Sztochasztikus temporális logikák

Teljesítmény és szolgáltatásbiztonság jellemzők formalizálása és ellenőrzése

Majzik István

Budapesti Műszaki és Gazdaságtudományi Egyetem

Méréstechnika és Információs Rendszerek Tanszék

http://www.mit.bme.hu/~majzik/

Motiváció: Szolgáltatásminőségi követelmények

- Nem tisztán állapot elérhetőségi jellegű követelmények
  - QoS: Quality of Service
  - SLA: Service Level Agreement
- Jellemzőek a követelményekre:
  - Adott szolgáltatási szintek (állapotok) valószínűségei
    - Példa: Rendelkezésre állás, mint valószínűség (állandósult állapotban)
  - Szolgáltatási szintek fenntartásának / kihagyásának időtartama
    - Példa: Javítási idő maximuma
- Példák összetett QoS követelményekre:
  - Annak a valószínűsége legfeljebb 20%, hogy a hiba utáni helyreállítás több mint 15 időegységet vegyen igénybe.
  - Annak a valószínűsége kisebb 10%-nál, hogy indítás után 85 időegység alatt a szolgáltatási szint Minimum alá csökken.
  - Több mint 70% annak a valószínűsége, hogy Minimum szolgáltatási szint elérése esetén 5 időegységen belül Premium szint nyújtható.

Milyen modellek használhatók?

- Teljesítmény- és megbízhatóság modellezés:
  - Sztochasztikus Petri-hálók
  - Sztochasztikus processz algebrák
  - Sztochasztikus aktivitás hálók

Tevékenységekhez exp. eloszlású időzítés rendelése a kezelhetőség érdekében

- Ezekből folytonos idejű Markov lánc képzése és megoldása (mint alacsony szintű formalizmus)
  - Állandósult állapotbeli analízis
  - Tranziens analízis

Folytonos idő
Diszkrét állapotok
Állapotátmeneti gyakoriság

- Megoldási módok:
  - Analitikus („képlettel”)
  - Numerikus („iterálva”)
  - Szimulációval („kimérve”)

