kongruencia reláció, amiből következik a gyenge biszimuláció ekvivalencia:

$s \approx^c t$, ha bármely $a \in Act$, $s', t' \in S$ esetén fennáll:

- ha $s \xrightarrow{a} s'$ akkor $\exists t': t \Rightarrow t'$ és $s' \approx t'$

- ha $t \xrightarrow{a} t'$ akkor $\exists s': s \Rightarrow s'$ és $s' \approx t'$

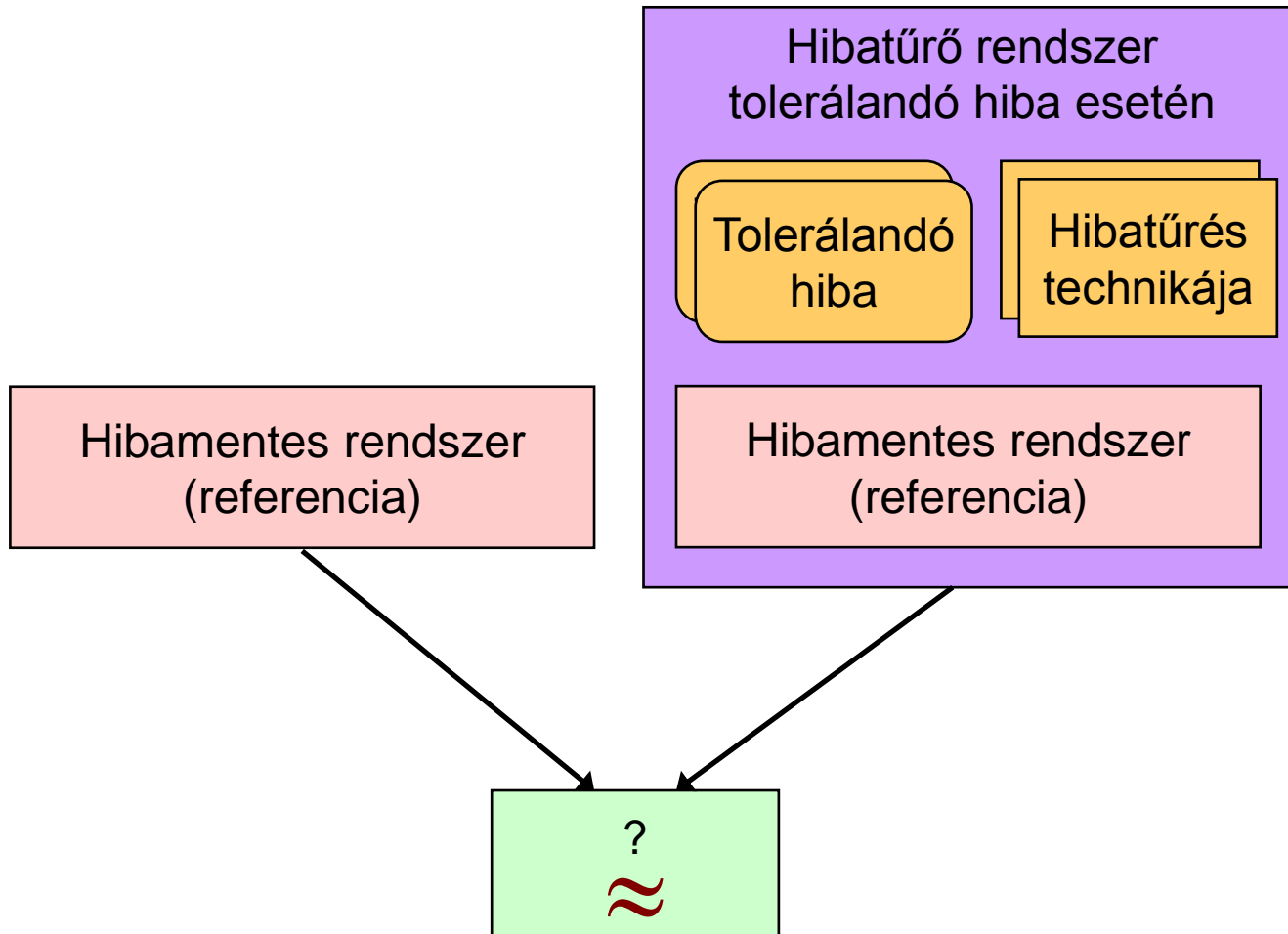
Ekvivalencia relációk számítási módszere

