Modellek viselkedési ekvivalenciájának és finomításának ellenőrzése

dr. Majzik István
BME Méréstechnika és Információs Rendszerek Tanszék

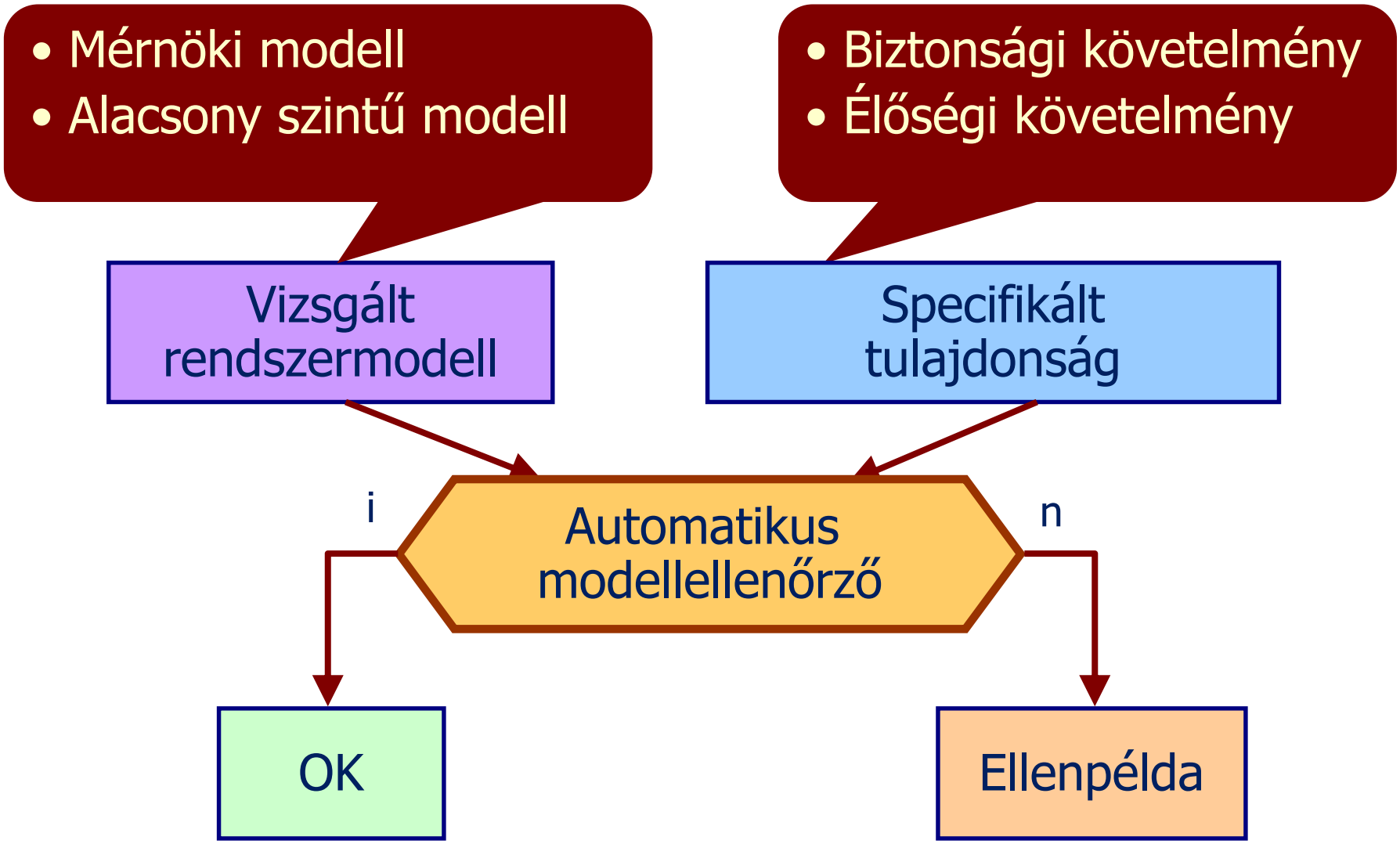
Ismétlés: A formális modellek használata

Formális módszerek része:

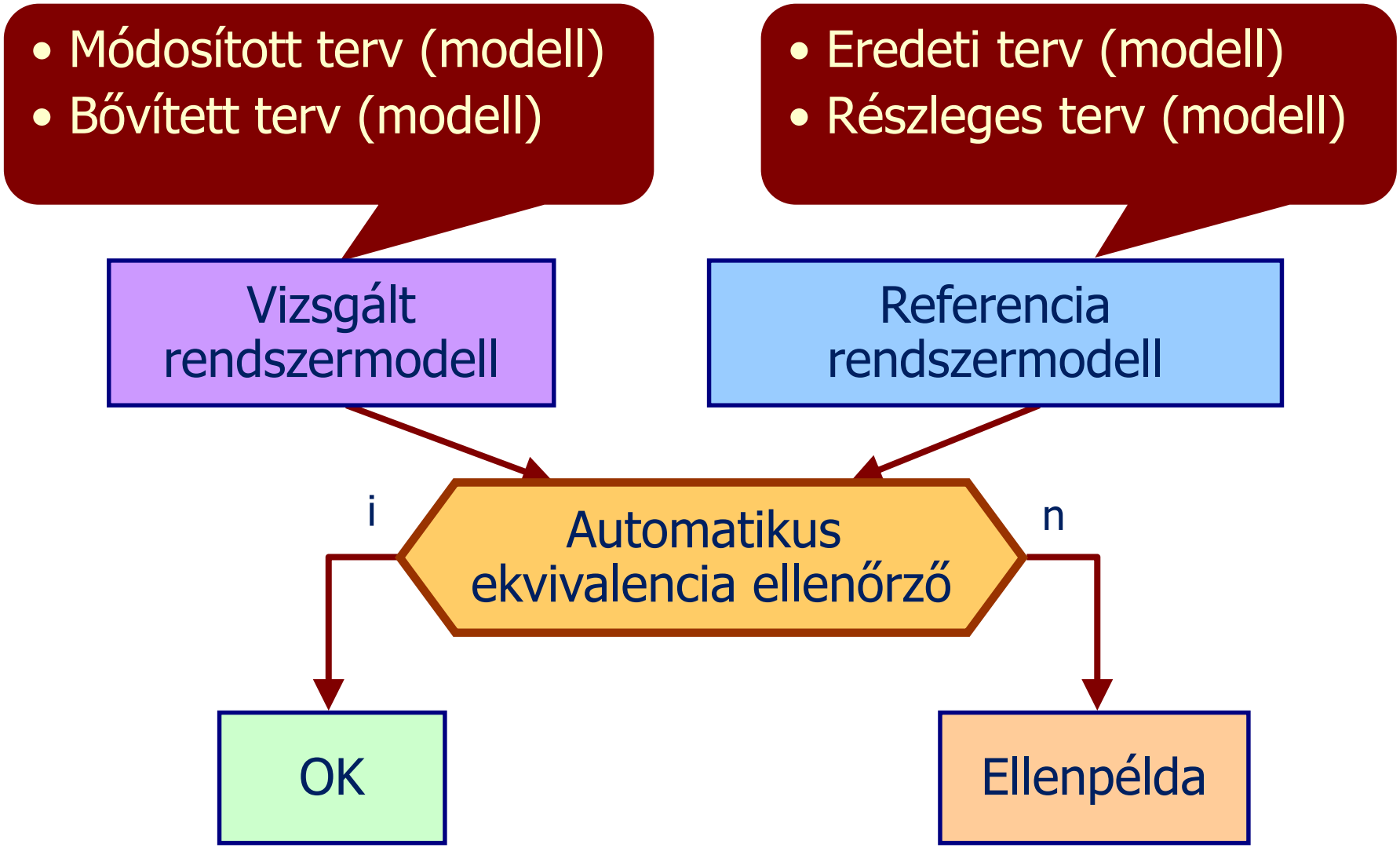
A formális modellről ismeretet adó (matematikai) eljárás

- A formális modell végrehajtása
  - Szimuláció
- A formális modell ellenőrzése: Formális verifikáció
  - „Önmagában való” vizsgálat
    - Konzisztencia, ellentmondás-mentesség
    - Teljesség, zártság
  - „Megfelelés” vizsgálata
    - Modellek és elvárt tulajdonságok között (terv ↔ specifikáció)
    - Modellek között (eredeti terv ↔ módosított terv)
- A formális modell alapján történő szintézis:
  - Szoftver (programkód, konfiguráció) generálása
  - Hardver implementáció generálása

Ismétlés: Modellellenőrzés



Modellek ekvivalenciájának ellenőrzése



Használat: Tervezői döntések ellenőrzése

- Ekvivalencia (megfelelőség) modellek között:

  Módosított modell ↔ Referencia modell

  Megvalósítás (konkrét) ↔ Specifikáció (absztrakt)

  Nyújtott viselkedés ↔ Elvárt viselkedés (protokollban)

  Hibatűrő rendszer hiba mellett ↔ Hibamentes rendszer

- Rendezés (finomítás) modellek között:
  - Referencia viselkedés megtartása, meghatározott bővítésekkel
  - Nemdeterminizmus csökkentése a viselkedésben

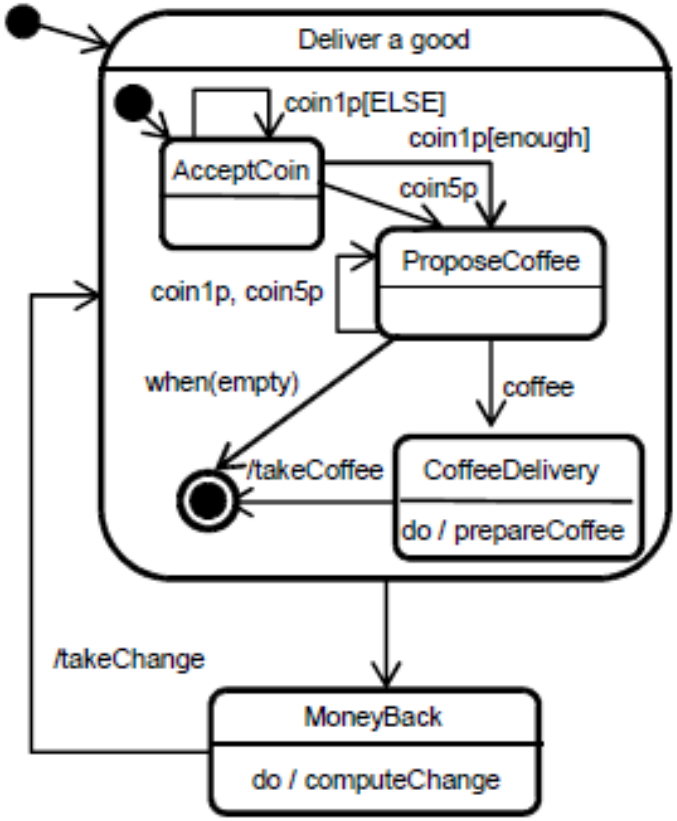
Használt matematikai relációk modellek között:

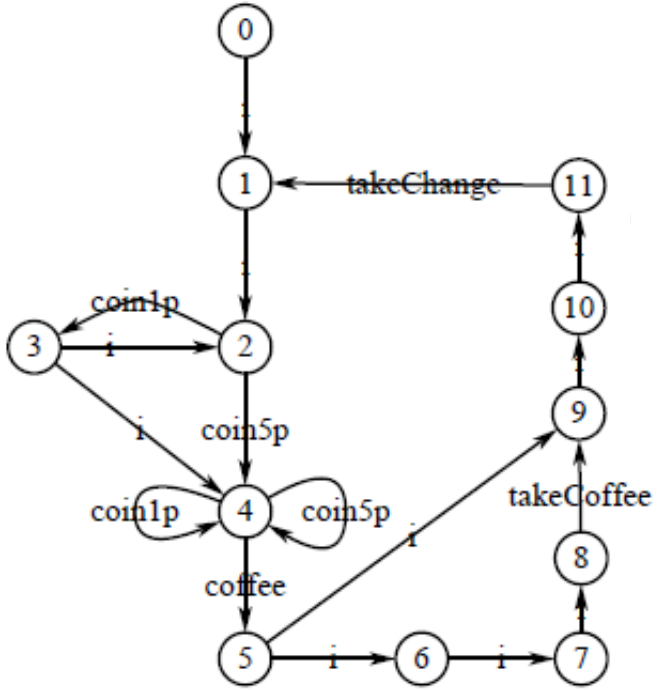
- Ekvivalencia: Reflexív, tranzitív, szimmetrikus
- Rendezés: Reflexív, tranzitív, antiszimmetrikus

Egy kétváltozós relációt akkor nevezünk antiszimmetrikusnak adott halmazon, ha a halmaz bármely két olyan a és b elemére, amelyre fennáll egyszerre, hogy a relációban áll b-vel és b relációban áll a-val, akkor az a és b azonos.

Viselkedési ekvivalencia relációk definiálása

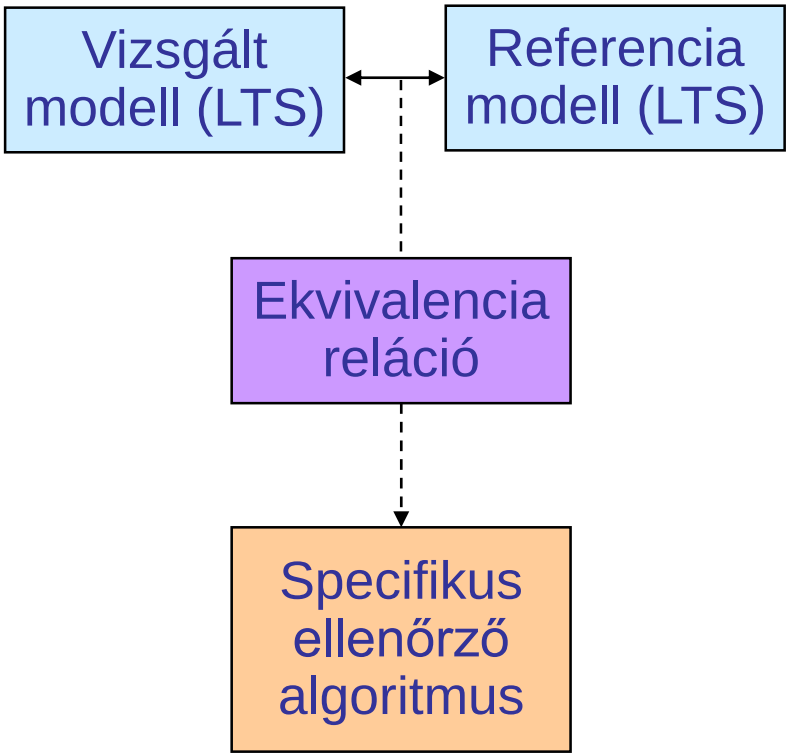
- Alacsonyszintű modell: LTS = (S, Act, →)
  - LTS modellek az állapottérképekből is származtathatók
  - Akciók átnevezése, elrejtése szükséges lehet



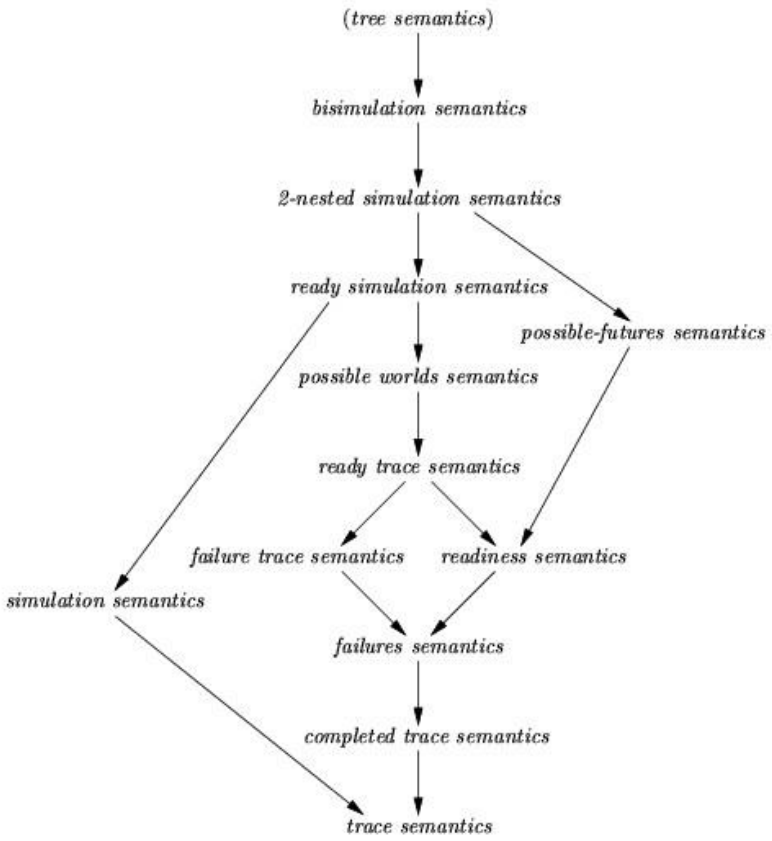


Az ekvivalencia ellenőrzés formalizálása

Ekvivalencia ellenőrzés:



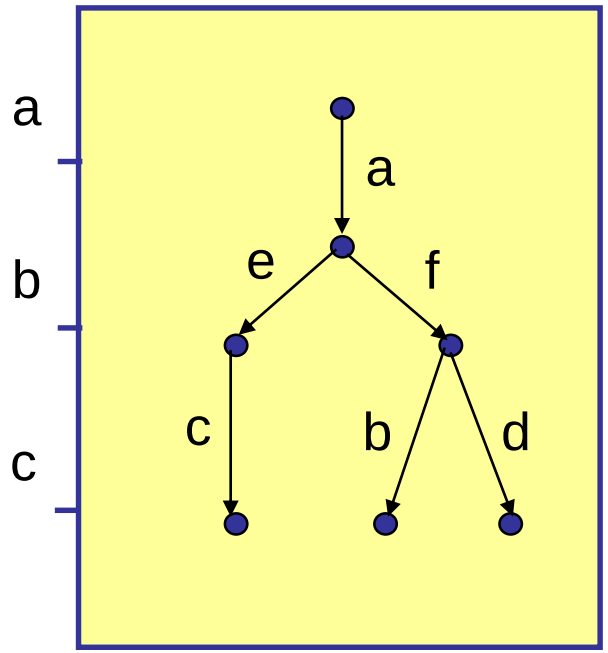
Ekvivalencia relációk:

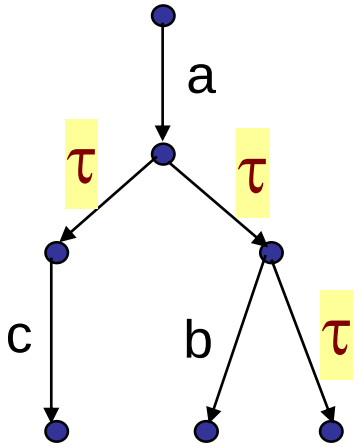


A komponensek megfigyelhető viselkedése

- Megfigyelhető akciók
  - A vizsgált komponens (modul) interfészén megjelenő, a környezet számára érdekes (releváns) viselkedés
    - Metódus hívása, metódushívás fogadása
    - Üzenet küldése, üzenet fogadása
- Nem megfigyelhető belső akciók (τ, i)
  - Az interfészen nem megjelenő, vagy a környezet számára nem érdekes (nem releváns) viselkedés
    - Belső működés (pl. belső metódusok, aktivitások)
    - Figyelmen kívül hagyható hívások, üzenetek
- Nemdeterminizmus
  - Egy állapotból több átmenet indul azonos akcióval
  - Nem megfigyelhető belső akció, mint alternatíva

Megfigyelhető viselkedés





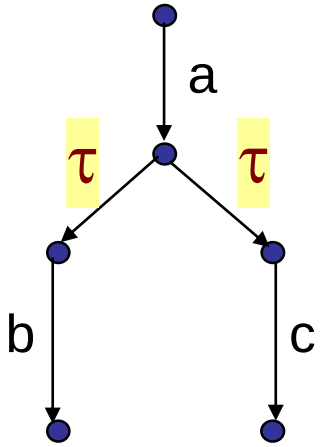
Komponens belső viselkedés: a,b,c,d,e,f akciók

Komponens interfész: a,b,c akciók

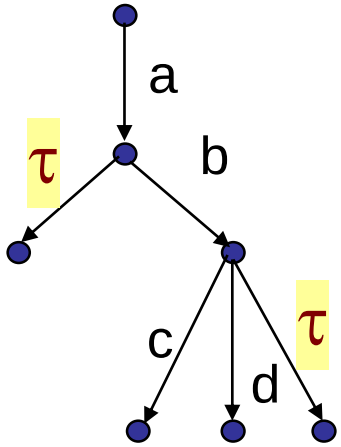
Megfigyelhető viselkedés modellje: a,b,c akciók és τ

Belső akció hatása a megfigyelhető akciókra

Példa: Az akciók üzenetek fogadását modellezik.



Az a üzenet fogadása után a belső működéstől függ, hogy b vagy c üzenet fogadása következhet.



Az a üzenet fogadása után a belső működéstől függően megállás következhet; ugyanígy az a és b után is.