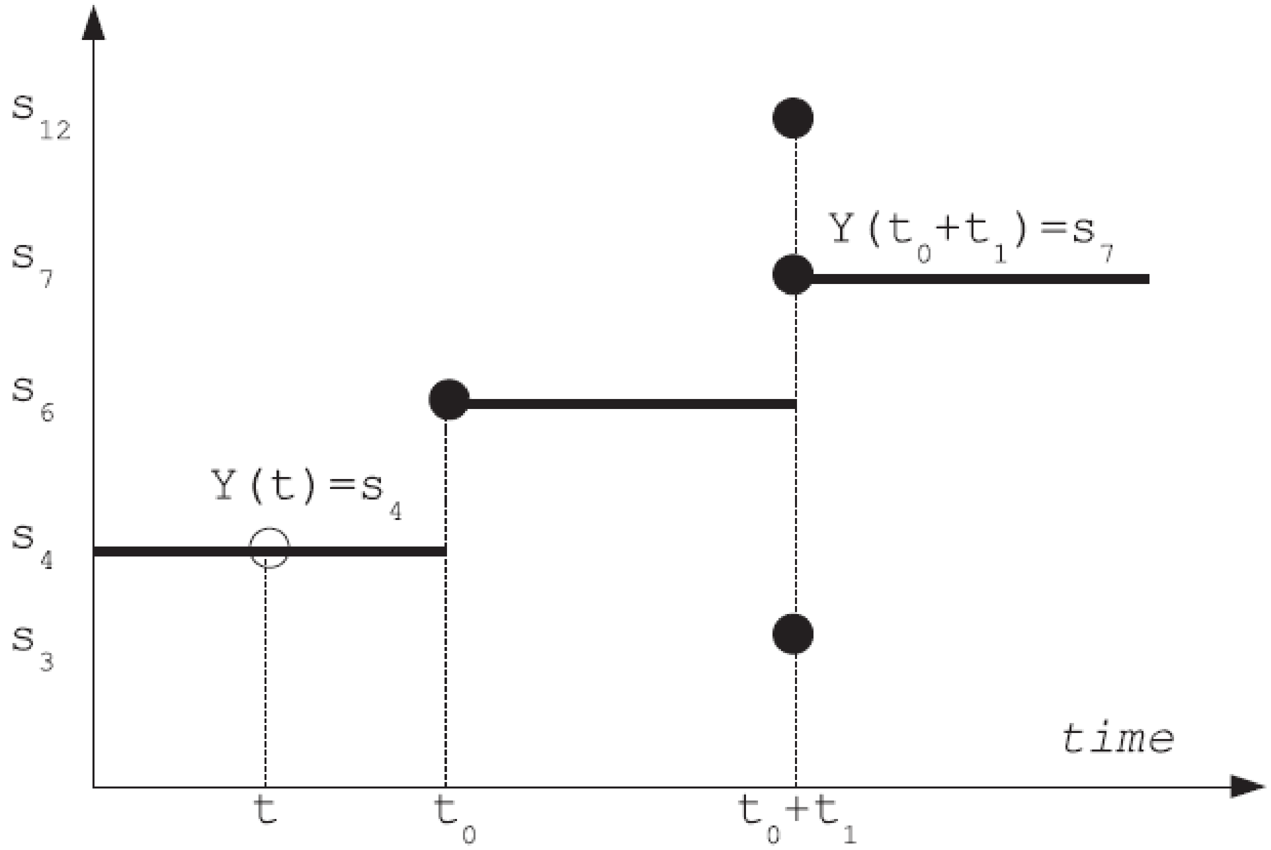
Markov folyamatok

- Sztochasztikus folyamat:
  - Valószínűségekkel jellemezhetően bekövetkező jelenségek modellezése, az idő paraméter függvényében
- Markov folyamat S(t) állapottal:

  $P\{S(t)=s \mid S(t_n)=s_n, S(t_{n-1})=s_{n-1}, \ldots, S(t_0)=s_0\} = P\{S(t)=s \mid S(t_n)=s_n\}$

  minden $t > t_n > t_{n-1} > \ldots > t_0$ esetén
- Informálisan:
  - A jövőbeli viselkedés (t-ben) csak az aktuális állapottól (t_n-ben) függ, és nem függ a korábbi állapotoktól
- Diszkrét állapotterű Markov folyamatok: Markov láncok
  - Diszkrét állapotokban való tartózkodás idejével (tartási idő) jellemezhetők a trajektóriák
  - Állapotok tartási ideje negatív exponenciális eloszlású
    - Az egyetlen eloszlásfüggvény, ami a Markov tulajdonságot teljesíti
    - Bármely időpillanatban a maradék tartási idő statisztikailag független attól, hogy eddig mennyi időt töltött már a folyamat az adott állapotban

Sztochasztikus folyamat: Egy trajektória



- Az összes lehetséges trajektória jellemzi a sztochasztikus folyamatot
- Ezek alapján állapotok valószínűségének időfüggvényei felvehetők

Folytonos idejű Markov láncok (CTMC)

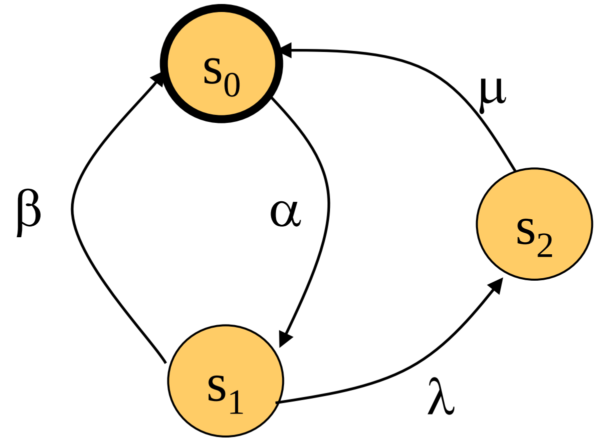
- CTMC: Continuous Time Markov Chain
  - Folytonos idő paraméter, diszkrét állapottér
- Jelölések, tulajdonságok:
  - Diszkrét állapotok: $s_0, s_1, \ldots, s_n$, a CTMC állapota $S(t)$
  - Állapotátmeneti valószínűség: $Q_{ij}(t_{n-1},t_n)= P\{S(t_n)=s_j \mid S(t_{n-1})=s_i\}$
  - Homogén Markov-folyamat: $Q_{ij}(t,t+\Delta t)= Q_{ij}(\Delta t)$
    - Állapotátmeneti valószínűség nem változik az idő függvényében
  - Állapotátmeneti intenzitás (gyakoriság, ráta):

$$R_{ij}(t) = \lim_{\Delta t \to 0} \frac{1}{\Delta t} Q_{ij}(\Delta t)$$

  - Állapot elhagyás összesített rátája: $E(s) = \sum_{s' \in S} R_{s,s'}$
  - Állapot tartási ideje: $P\{\text{s-ben marad t ideig}\} = e^{-E(s)t}$

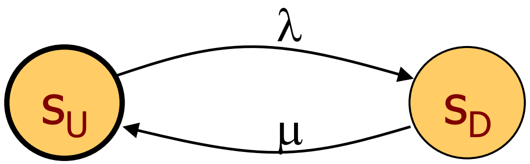
Egy egyszerű CTMC

- CTMC szokásos megjelenítése:
  - Állapotok halmaza (kezdő valószínűségekkel)
  - Minden állapotpárra az állapotátmeneti intenzitás (ahol nem nulla, csak ott van feltüntetve)