Partíció finomítás

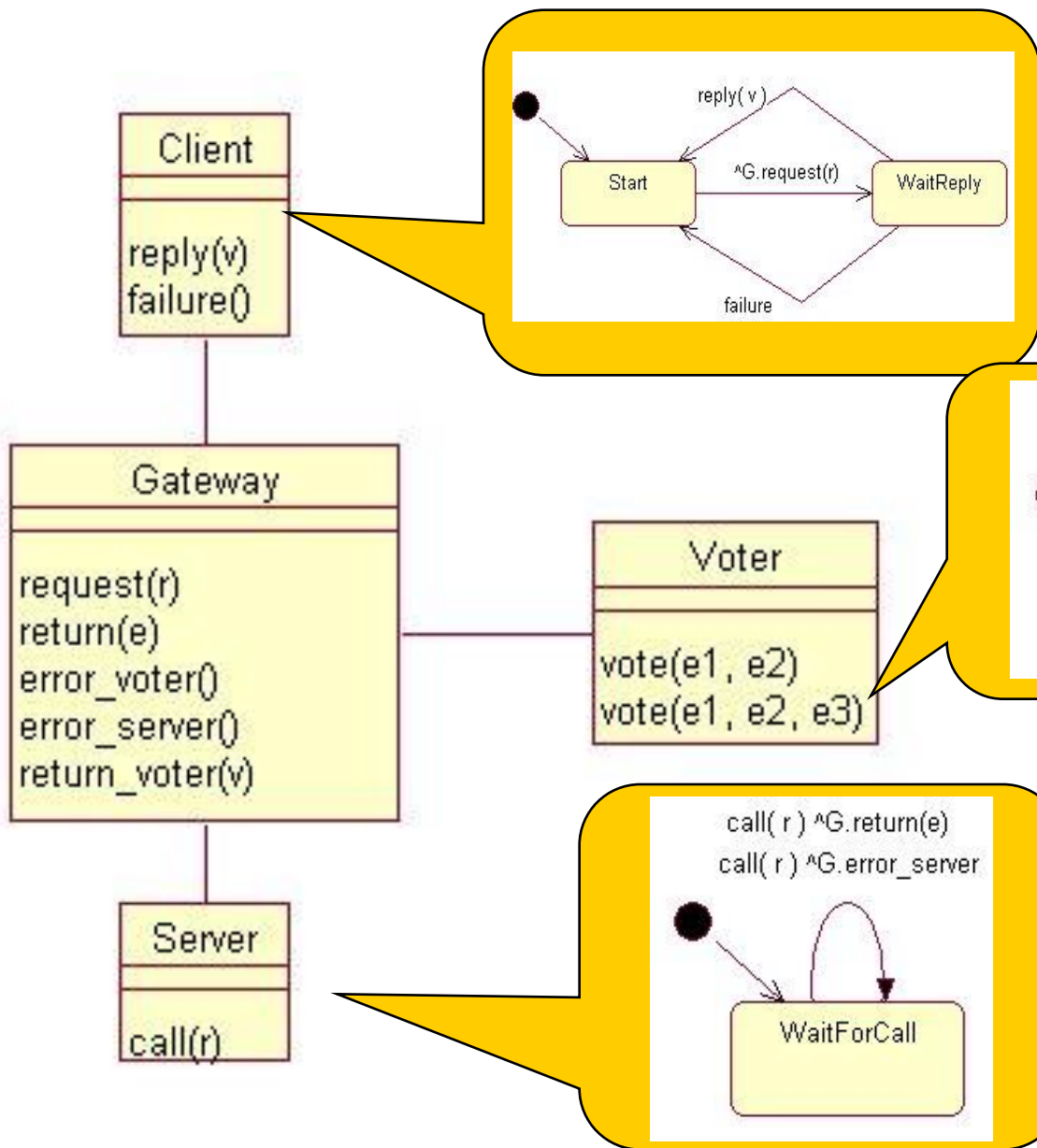
1. Kezdetben minden állapotpár eleme a relációnak
Egy partíciót (ekvivalencia osztályt) képeznek
2. Minden állapotpárra:
Ha az egyikből indulva van olyan átmenet,
ami a másiktól indulva a definíció szerint nem szimulálható, akkor
 - Az adott állapotpár kizárása (nem ekvivalensek);
 - A következmények végigvezetése a bejövő átmenetek végein lévő állapotokra
 - Hiszen nem ekvivalensek, ha nem ekvivalens állapotokba kerülnek
3. Ha már nincs változás (fixpont):
Végleges ekvivalencia osztályok adódtak
Ha a kezdőállapotok azonos ekvivalencia osztályban vannak,
akkor az LTS-ek ekvivalensek

