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: QoS, SLA formalizálása

- Nem tisztán elérhetőségi jellegű követelmények
  - QoS: Quality of Service
  - SLA: Service Level Agreement
- Jellemzőek a követelményekre:
  - Adott szolgáltatási szintek valószínűségei
    - Példa: Rendelkezésre állás, mint aszimptotikus valószínűség
  - 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 85 időegység alatt a szolgáltatási szint Minimum alá csökken.
  - Annak a valószínűsége, hogy Minimum szolgáltatási szint elérése esetén 5 időegységen belül Premium szint nyújtható, több mint 70%.

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 (steady-state) – valsz.
  - Tranziens analízis (transient measures) – valsz. időfv.
- Megoldási módok:
  - Analitikus („képlettel”)
  - Numerikus („iterálva”)
  - Szimulációval („kimérve”)

Folytonos idő
Diszkrét állapotok
Állapotátmeneti gyakoriság

Markov folyamatok

- Olyan sztochasztikus folyamat, amelyik kielégíti a Markov tulajdonságot:

  $P\{X(t)=x \mid X(t_n)=x_n, X(t_{n-1})=x_{n-1}, \ldots, X(t_0)=x_0\} = P\{X(t)=x \mid X(t_n)=x_n\}$

  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
  - A Markov folyamatnak nincs „emlékezete” a korábbi állapotokról
- Diszkrét állapotterű Markov folyamatok: Markov láncok
  - Diszkrét állapotokban való tartózkodás idejével (tartási idő) jellemezhetők a trajektóriák
  - Tartási idő negatív exponenciális eloszlású
    - Az egyetlen eloszlásfüggvény, ami a Markov tulajdonságot teljesíti
    - Bármely időpillanatban a maradék tartási idő nem függ attól, hogy eddig mennyi időt töltött a folyamat az adott állapotban

Folytonos idejű Markov láncok (CTMC)

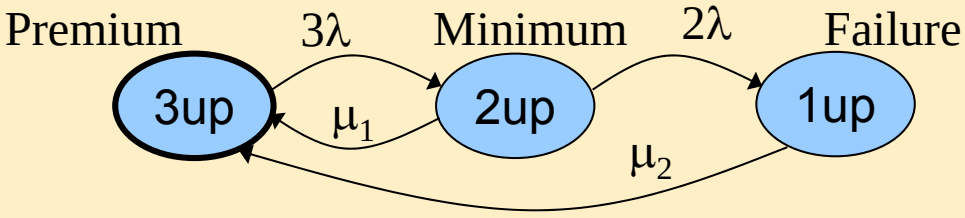
- CTMC: Continuous Time Markov Chain
  - Folytonos idő paraméter, diszkrét állapottér
- Jelölések, tulajdonságok:
  - Diszkrét állapotok: s_0, s_1, ..., s_n
  - Állapotátmeneti valószínűség: $Q_{ij}(t_{n-1},t_n)= P\{S(t_n)=s_j \mid S(t_{n-1})=s_i\}$
  - Homogén Markov-folyamat: $Q_{ij}(t,t+\Delta t)= Q_{ij}(\Delta t)$
    - Állapotátmeneti valószínűség nem változik az idő függvényében
  - Állapotátmeneti intenzitás (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: $P\{\text{s-ben marad t ideig}\} = e^{-E(s)t}$

Példa: Megbízhatósági modellezés Markov láncokkal

- Architektúra: Triple Modular Redundancy
  - Állapotok jellemzése a szolgáltatás szempontjából:
    - 3 egység jó (3up): Premium
    - 2 egység jó (2up): Minimum
    - 1 vagy kevesebb egység jó (1up): Failure
  - Állapotátmenetek (exponenciális eloszlású időzítés):
    - Egy egység meghibásodása: λ meghibásodási tényező
    - Egy egység javítása: μ_1 javítási tényező
    - Teljes rendszer javítása: μ_2 javítási tényező



Folytonos idejű Markov-láncok (jelölések)

- CTMC=(S,$\underline{\boldsymbol{R}}$)

  S állapotok

  $\underline{\boldsymbol{R}}$: $S\times S\to R_{\geq 0}$ állapotátmeneti gyakoriság (ráta) mátrix

  - P{s-ből s'-be megy át t időn belül} = $1-e^{-R(s,s')t}$
  - $\underline{E}(s) = \sum_{s'\in S} R(s,s')$ állapot elhagyás összesített gyakorisága
  - P{s állapot elhagyása t időn belül} = $1-e^{-E(s)t}$
  - $\underline{\boldsymbol{Q}} = \underline{\boldsymbol{R}} - \text{diag}(\underline{E})$ „infinitezimális generátormátrix"