CTMC alkalmazások

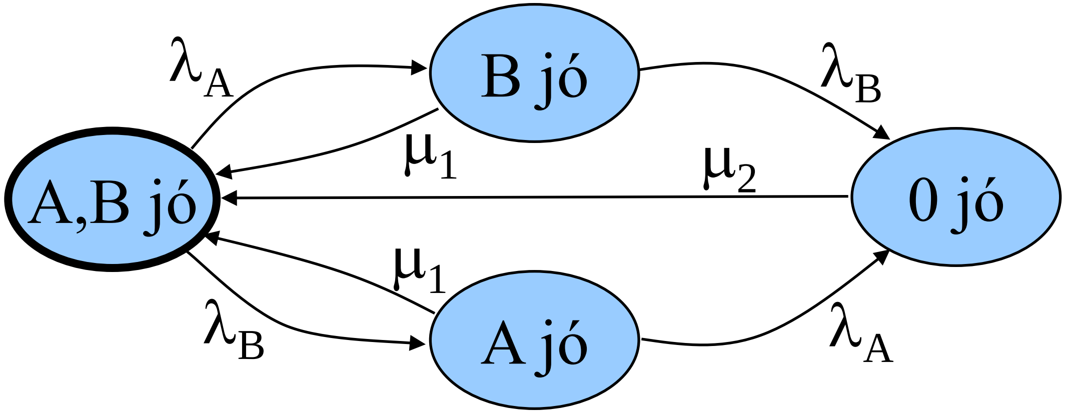
- Megbízhatósági modellezés:
  - Komponens állapottere: Hibamentes s_U vagy hibás s_D állapot
  - Gyakorlati tapasztalat elektronikai komponensekre:
    - A hibamentes állapot tartási ideje exponenciális eloszlással jellemezhető a tipikus használati tartományban
    - Az exp. eloszlásfüggvény paramétere: Meghibásodási tényező, λ
    - A javítási időt is exp. eloszlással számítják (egyszerűsítés), μ



- Teljesítmény modellezés
  - Sorbanállás - kiszolgálás
    - M/M/1 sor: „Markovi” beérkezési és kiszolgálási idők
    - Állapottér mint CTMC vehető fel
  - Sorbanállási hálózatok

Példa: Megbízhatósági modellezés

- Két szerverből (A, B) álló rendszer:
  - Bármelyik szerver meghibásodhat
  - A szerverek külön-külön vagy együtt is javíthatók
  - Rendszerszintű állapotokat modellezünk
- Állapotátmenetek (exponenciális eloszlású időzítés):
  - Az A szerver meghibásodása: λ_A meghibásodási tényező
  - A B szerver meghibásodása: λ_B meghibásodási tényező
  - Egy hibás szerver javítása: μ_1 javítási tényező
  - Teljes rendszer javítása: μ_2 javítási tényező



Folytonos idejű Markov-láncok (jelölések)

- CTMC=(S,***R***)

  S állapotok halmaza

  R: $S \times S \rightarrow R_{\geq 0}$ állapotátmeneti intenzitás (ráta) mátrix

  - $\underline{E}(s) = \sum_{s' \in S} R(s,s')$ állapot elhagyás összesített intenzitása
  - $\underline{\boldsymbol{Q}} = \underline{\boldsymbol{R}} - \mathrm{diag}(\underline{E})$ „infinitezimális generátormátrix”

- Útvonalak:

  $\sigma = s_0, t_0, s_1, t_1, \ldots$ útvonal (t_i időpontban lép ki s_i-ből)

  $\sigma@t$ az állapot a t időpillanatban

  Path(s) az s-ből induló útvonalak halmaza

  P(s, σ) egy útvonal bejárásának valószínűsége

Markov-láncok megoldása

- Tranziens valószínűségek:
  - $\pi(s,s',t) = P\{\sigma \in Path(s) \mid \sigma@t=s'\}$ annak valószínűsége, hogy s-ből indulva a t időpillanatban s'-ben tartózkodik
  - $\underline{\pi}(s,t)$: s-ből indulva az állapotok valószínűsége t időpillanatban
  - CTMC tranziens megoldása:

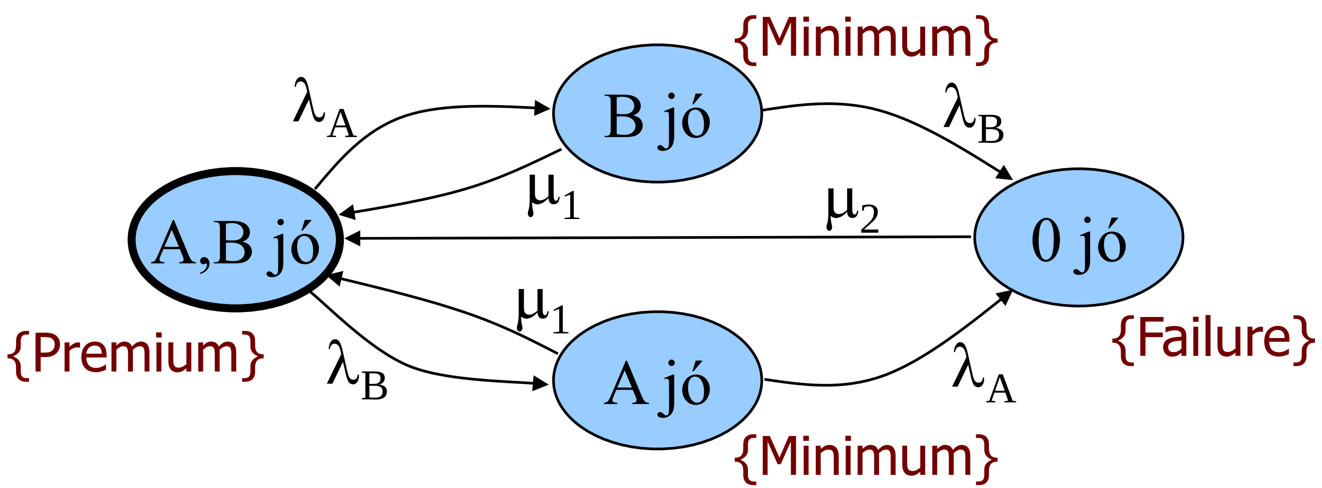
$$\frac{d\,\underline{\pi}(s,t)}{dt} = \underline{\pi}(s,t)\underline{\underline{Q}}$$