Viselkedési ekvivalencia relációk

Trace ekvivalencia: Jelölések

- Minta: Automaták ekvivalenciája az elfogadott nyelvek alapján

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

- LTS-ek esetén analógia:
  - Minden állapot „elfogadó állapot”
  - Nyelv: Minden akciószekvencia (trace), ami elfogadó állapotba vezet
- Jelölések:

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

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

$\Lambda(s)$ egy s állapotból induló trace-ek halmaza: $\Lambda(s) = \left\{ \alpha \mid \exists s' : s \xrightarrow{\alpha} s' \right\}$

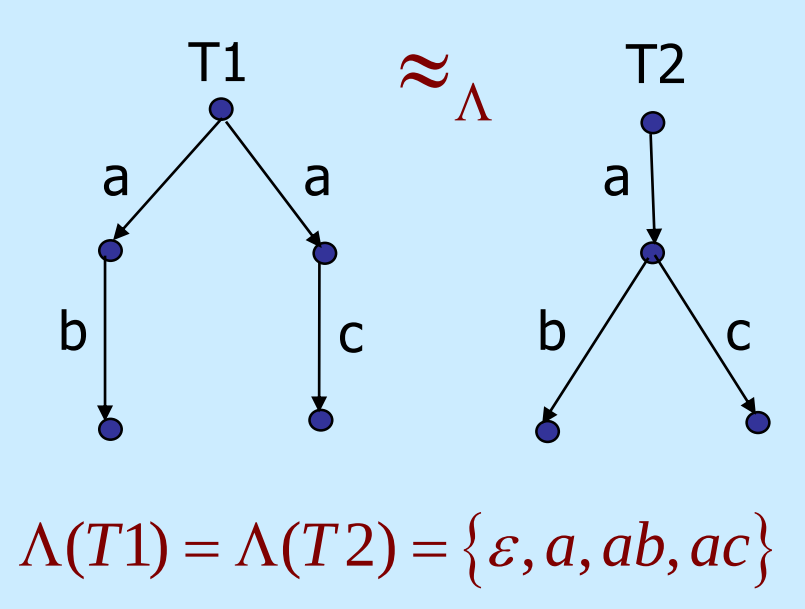
$\Lambda(T)$ egy s kezdőállapotú T LTS trace-einek halmaza: $\Lambda(T) = \Lambda(s)$

Trace ekvivalencia: Definíció és példák

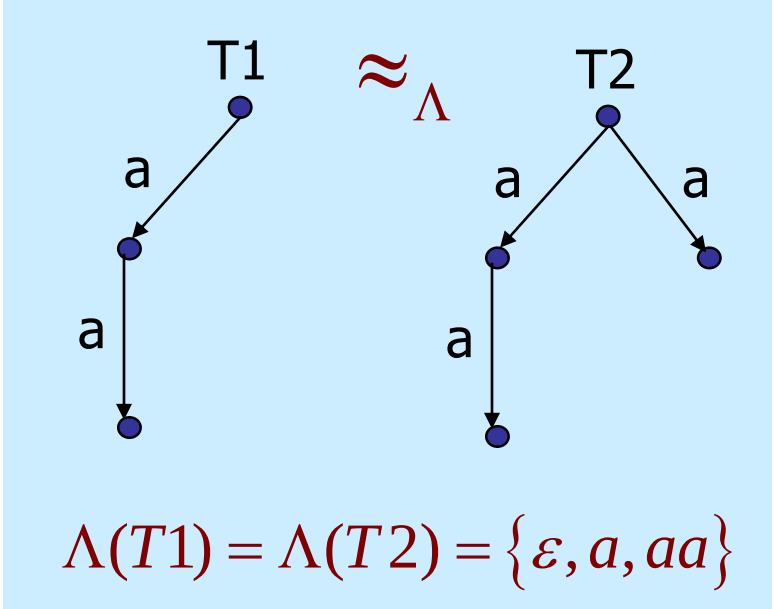
- Legyen T_1 és T_2 két LTS, s_1 és s_2 kezdőállapottal
- Definíció:

$$T_1 \approx_\Lambda T_2 \quad \text{a.cs.a.} \quad \Lambda(T_1) = \Lambda(T_2) \text{ azaz } \Lambda(s_1) = \Lambda(s_2)$$

- Példák:



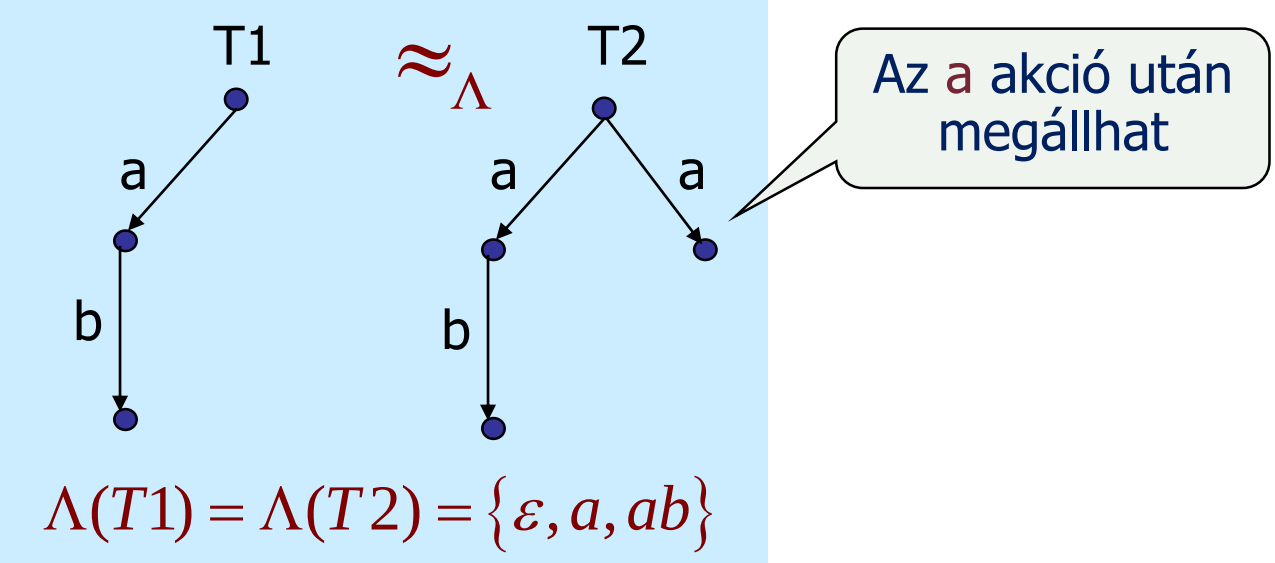
$$\Lambda(T1) = \Lambda(T2) = \{\varepsilon, a, ab, ac\}$$



$$\Lambda(T1) = \Lambda(T2) = \{\varepsilon, a, aa\}$$

A trace ekvivalencia hátrányai

- Nem érzékeny a lehetséges megállásra
  - Trace ekvivalens LTS-ek különbözőképpen viselkedhetnek megállás szempontjából (pl. nemdeterminizmus miatt)



- Megoldás:
  - Azt is figyelni kell, hogy az azonos trace által elért állapotok azonos folytatásra adnak-e lehetőséget

Biszimuláció ekvivalenciák

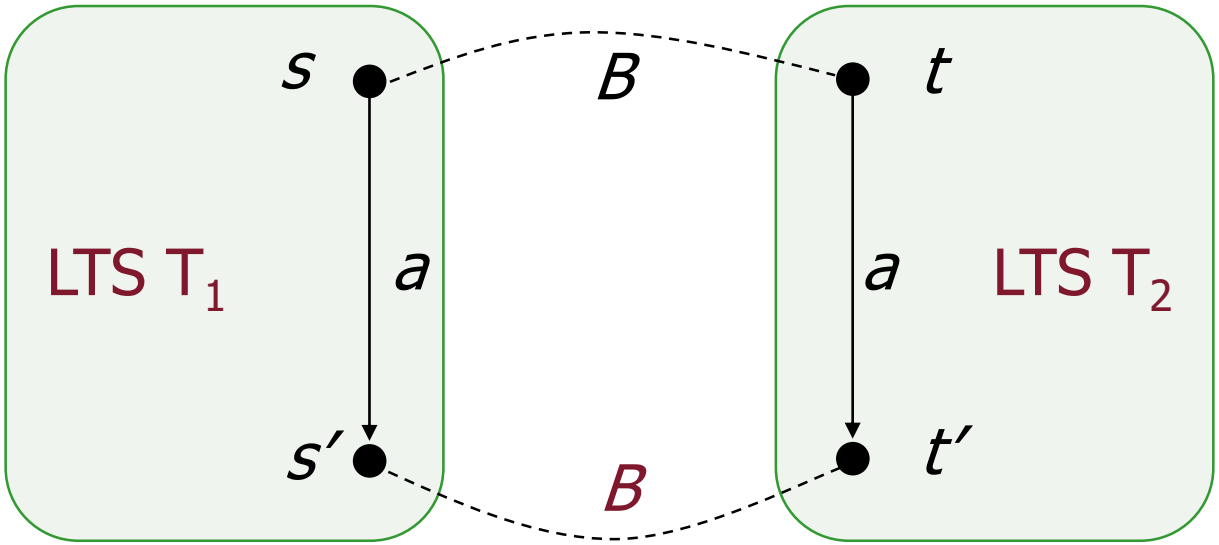
- Informális definíció: Két LTS biszimuláció ekvivalens, ha kölcsönösen szimulálni tudják egymás akciósorozatait ekvivalens állapotokon keresztül
  - Szimuláció adott állapotokból: Azonos akciók végrehajtása
    - Ha az egyik LTS képes egy adott akcióra, akkor a szimuláló LTS is
  - Ekvivalens állapotok: Innen indulva egymást szimulálni tudják, azaz azonos akciókra képesek
- Két biszimuláció reláció
  - Erős biszimuláció: Azonos módon kezeli a megfigyelhető és a nem megfigyelhető akciókat is
  - Gyenge biszimuláció (megfigyelési ekvivalencia): Nem érzékeny a hatás nélküli nem megfigyelhető akciókra

Erős biszimuláció reláció állapotok között

- Definíció az LTS-ek állapotpárjaira:

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

  - 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 $(s',t') \in B$

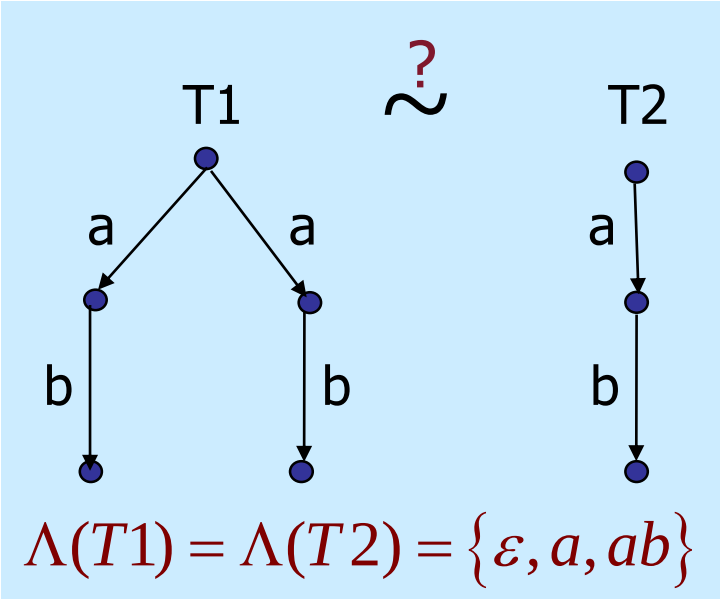


Erős biszimuláció ekvivalencia LTS-ekre

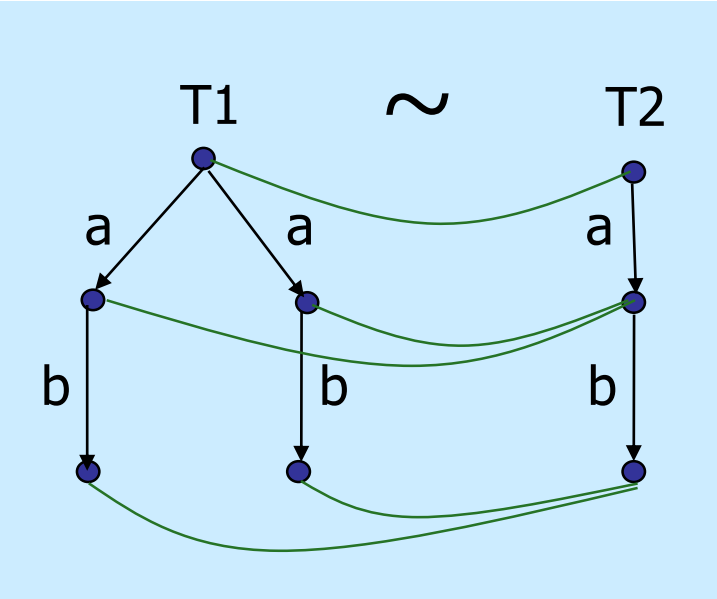
- Erős biszimuláció ekvivalencia $\sim$:

$$T_1 \sim T_2 \quad \text{a.cs.a.} \quad \exists B : (s_1, s_2) \in B$$

- Ekvivalens modellek tudják szimulálni egymást
  - Egyező akciókkal címkézett tranzíciók ekvivalens állapotokból
  - Erős biszimuláció ekvivalencia implikálja a trace ekvivalenciát

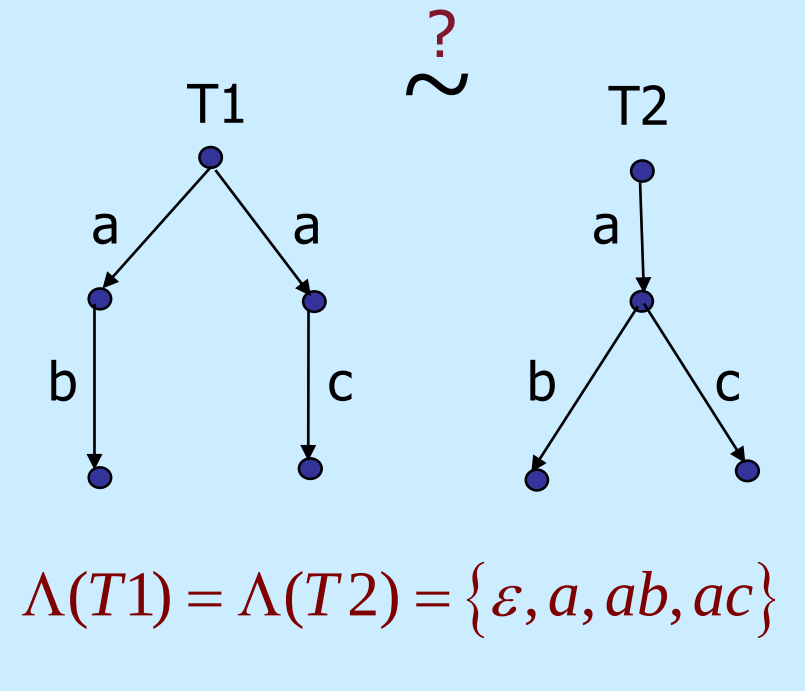


$$\Lambda(T1) = \Lambda(T2) = \{\varepsilon, a, ab\}$$

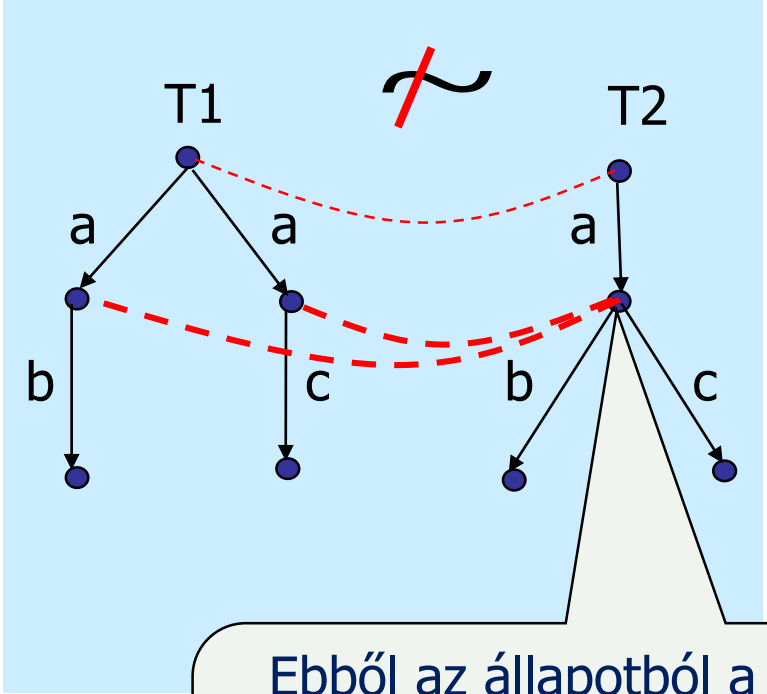


Erős biszimuláció ellenőrzése LTS-ekre: Példa

- Erős biszimuláció ellenőrzése LTS-ek között:



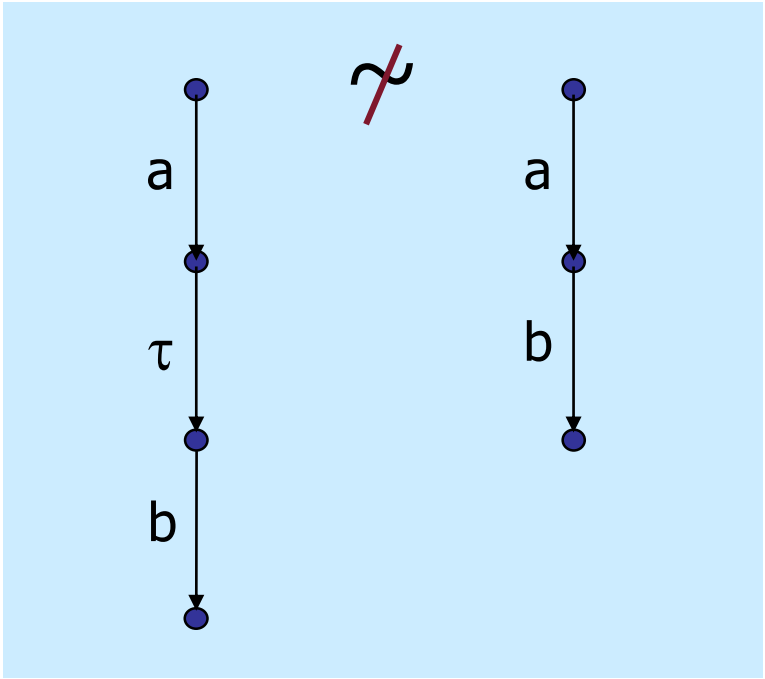
$$\Lambda(T1) = \Lambda(T2) = \{\varepsilon, a, ab, ac\}$$



Ebből az állapotból a b vagy a c akció is következhet, de a bal oldali állapotokból egyszerre csak az egyik.

Erős biszimuláció ekvivalencia: Hátrányok

- Érzékeny a hatás nélküli belső akcióra:
  - Egyes esetekben a belső akciónak nincs hatása a megfigyelhető viselkedésre, de az erős biszimuláció reláció különbséget tesz
  - Egyszerű példa:



Egy kevésbé érzékeny ekvivalencia relációra van szükség.

Gyenge biszimuláció (megfigyelési ekvivalencia)

- Két LTS gyenge biszimuláció ekvivalens, ha szimulálni tudják egymás megfigyelhető akciósorozatait ekvivalens állapotokon keresztül
  - Ekvivalens állapotok: Innen indulva egymást szimulálni tudják, azaz azonos megfigyelhető akciókat nyújtanak
  - Nem érzékeny a hatás nélküli belső átmenetekre
- Jelölések:

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

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

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

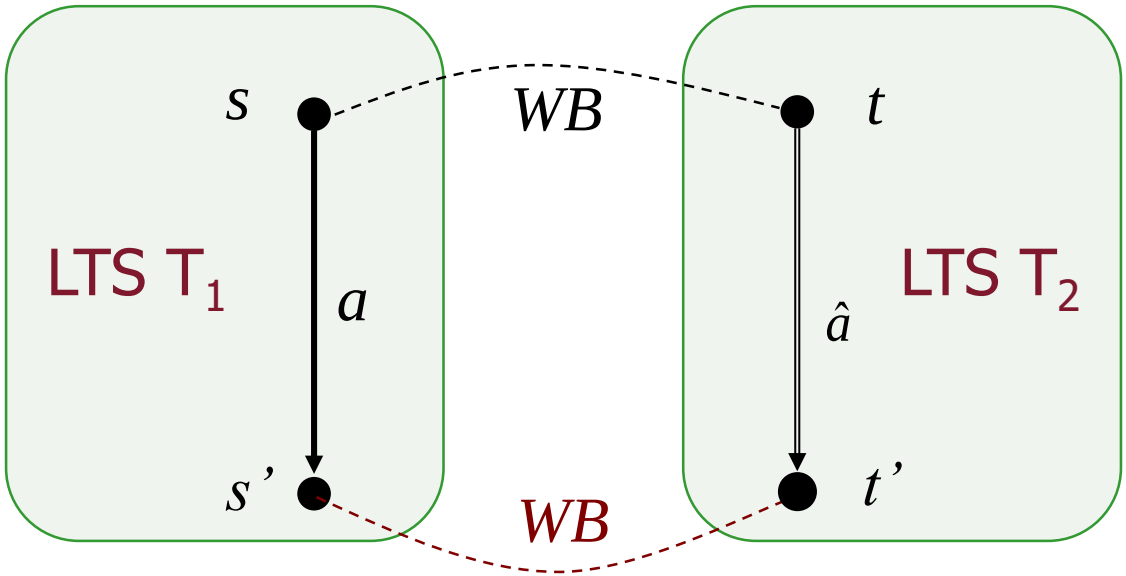
$s \overset{\beta}{\Rightarrow} s'$ ha $\exists \alpha: s \overset{\alpha}{\rightarrow} s'$ és $\beta = \hat{\alpha}$