Esettanulmány:
**Hibatűrés ellenőrzése megfigyelési
ekvivalencia reláció használatával**

Mintapélda: Hibatűrés verifikációja



Rendszerarchitektúra



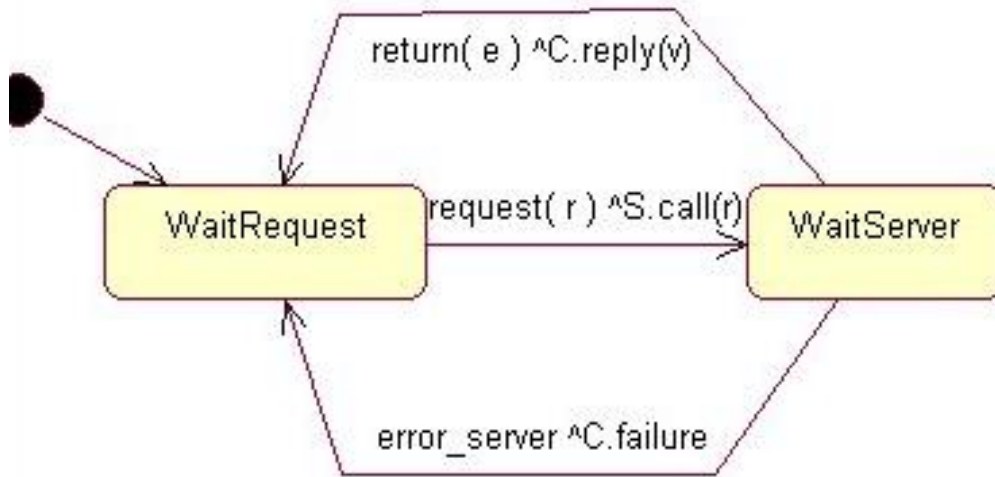
Hibamodell: Szerver által adott válasz **adathibája**

Hibatűrés: Szavazás és alternatív szerver

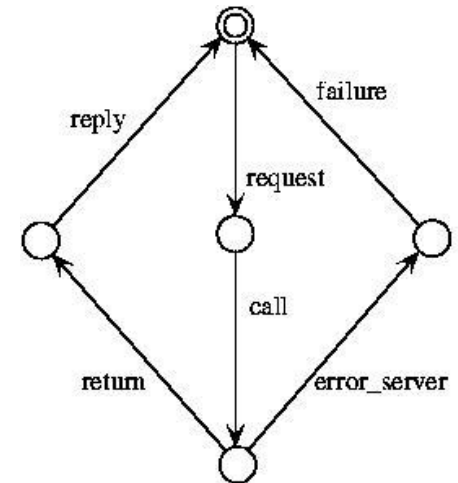
Ellenőrzés a kliens szempontjából:
Gateway viselkedése megfigyelhető