- Állandósult állapot: ha véges állapotú és irreducibilis CTMC
  - $\pi(s,s') = \lim_{t\to\infty} \pi(s,s',t)$ - s-ből indulva az állapotok valószínűsége
  - $\underline{\pi}(s)$ az állapotok valószínűsége (sorvektor)
  - $\pi(s,S') = \Sigma_{s' \in S'} \pi(s,s')$ egy állapothalmaz valószínűsége
  - CTMC állandósult állapotbeli megoldása:

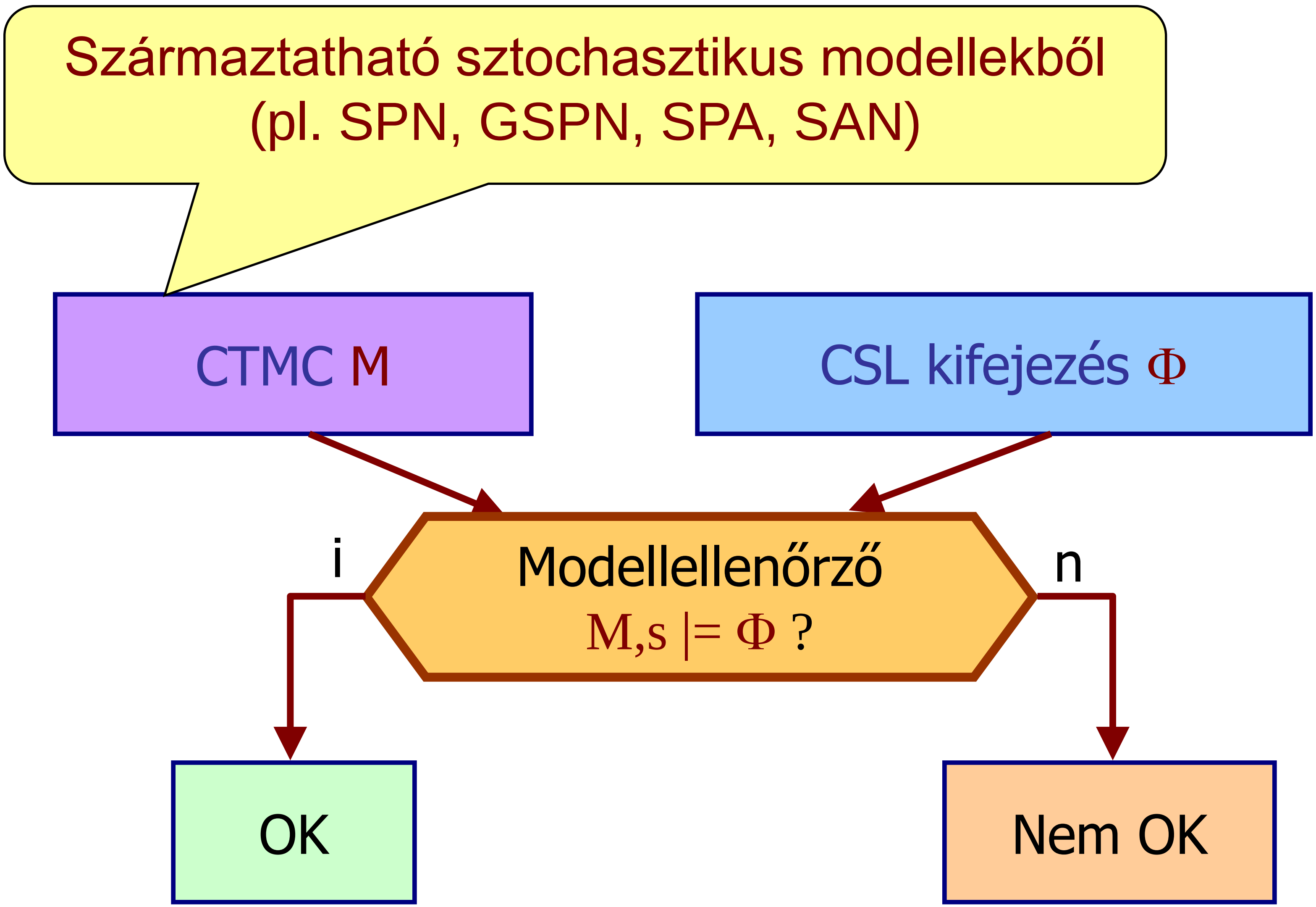
$$\underline{\pi}(s)\underline{\underline{Q}} = 0 \quad \text{ahol} \quad \sum_{s'} \pi(s,s') = 1$$

Hogyan formalizálhatók a követelmények?