Gyenge biszimuláció reláció állapotokra

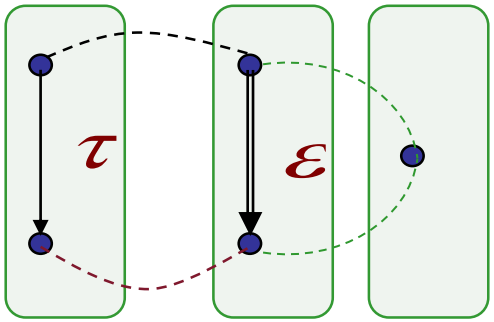
- Definíció az LTS-ek állapotpárjaira:

  $WB \subseteq S \times S$ 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 $\exists t' : t \overset{\hat{a}}{\Rightarrow} t'$ és $(s',t') \in WB$
  - ha $t \xrightarrow{a} t'$ akkor $\exists s' : s \overset{\hat{a}}{\Rightarrow} s'$ és $(s',t') \in WB$



Extrém eset:

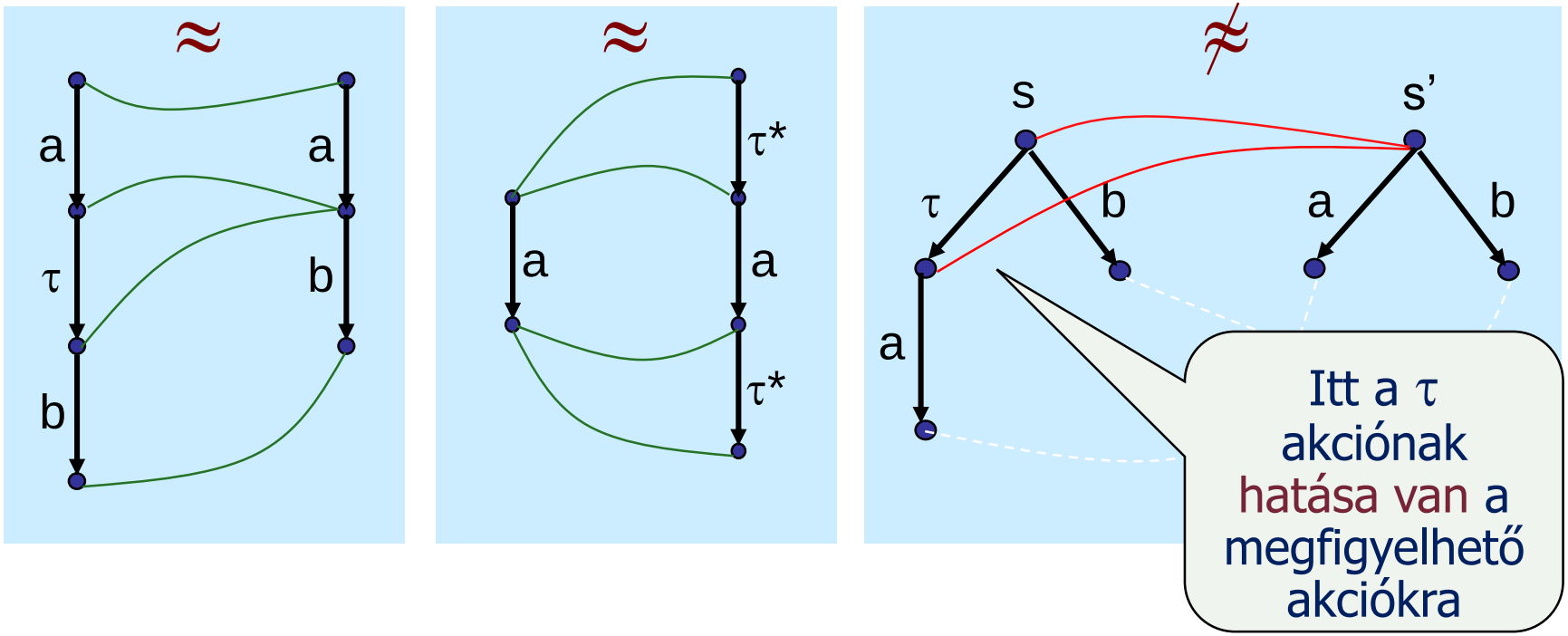


Gyenge biszimuláció ekvivalencia LTS-ekre

- Gyenge biszimuláció (megfigyelési ekvivalencia) $\approx$

$$T_1 \approx T_2 \quad \text{a.cs.a.} \quad \exists WB : (s_1, s_2) \in WB$$

- Példák:



Ekvivalencia relációk számítási módszere (alapötlet)

1. Kezdetben minden állapotpár eleme a relációnak
2. Minden állapotpárra:

   Ha az egyikből indulva van olyan átmenet, amit a másik nem tud szimulálni a definíció szerint, akkor
   - Az állapotpár kizárása a relációból (nem ekvivalensek)
   - Következmények végigvezetése a bejövő átmenetek végén lévő állapotokra:
     Nem ekvivalensek, mivel nem ekvivalens állapotokba kerülnek az átmenetekkel - kizárhatók
3. Ha már nincs változás: Végleges reláció adódik (állapotpárok, amelyek nem kerültek kizárásra)

   Ha a kezdőállapotok bennmaradtak a relációban, akkor az LTS-ek ekvivalensek

Viselkedés finomítási relációk

Lehetséges viselkedés szerinti rendezés

- Célkitűzés: A finomított LTS tartsa meg az eredeti LTS lehetséges megfigyelhető akciószekvenciáit
- Jelölések:

$\beta \in (Act - \tau)^*$ megfigyelhető akciószekvencia τ törlésével

$s \overset{\beta}{\Rightarrow} s'$ ha $\exists \alpha \in Act^*: s \overset{\alpha}{\rightarrow} s'$ és $\beta = \hat{\alpha}$

$\Delta(s)$ az s-ből induló megfigyelhető akciószekvenciák halmaza:

$$\Delta(s) = \left\{ \beta \mid \exists s': s \overset{\beta}{\Rightarrow} s' \right\}$$

$\Delta(T)$ egy s kezdőállapotú T LTS esetén: $\Delta(T) = \Delta(s)$

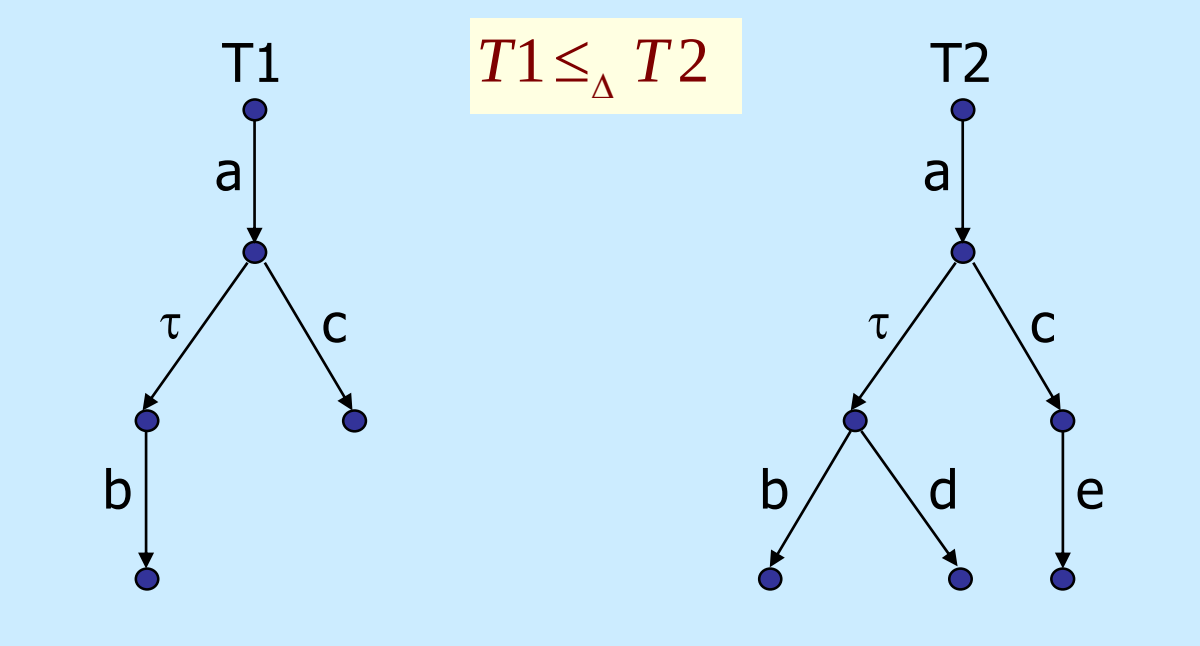
Lehetséges viselkedés szerinti rendezés: Definíció

- Lehetséges viselkedés szerinti rendezés:

$T_1 \leq_\Delta T_2$ a.cs.a. $\Delta(T_1) \subseteq \Delta(T_2)$ azaz $\Delta(s_1) \subseteq \Delta(s_2)$

itt T_2 esetén több a megfigyelhető akciószekvencia

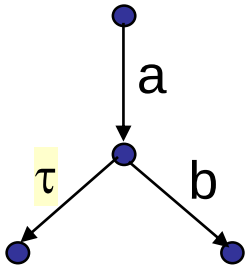
- Példa:



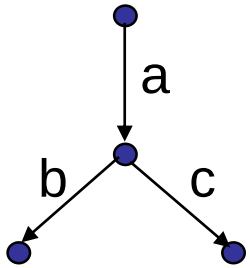
$\Delta(T1) = \{a, ab, ac\}$ $\Delta(T2) = \{a, ab, ac, ad, ace\}$

Kapcsolat a teszteléssel

- Itt: Az akciók az interakciókat modellezik egy teszt szekvencia során
  - Sikeres interakció (elvártan végrehajtja a tesztlépést): Az LTS képes rá, az aktuális állapot egy kimenő átmenetén megtalálható az akció
  - Elakad egy interakció: Az LTS nem képes az adott interakcióra, az aktuális állapot egy kimenetén sem található meg



Az a interakció mindig sikeres.
Ezután lehetséges, hogy b sikeres, de el is akadhat (τ lépéstől függően).