A Gateway komponens hibatűrés nélküli viselkedése

- Állapotdiagram:



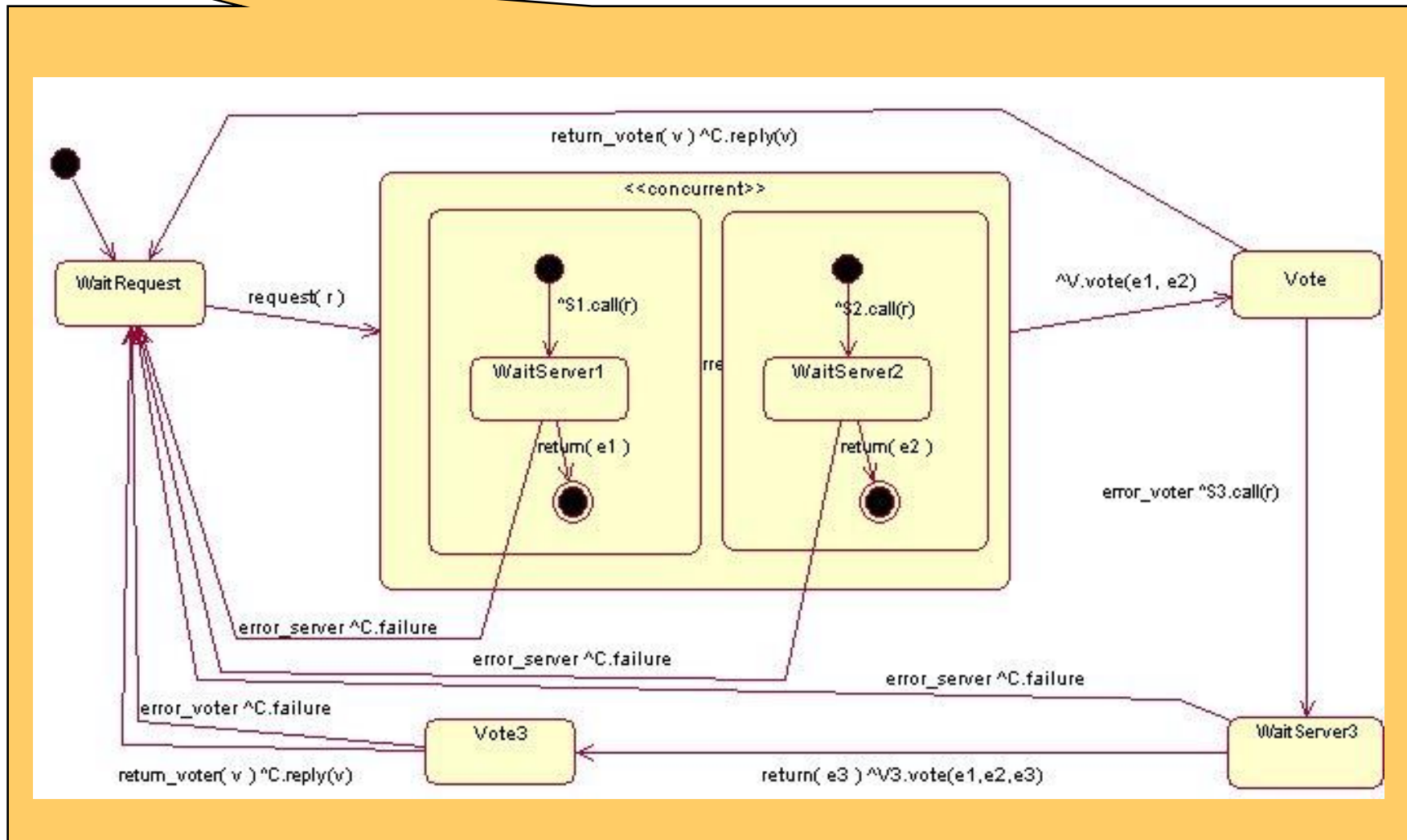
- LTS megfelelője:



A Gateway komponens hibatűrés esetén

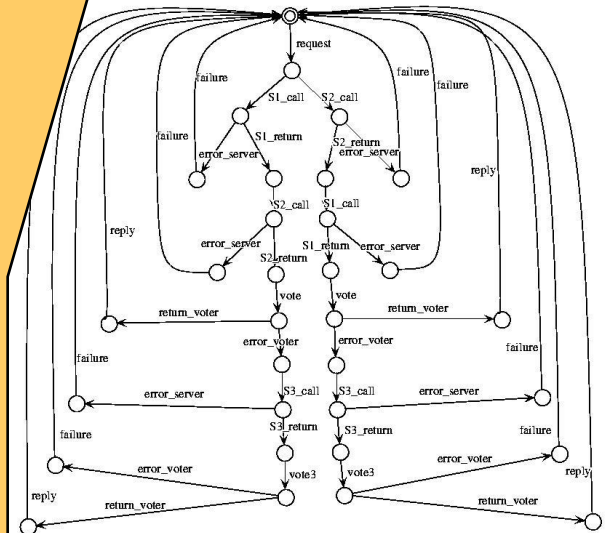
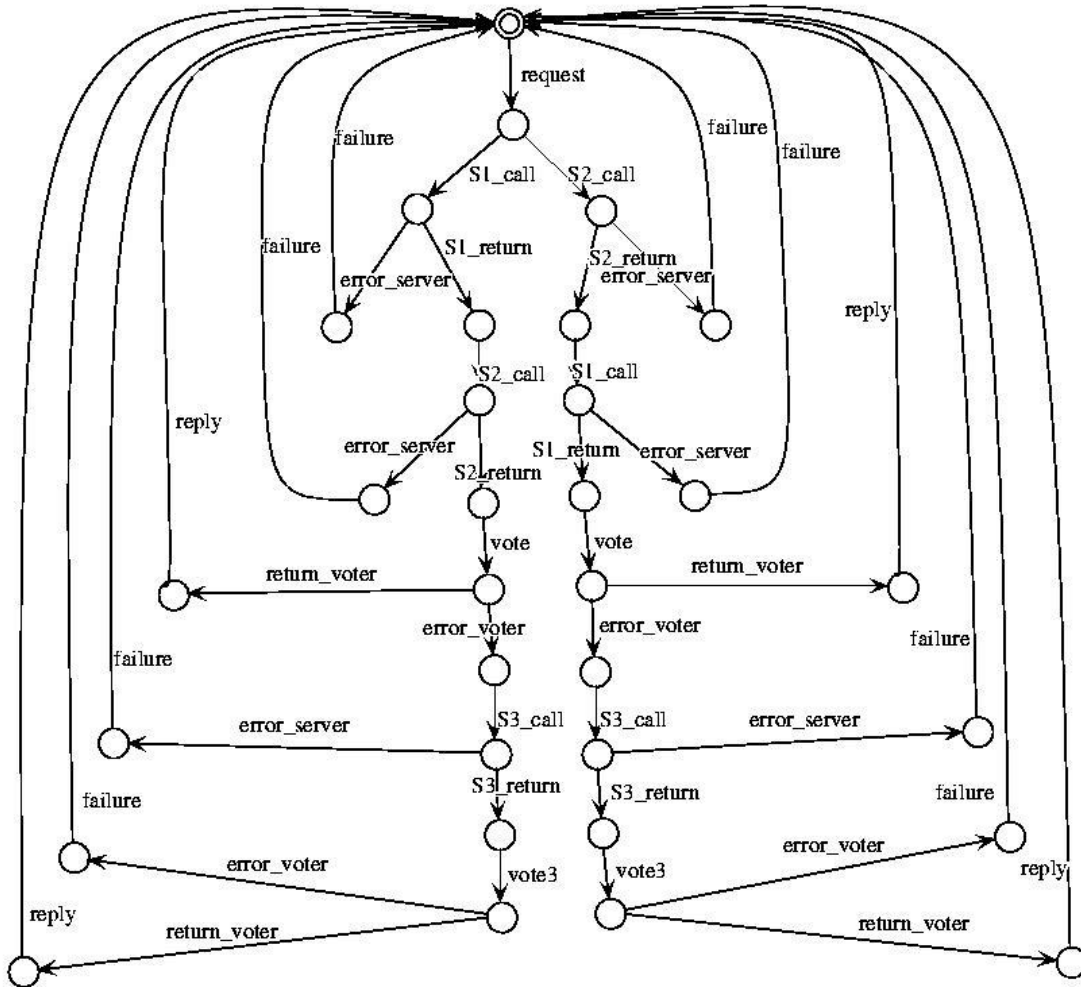
- Állapotdiagram:

- LTS megfelelője:

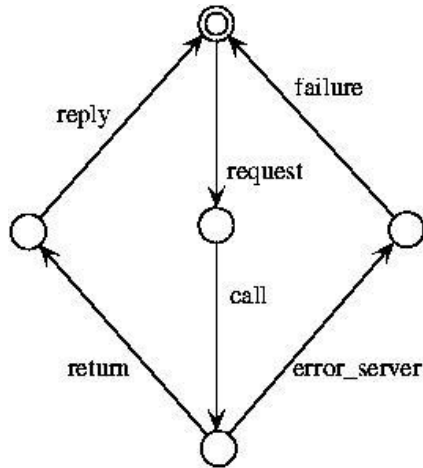


A Gateway komponens hibatűrés esetén

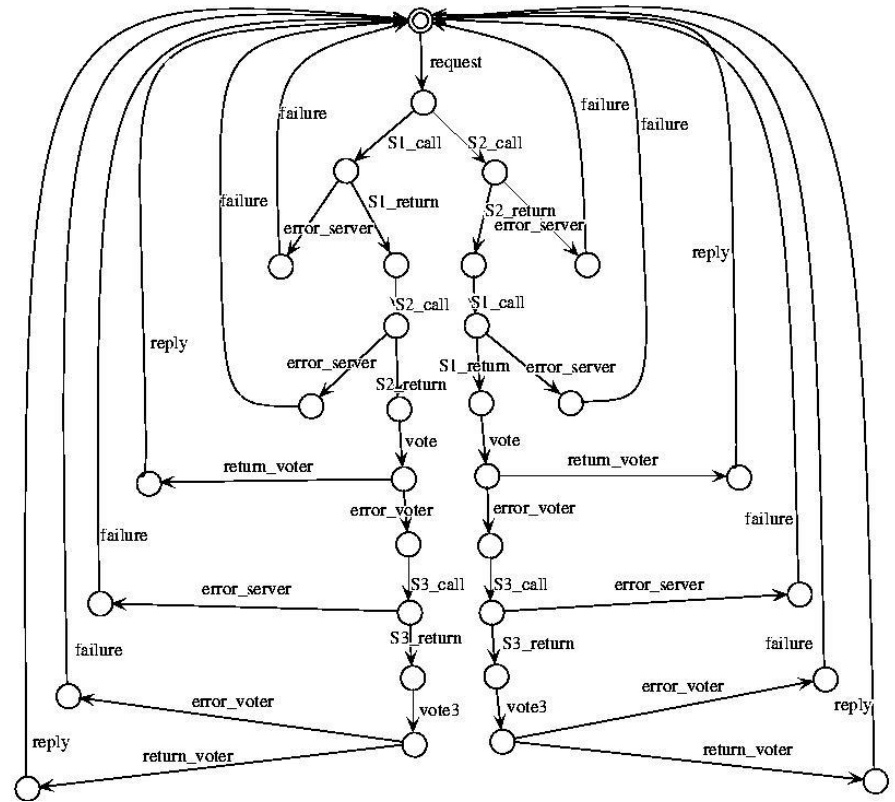
LTS megfelelője:



Viselkedési ekvivalencia igazolása



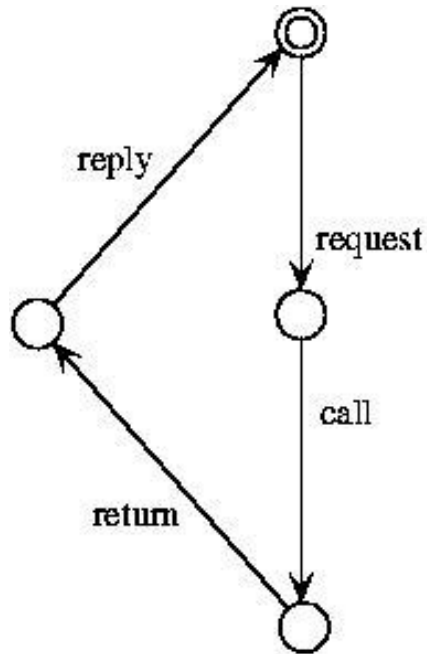
Gateway
referencia
viselkedés



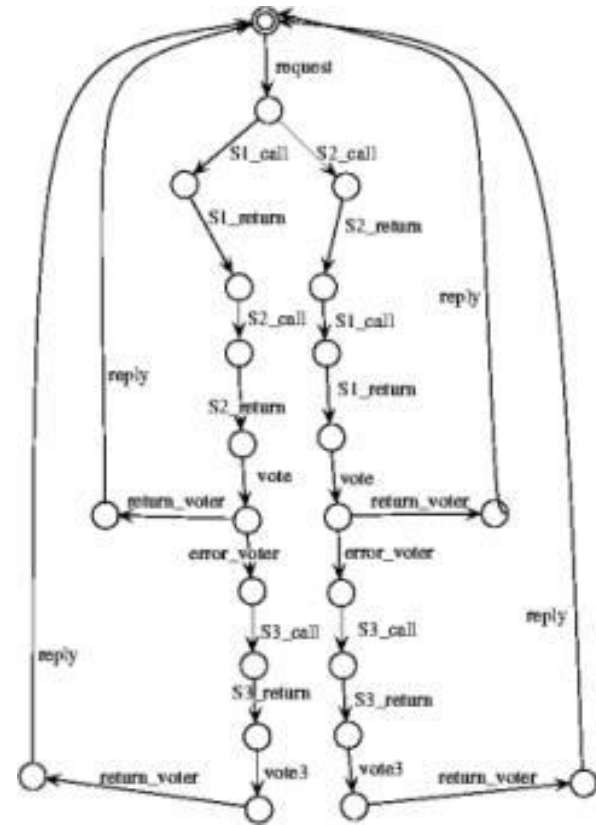
Így igazolható, hogy a
kliens számára
transzparens a hibatűrő
mechanizmus működése.

Hibatűrő Gateway teljes viselkedése;
Itt minden olyan akció τ lesz,
ami nincs a referencia viselkedésben!

Hibatűrés igazolása az első szerver hibája esetén



Hibamentes
Gateway



Hibatűrő Gateway a hiba esetén;
Itt minden olyan akció τ lesz,
ami nincs a referencia viselkedésben

Az adott hiba esetén a kliens
szempontjából megvalósul a
hibatűrés.