- Modell: CTMC, egyszerű állapot-alapú formalizmus
  - Kiterjesztés: Állapotok címkézése atomi kijelentésekkel
    - Ld. Premium, Minimum, Failure a lenti modellen
  - Állapotokra: Számítható állandósult vagy tranziens valószínűségek
  - Útvonalakra: Számítható bejárási valószínűségek
- Követelmények formalizálása: CTL analógia alapján
  - Állapot és útvonal kifejezések
- CSL: Continuous Stochastic Logic
  - Állapotokra és útvonalakra vonatkozó valószínűségi kifejezések és időtartamok megadása



CSL modellellenőrzés



Continuous Stochastic Logic: Szintaxis

- Kiterjesztések a CTL-hez képest:
  - Valószínűségi operátorok:
    - Állandósult állapotra: Állapot-kifejezések által megadott állapot-halmazokban való tartózkodás valószínűsége
    - (Tranziens) útvonalakra: Útvonal-kifejezések által megadott útvonal bejárásának valószínűsége
  - Időtartományok megadása:
    - X és U temporális operátorokhoz időintervallum megadása: az adott időintervallumon belüli bekövetkezés
- Jelölések:

I intervallum, pl. [0, 12), [15,∞)

p valószínűség

~ az összehasonlítás operátora, pl. $\geq$, $\leq$, <, >

CSL állapot-kifejezések

- Jelölések:
  - Φ állapot-kifejezések (ezek alkotják a CSL kifejezéseket)
  - φ útvonal-kifejezések
- Szintaxis: $\Phi ::= P \mid \neg\Phi \mid \Phi\vee\Phi \mid S_{\sim p}(\Phi) \mid P_{\sim p}(\varphi)$
  - $S_{\sim p}(\Phi)$ - állandósult állapotban az olyan állapotokban való tartózkodás valószínűsége ~p, ahol Φ igaz

    P{olyan állapotban tartózkodik, ahol Φ igaz} ~ p

    - Példa: $S_{>0,8}(\text{Minimum}\vee\text{Premium})$
  - $P_{\sim p}(\varphi)$ - olyan utak bejárásának valószínűsége ~p, amelyeken φ igaz

    P{olyan utat jár be, ahol φ igaz} ~p

    - Példa: $P_{>0,7}(\text{true U Premium})$

CSL útvonal-kifejezések

- Szintaxis: $\varphi ::= X^I \Phi \mid \Phi\ U^I \Phi$
  - $X^I \Phi$ – a következő állapotot a $t \in I$ időpillanatban érjük el, és ebben a következő állapotban igaz Φ
    - Példa: $X^{[0,10]}$Premium
  - $\Phi_1\ U^I\ \Phi_2$ – a $t \in I$ időpillanatban elérünk egy olyan állapotba, ahol Φ_2 igaz, és az odavezető úton Φ_1 igaz
    - Példa: Minimum $U^{[5,10]}$ Premium
- Rövidítések:
  - $E\ \varphi = P_{>0}(\varphi)$
  - $A\ \varphi = P_{\geq 1}(\varphi)$
  - $F^I\ \Phi = \mathrm{true}\ U^I\ \Phi$
  - $X\ \Phi = X^I\ \Phi$, $\quad \Phi_1\ U\ \Phi_2 = \Phi_1\ U^I\ \Phi_2$ ahol $I=[0,\infty)$

CSL szemantika

- M=(S,***R***,L) egy CTMC az állapotok címkézésével
  - L: S → 2^{AP} állapot címkézés
- Alap operátorok:
  - M,s |= P a.cs.a. $P \in L(s)$
  - M,s |= $\neg\Phi$ a.cs.a. nem igaz M,s |= Φ
  - M,s |= $\Phi_1 \vee \Phi_2$ a.cs.a. M,s |= Φ_1 vagy M,s |= Φ_2
- Állapot kvantorok:
  - M,s |= $S_{\sim p}(\Phi)$ a.cs.a. $\pi(s, Sat(\Phi)) \sim p$,

    s-ből indulva Sat(Φ) áll. állapotban való tartózkodás vsz. ~p

    azaz M,s |= $S_{\sim p}(\Phi)$ a.cs.a. $\sum_{s' \in Sat(\Phi)} \pi(s,s') \sim p$
  - M,s |= $P_{\sim p}(\varphi)$ a.cs.a. $P(s, \sigma \mid \sigma \models \varphi) \sim p$,

    σ|=φ útvonal bejárás vsz. ~p

    azaz M,s |= $P_{\sim p}(\varphi)$ a.cs.a. $\sum_{\substack{\sigma \in Path(s) \\ \sigma \models \varphi}} P(s,\sigma) \sim p$

CSL szemantika (folytatás)

- Útvonal kvantorok:
  - $M,\sigma \models X^I \Phi$ a.cs.a.