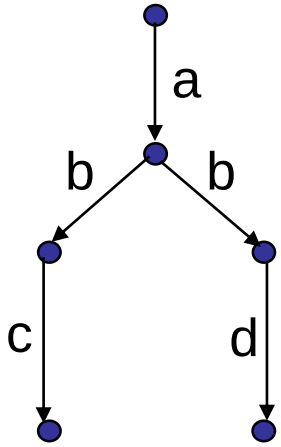


Az a interakció mindig sikeres.
Ezután a b és a c is mindig sikeres, egyik sem akadhat el.

- A $T_1 \leq_\Delta T_2$ rendezés esetén:
  - Megfigyelhető trace-ek: A lehetséges sikeres interakciók sorozatai
    Természetesen a mindig sikeres interakció is a lehetségesek között van
  - Minden interakciósorozat, ami T_1 esetén lehetséges, T_2 esetén is lehetséges
  - Tesztekre: T_1 lehetséges sikeres teszt szekvenciái T_2 lehetséges sikeres teszt szekvenciái között vannak

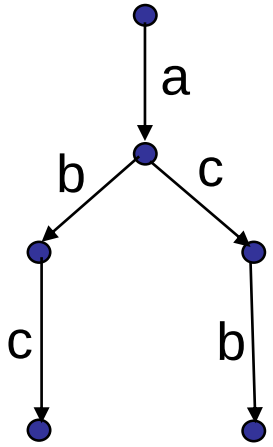
Lehetséges viselkedés és szükséges viselkedés

- Lehetséges és mindig sikeres akciószekvenciák:



Az abc és az abd is lehetséges szekvencia, de egyik sem mindig sikeres (elakadhat az ab szekvencia után).

Újabb állapotokkal, átmenetekkel és akciókkal bővíthető a lehetséges viselkedés.



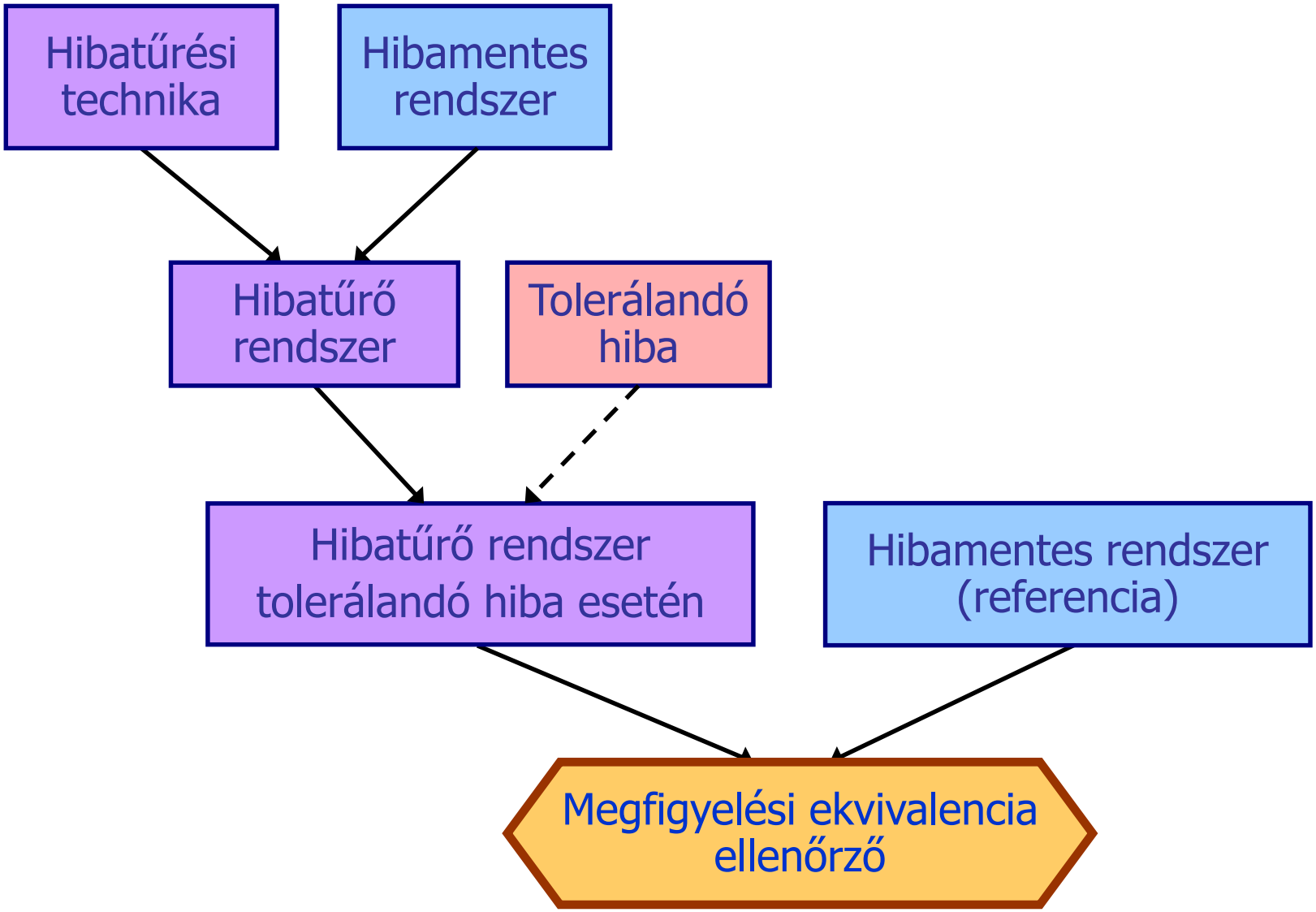
Az abc és az acb szekvencia is mindig sikeres (nem akadhat el).

A mindig sikeres viselkedés is bővíthető (nem lesz elakadás)

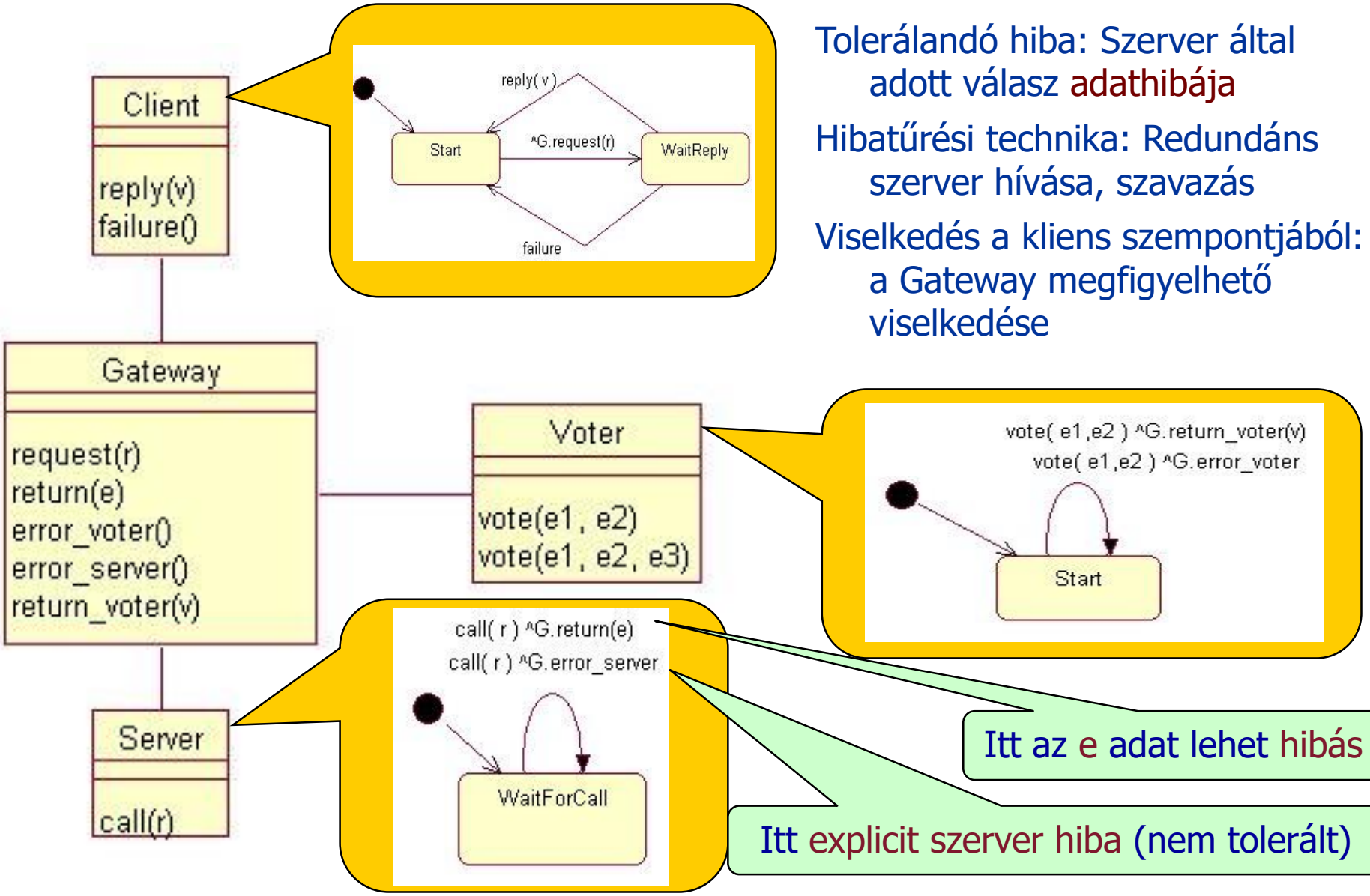
- A $T_1 \leq_\Delta T_2$ rendezés:
  - Olyan finomítást definiál, amelynek során nem lesz kevesebb lehetséges megfigyelhető viselkedés
  - (Természetesen a mindig sikeres viselkedés is lehetséges viselkedés)
- Kitekintés: Egy másik rendezési reláció: Szükséges viselkedés szerint
  - A rendezés olyan finomítást definiál, amelynek során nem lesz kevesebb mindig sikeres viselkedés (mindenképpen szükséges viselkedés)