    $\exists s_1$: $M,s_1 \models \Phi$ és $t_0 \in I$

  - $M,\sigma \models \Phi_1 U^I \Phi_2$ a.cs.a.

    $\exists t \in I$: $(\sigma@t \models \Phi_2$ és $\forall u \in [0,t)$: $\sigma@u \models \Phi_1)$

CSL modellellenőrzés

- $S_{\sim p}(\Phi)$ esetén:
  - Állandósult állapotbeli CTMC megoldásból származik
- $X^I\ \Phi$ esetén:
  - CTMC tranziens megoldás (következő állapotba lépés)
- $P_{\sim p}(\varphi)$ illetve $\Phi_1\ U^I\ \Phi_2$ esetén:
  - Tranziens megoldás kell + időintervallumokra
  - Általános: Volterra integrál-egyenlet megoldása

$$\int_0^t \sum_{s' \in S} \mathbf{R}(s,s') \cdot e^{-\mathbf{E}(s)\cdot x} \cdot Prob(s', \Phi\, \mathcal{U}^{[0,t-x]}\, \Psi)\, dx$$

  - Egyszerűsítés: CTMC és követelmény átalakítása úgy, hogy elég legyen t-re egy tranziens analízis
    - Átalakítás: $M \rightarrow M'$, $\Phi \rightarrow \Phi'$
    - Bizonyítandó: $M,s \models \Phi$ a.cs.a $M',s \models \Phi'$

Az egyszerűsítés illusztrálása $\Phi_1 \, U^{[0,t)} \, \Phi_2$ esetén

- Célkitűzés: $\Phi_1 \, U^{[0,t)} \, \Phi_2$ ellenőrzése M modellen
- A modell átalakítása M-ről M'-re:
  - Φ_2 -t teljesítő állapotok (Φ_1 teljesítése mentén, t előtt) elérése után a viselkedés nem érdekes,
    így minden Φ_2 tulajdonságú állapot nyelő lesz M'-ben
  - $\neg (\Phi_1 \vee \Phi_2)$ esetén, tehát ha egyiket sem teljesíti,
    akkor a további viselkedés nem érdekes,
    így ezek is nyelők lesznek M'-ben
- A követelmény átalakítása M' esetén:
  - Bizonyítható tétel:

    M,s |= $\Phi_1 \, U^{[0,t)} \, \Phi_2$ ellenőrzésének eredménye ekvivalens

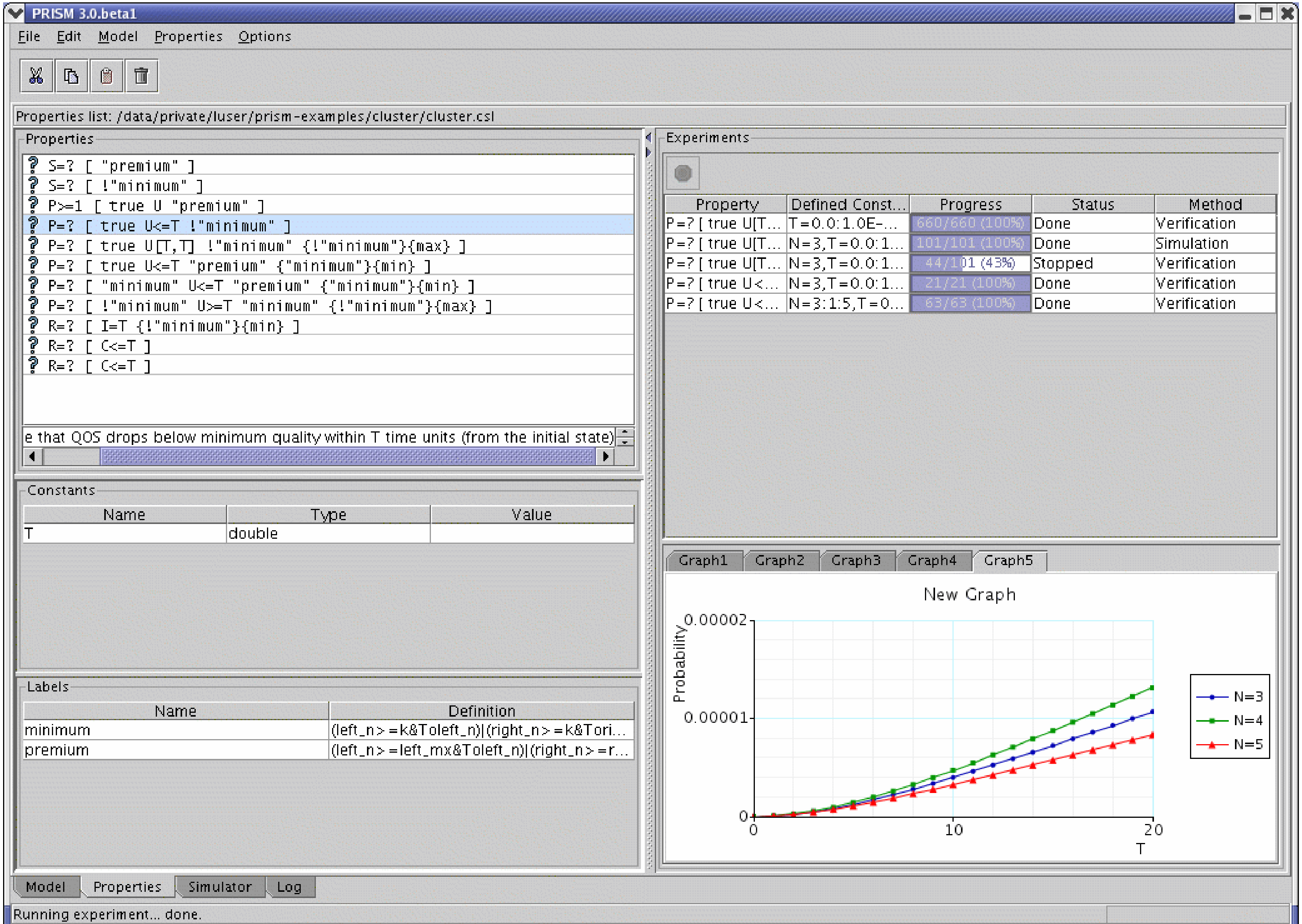
    M',s |= true $U^{[t,t]} \, \Phi_2$ ellenőrzésével (a módosított modellen!);