Mintapélda: Hibatűrés verifikációja ekvivalencia ellenőrzéssel

Mintapélda: Hibatűrés verifikációja



Rendszerarchitektúra



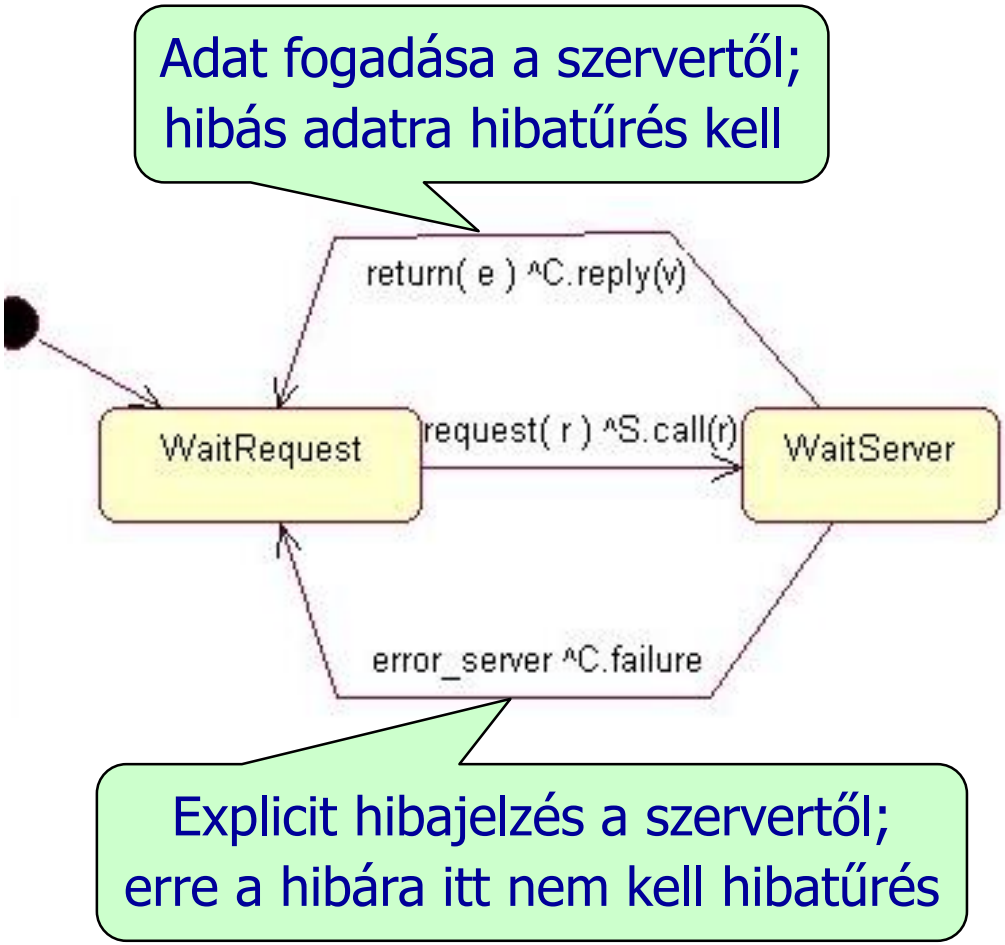
Tolerálandó hiba: Szerver által adott válasz adathibája

Hibatűrési technika: Redundáns szerver hívása, szavazás

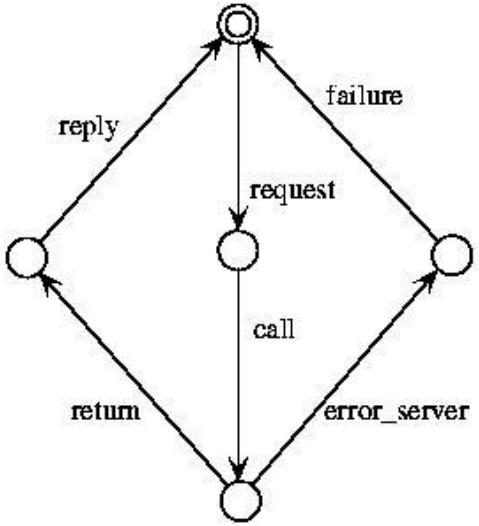
Viselkedés a kliens szempontjából: a Gateway megfigyelhető viselkedése

A Gateway referencia viselkedése

- Állapotdiagram:

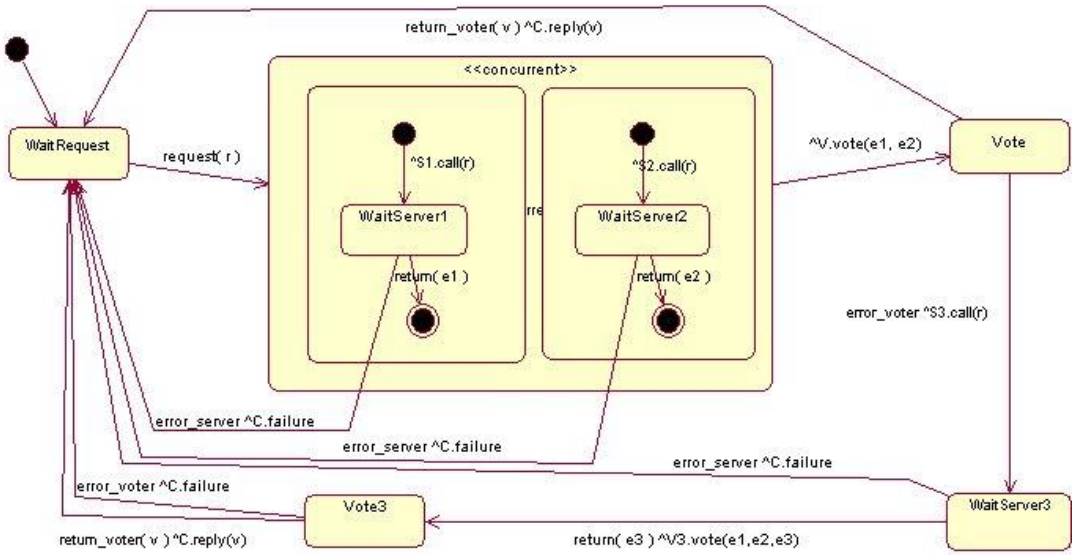


- LTS:

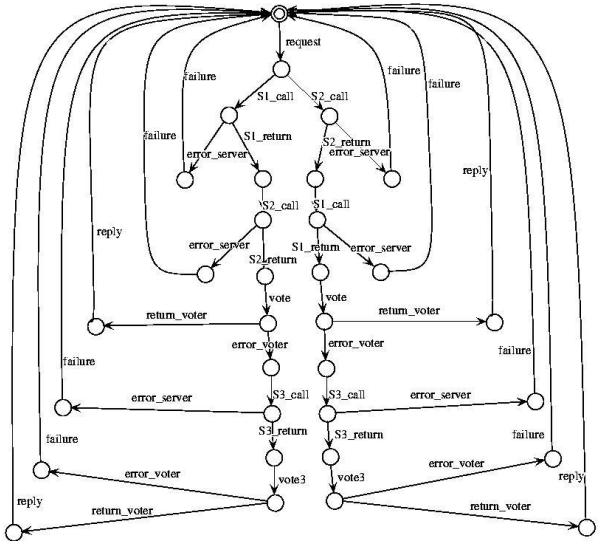


A Gateway viselkedése hibatűrő esetben

- Állapotdiagram:

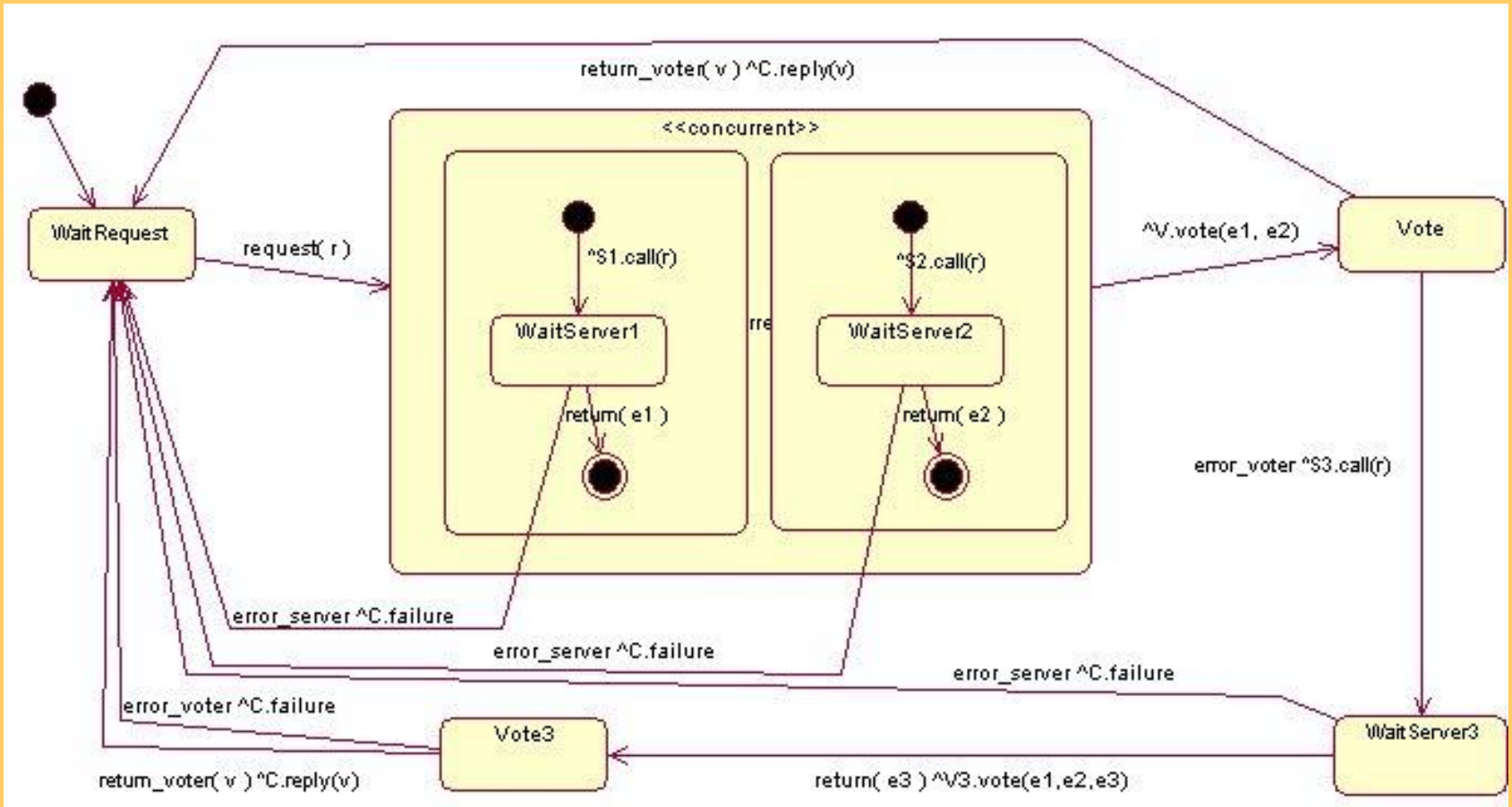


- LTS:



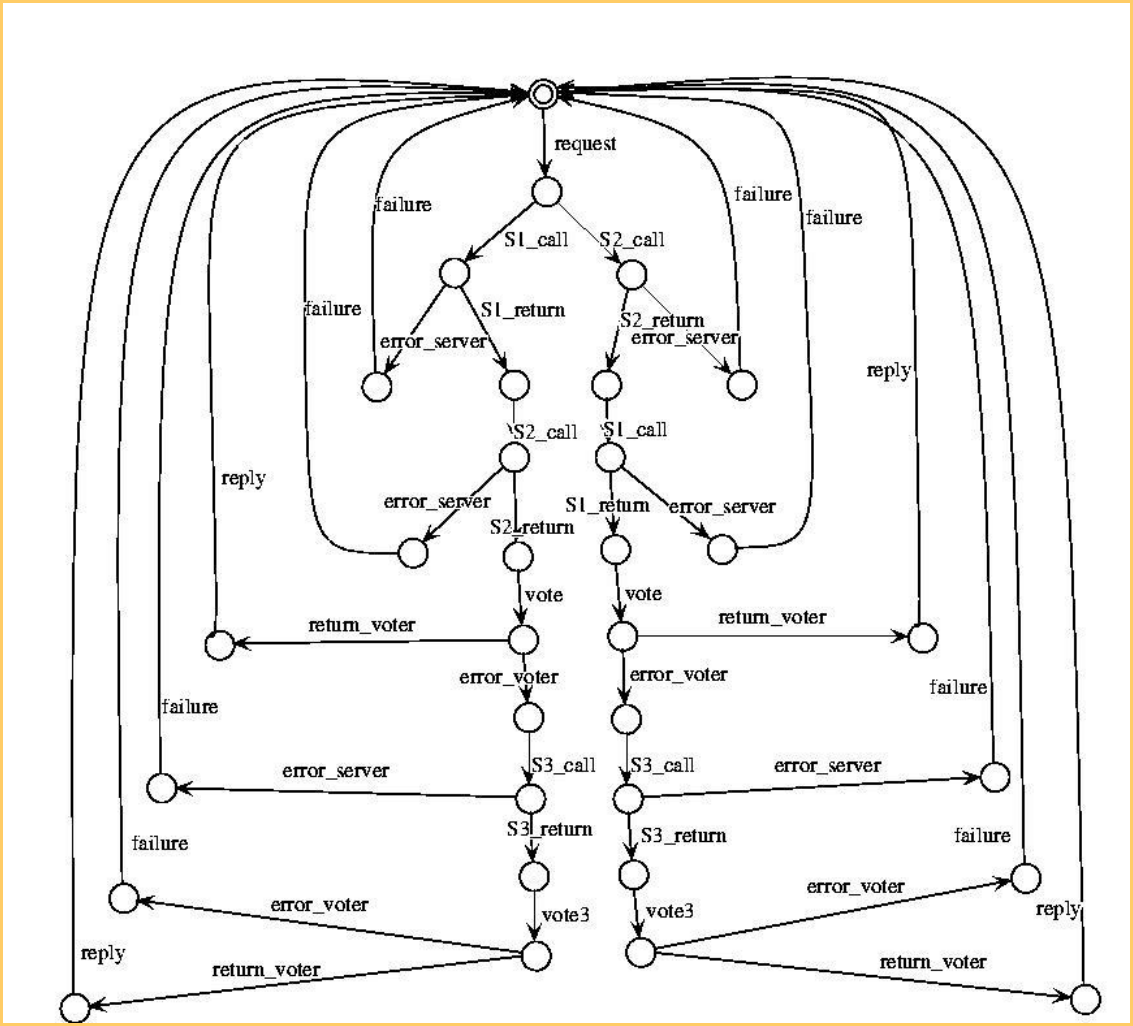
A Gateway viselkedése hibatűrő esetben

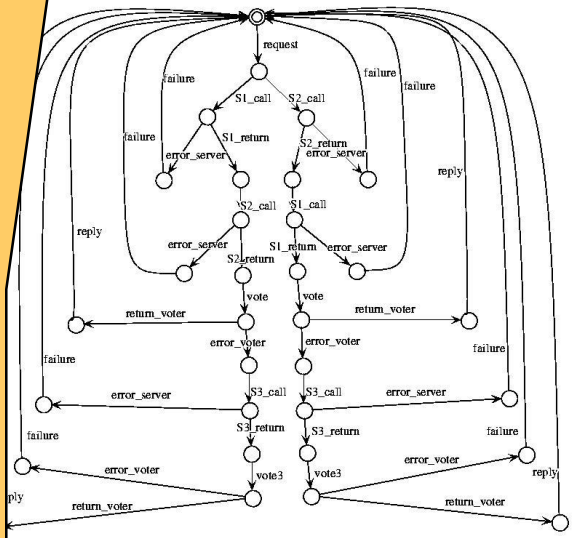
- Állapotdiagram:
- LTS:



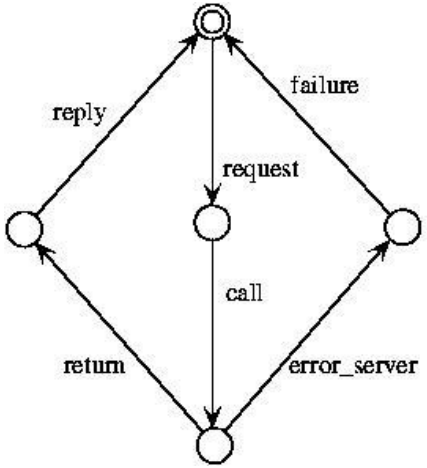
A Gateway viselkedése hibatűrő esetben

LTS:



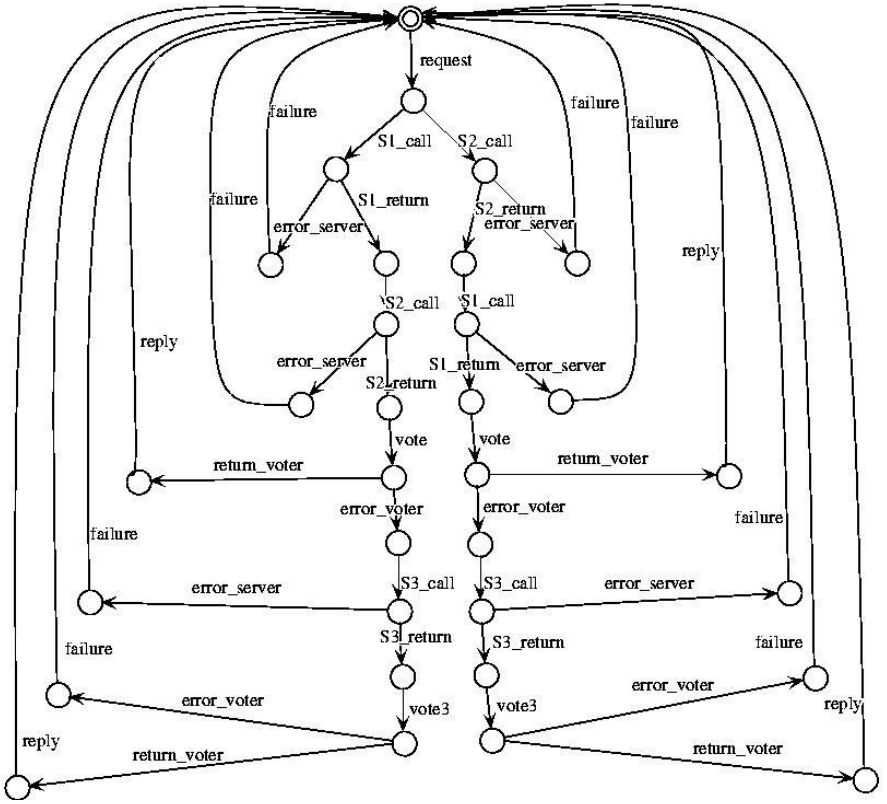


Viselkedési ekvivalencia igazolása



Gateway
referencia
viselkedés

≈

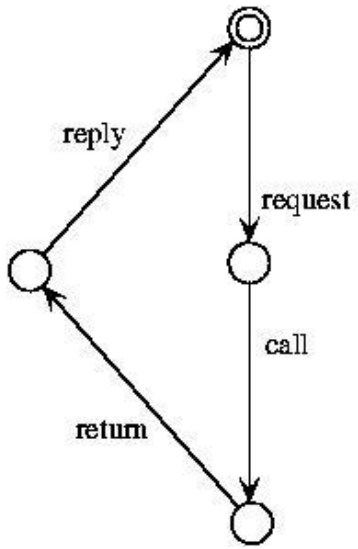


Az ekvivalencia alapján kijelenthető:
a kliens számára
a hibatűrő mechanizmus működése transzparens.

Hibatűrő Gateway teljes viselkedése;

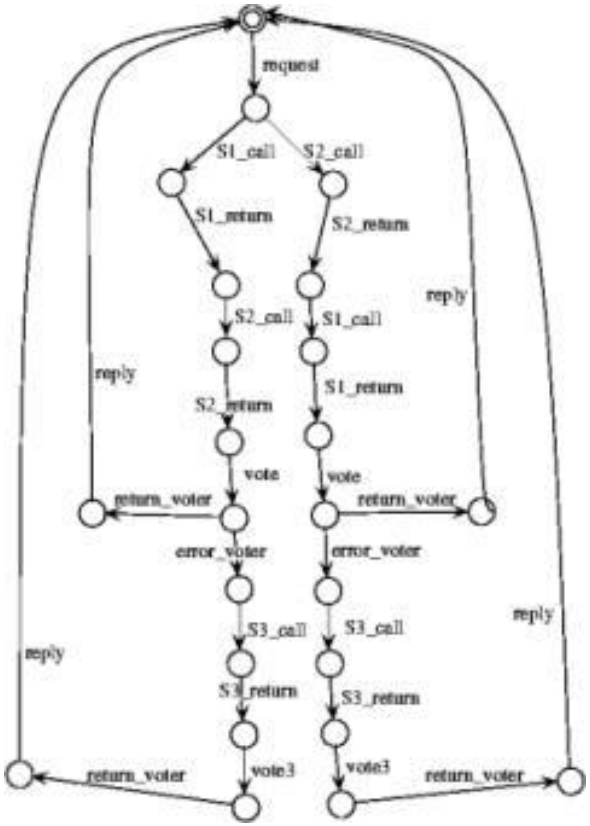
minden olyan akció τ lesz,
ami nincs a referencia viselkedésben!

Hibatűrés igazolása az első szerver adathibája esetén



Hibamentes Gateway

≈



Az ekvivalencia alapján kijelenthető:
Az adott hiba esetén a kliens szempontjából megvalósul a hibatűrés.

Hibatűrő Gateway az első szerver adathibája esetén;
minden olyan akció τ,
ami nincs a referencia viselkedésben

Összefoglalás

- Motiváció
  - Modellek közötti viselkedési ekvivalencia
  - Modellek finomítása meghatározott reláció szerint
- Ekvivalencia relációk
  - Trace ekvivalencia
  - Megfigyelési ekvivalencia (gyenge biszimuláció)
- Finomítási relációk
  - Lehetséges viselkedés szerint
  - (Említve: szükséges viselkedés szerint)
- Esettanulmány
  - Hibatűrés vizsgálata