  azaz a módosított modellen t-re tranziens analízis elég

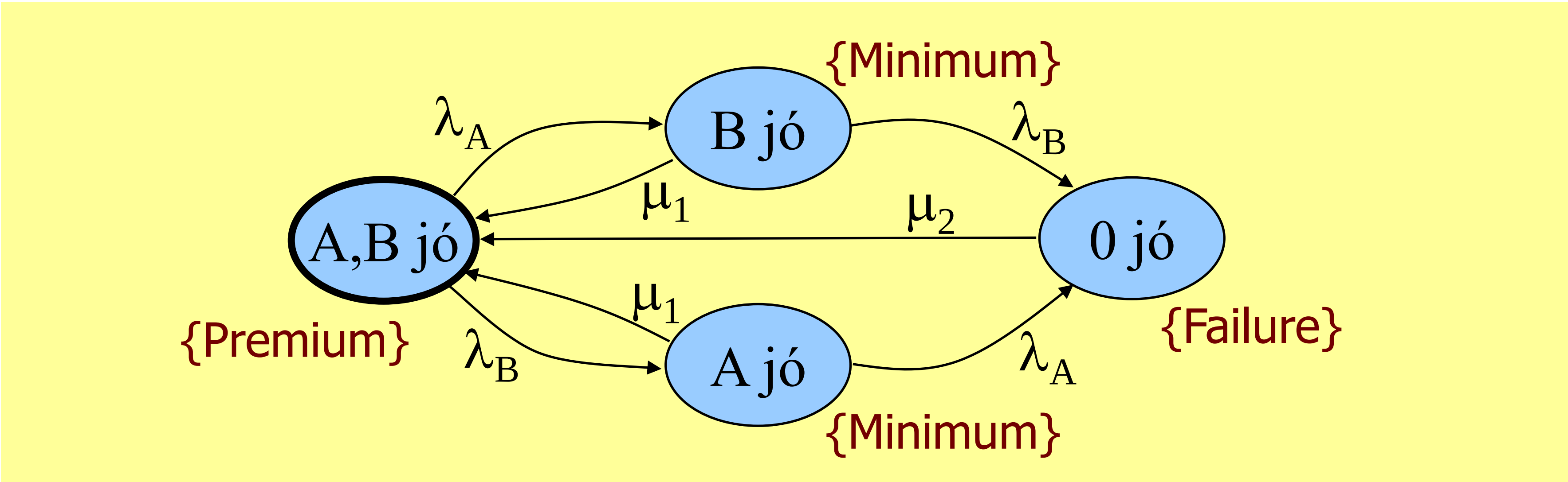
CSL modellellenőrzők

- Az első megvalósítás:
  ETMCC: Erlangen-Twente Markov Chain Checker (E|-MC^2)
  - Markov-láncok
  - Sztochasztikus processz algebrák
- PRISM: Probabilistic Symbolic Model Checker
  - GreatSPN kiterjesztése
  - BDD alapú reprezentációval kombinálva az állapottér kezelése
- MRMC Markov Reward Model Checker
  - Diszkrét idejű Markov-lánc is használható
  - CSRL: CSL kiterjesztése reward hozzárendeléssel
  - Reward: Költség/haszon megadása
    - Állapotokhoz: Rate reward (integrálható időtartamra)
    - Átmenetekhez: Impulse reward (összegezhető a tüzelő átmenetekre)

PRISM


PRISM 3.0.beta1
File Edit Model Properties Options
Properties list: /data/private/luser/prism-examples/cluster/cluster.csl
Properties
S=? ["premium"]
S=? [!"minimum"]
P>=1 [true U "premium"]
P=? [true U<=T !"minimum"]
P=? [true U[T,T] !"minimum" {!"minimum"}{max}]
P=? [true U<=T "premium" {"minimum"}{min}]
P=? ["minimum" U<=T "premium" {"minimum"}{min}]
P=? [!"minimum" U>=T "minimum" {!"minimum"}{max}]
R=? [I=T {!"minimum"}{min}]
R=? [C<=T]
R=? [C<=T]
e that QOS drops below minimum quality within T time units (from the initial state)
Constants
Name Type Value
T double
Labels
Name Definition
minimum (left_n>=k&Toleft_n)|(right_n>=k&Tori...
premium (left_n>=left_mx&Toleft_n)|(right_n>=r...
Experiments
Property Defined Const... Progress Status Method
P=? [true U[T... T=0.0:1.0E-... 660/660 (100%) Done Verification
P=? [true U[T... N=3,T=0.0:1... 101/101 (100%) Done Simulation
P=? [true U[T... N=3,T=0.0:1... 44/101 (43%) Stopped Verification
P=? [true U<... N=3,T=0.0:1... 21/21 (100%) Done Verification
P=? [true U<... N=3:1:5,T=0... 63/63 (100%) Done Verification
Graph1 Graph2 Graph3 Graph4 Graph5
New Graph
Probability
0.00002
0.00001
0
0
10
20
T
N=3
N=4
N=5
Model Properties Simulator Log
Running experiment... done.

CSL használata QoS formalizálására I.



- Követelmények:
  - Rendelkezésre állás nagyobb 99%-nál:

    $$S_{\geq 0.99}(\text{Premium} \vee \text{Minimum})$$

  - Hosszú távon legalább 90% valószínűséggel Premium szolgáltatás:

    $$S_{\geq 0.9}(\text{Premium})$$

CSL használata QoS formalizálására II.

- Követelmények (folytatás):
  - Annak a valószínűsége kisebb 10%-nál, hogy 85 időegység alatt a szolgáltatási szint Minimum alatti lesz:

    $$P_{<0.1}(\mathrm{F}^{[0,85]}\ \mathrm{Failure}) = P_{<0.1}(\mathrm{true}\ \mathrm{U}^{[0,85]}\ \mathrm{Failure})$$

  - Lehetőség van a Premium szolgáltatás szint elérésére:

    $$P_{>0}(\mathrm{F}\ \mathrm{Premium}) = P_{>0}(\mathrm{true}\ \mathrm{U}^{(0,\infty)}\ \mathrm{Premium})$$

  - Ha kezdetben hibás, akkor a hiba kisebb mint 30% valószínűséggel áll fenn 2 időegység múlva:

    $$\mathrm{Failure} \Rightarrow P_{<0.3}(\mathrm{F}^{[2,2]}\ \mathrm{Failure})$$

  - Annak a valószínűsége legfeljebb 20%, hogy kezdeti hiba esetén a helyreállítás több mint 15 időegységet igényel:

    $$\mathrm{Failure} \Rightarrow P_{\leq 0.2}(\mathrm{Failure}\ \mathrm{U}^{[15,\infty)}\ (\mathrm{Minimum} \vee \mathrm{Premium}))$$

CSL használata QoS formalizálására III.

- Követelmények (folytatás):
  - 1%-nál kisebb a valószínűsége, hogy 9 időegység alatti folyamatos működés után egy időegységen belül hibásodik meg:

$$P_{<0.01}((\text{Premium} \vee \text{Minimum})\ \mathrm{U}^{[9,10]}\ \text{Failure})$$

  - Annak a valószínűsége, hogy Minimum szolgáltatási szint esetén 5 időegységen belül (ezalatt legalább a Minimum szintet megtartva) Premium szint nyújtható, több mint 70%:

$$\text{Minimum} \Rightarrow \mathrm{P}_{>0.7}(\text{Minimum}\ \mathrm{U}^{[0,5)}\ \text{Premium})$$

Összefoglalás

- Motiváció: Szolgáltatásminőségi követelmények verifikációja
  - QoS, SLA
- Alapszintű modell: CTMC, állapotcímkézéssel
  - Magasabb szintű modellekből leképezhető
  - Megoldás: Állandósult állapotbeli és tranziens analízis
- Követelmények formalizálása: CSL
  - Szintaxis: Állapot- és útvonal kifejezések
  - Szemantika: CTMC fogalmakkal
- Modellellenőrzés
  - Modell és követelmény együttes átalakításával egyszerűsíthető
- Eszközök
- Követelmények (példák)