- Útvonal:

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

  $\sigma@t$ az állapot a t időpillanatban

  Path(s) az s-ből induló útvonalak halmaza

  Prob(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:

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

Itt kb.: Van javítás minden állapotból (nincs nyelő)

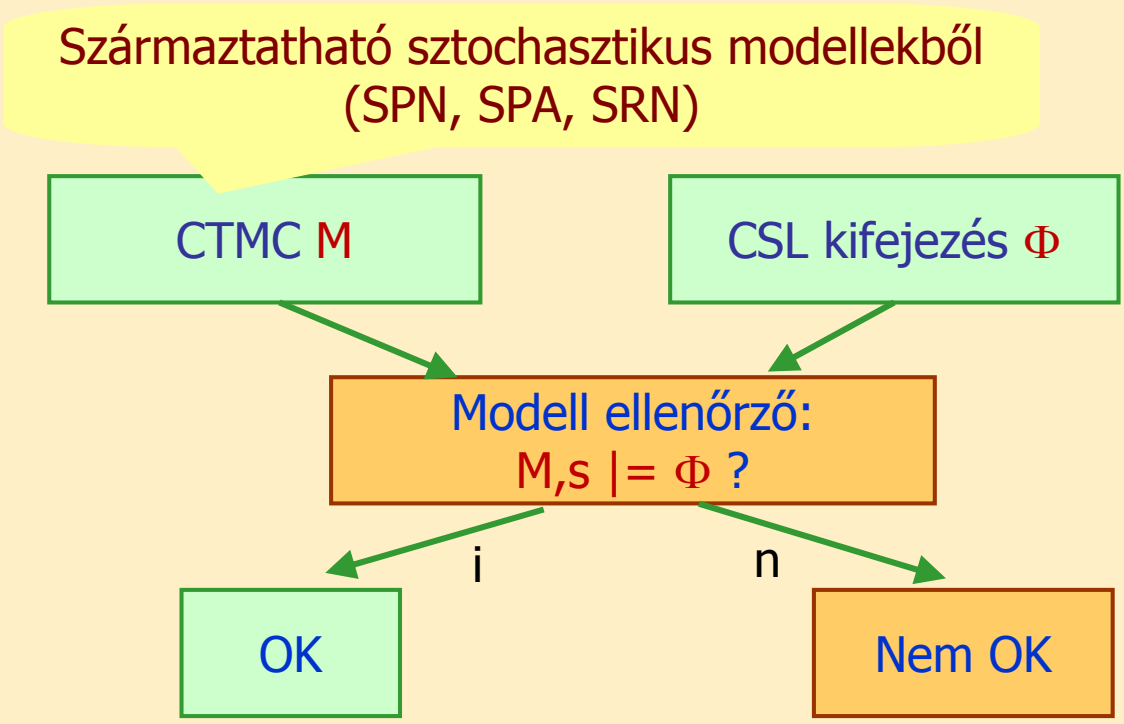
- Állandósult állapot (véges állapotú és irreducibilis CTMC):
  - $\pi(s,s') = \lim_{t\to\infty}\pi(s,s',t)$ - s-ből indulva az állapotok valószínűsége
  - $\underline{\pi}(s)$ az állapotok valószínűsége (sorvektor)
  - $\pi(s,S') = \sum_{s'\in S'}\pi(s,s')$ egy állapothalmaz valószínűsége
  - CTMC állandósult 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
  - Állapotokban való tartózkodás valószínűsége (állandósult állapotban, illetve időfüggvénnyel)
  - Állapot elhagyás gyakorisága (ráta)
- CTL analógia: Állapot- illetve útvonal kifejezések
  - Állapotban értelmezett útvonal kvantorok: A, E
  - Útvonalon értelmezett operátorok: F, G, X, U
- CSL: Continuous Stochastic Logic
  - Állapotokra és útvonalakra vonatkozó valószínűségi kifejezések és időtartamok megadása
  - Modell ellenőrzés „gombnyomásra” a CTMC alapján

Modell ellenőrzés



Continuous Stochastic Logic: Szintaxis

- Kiterjesztések a CTL-hez képest:
  - Valószínűségi operátorok:
    - Állandósult állapotban: állapot-kifejezések által megadott állapot-halmazokban való tartózkodás valószínűsége
    - Útvonal-kifejezések által megadott útvonal bejárásának valószínűsége (tranziens analízis)
  - Időtartományok megadása:
    - Útvonal kvantorokhoz időintervallum megadása: az adott időintervallumon belüli bekövetkezés (X, U)
- Jelölések:

  I intervallum, pl. [0, 12), [15,∞)

  p valószínűség

  ~ az összehasonlítás operátora, pl. ≥, ≤, <, >

CSL állapot-kifejezések

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

    P{olyan állapotban tartózkodik, ahol Φ igaz} ~ p
    - Példa: $S_{>0,8}$(Minimum∨Premium)
  - $P_{\sim p}(\varphi)$ - olyan utak bejárásának valószínűsége ~p, amelyeken φ igaz

    P{olyan utat jár be, ahol φ igaz} ~p
    - Példa: $P_{>0,7}$(true U Premium)

CSL útvonal-kifejezések

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

CSL szemantika

- M=(S,***R***,L) egy CTMC az állapotok címkézésével
  - L: $S \rightarrow 2^{AP}$ 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. $\pi(s, Sat(\Phi)) \sim p$,

    azaz $s \in Sat(S_{\sim p}(\Phi))$ a.cs.a. $\sum_{s' \in Sat(\Phi)} \pi(s,s') \sim p$

    s-ből indulva Sat(Φ) áll. állapotban való tartózkodás vsz. ~p
  - M,s |= $P_{\sim p}(\varphi)$ a.cs.a. $Prob(s, \sigma \mid \sigma|=\varphi) \sim p$,

    azaz $s \in Sat(P_{\sim p}(\varphi))$ a.cs.a. $\sum_{\substack{\sigma \in Path(s) \\ \sigma|=\varphi}} \text{Prob}(s,\sigma) \sim p$

    σ|=φ útvonal bejárás vsz. ~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 modell ellenőrzés

- $S_{\sim p}(\Phi)$ 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, de 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 átalakítás úgy, hogy elég legyen t-re egy tranziens analízis
    - Átalakítás: M→M', $\Phi \rightarrow \Phi'$
    - Bizonyítandó: M,s $\models \Phi$ ekvivalens 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 |= $\Phi_1 \, U^{[0,t)} \, \Phi_2$ ellenőrzése ekvivalens

    M',s |= true $U^{[t,t]} \, \Phi_2$ ellenőrzésével;

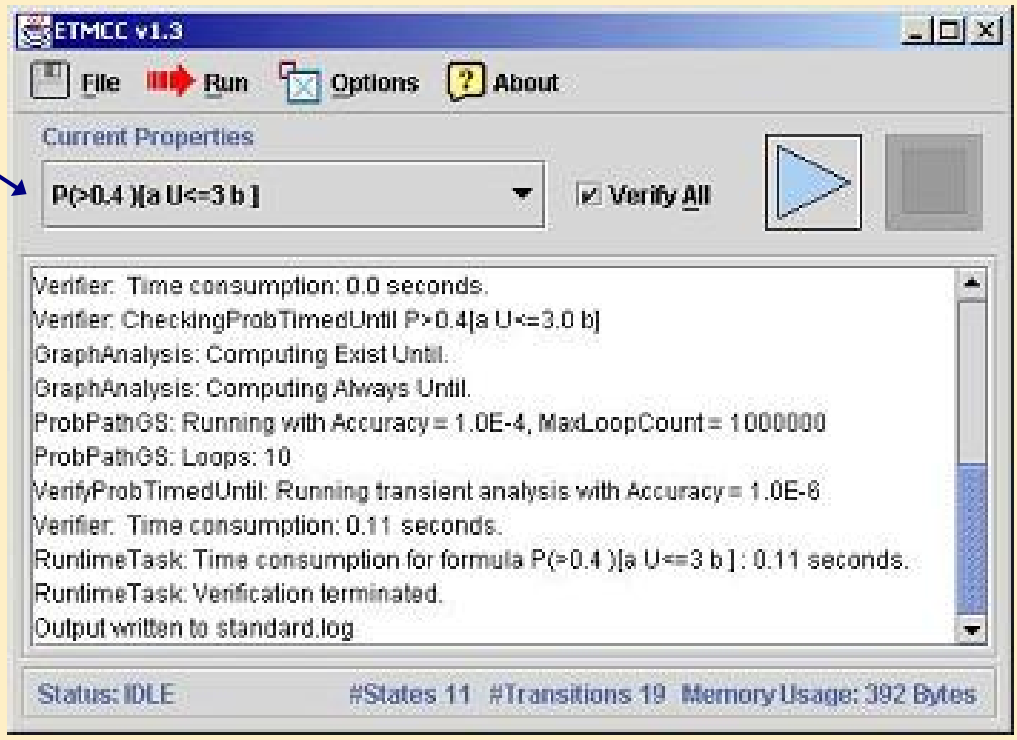
    itt t-re tranziens analízis elég az ellenőrzéshez!

CSL modell ellenőrzők

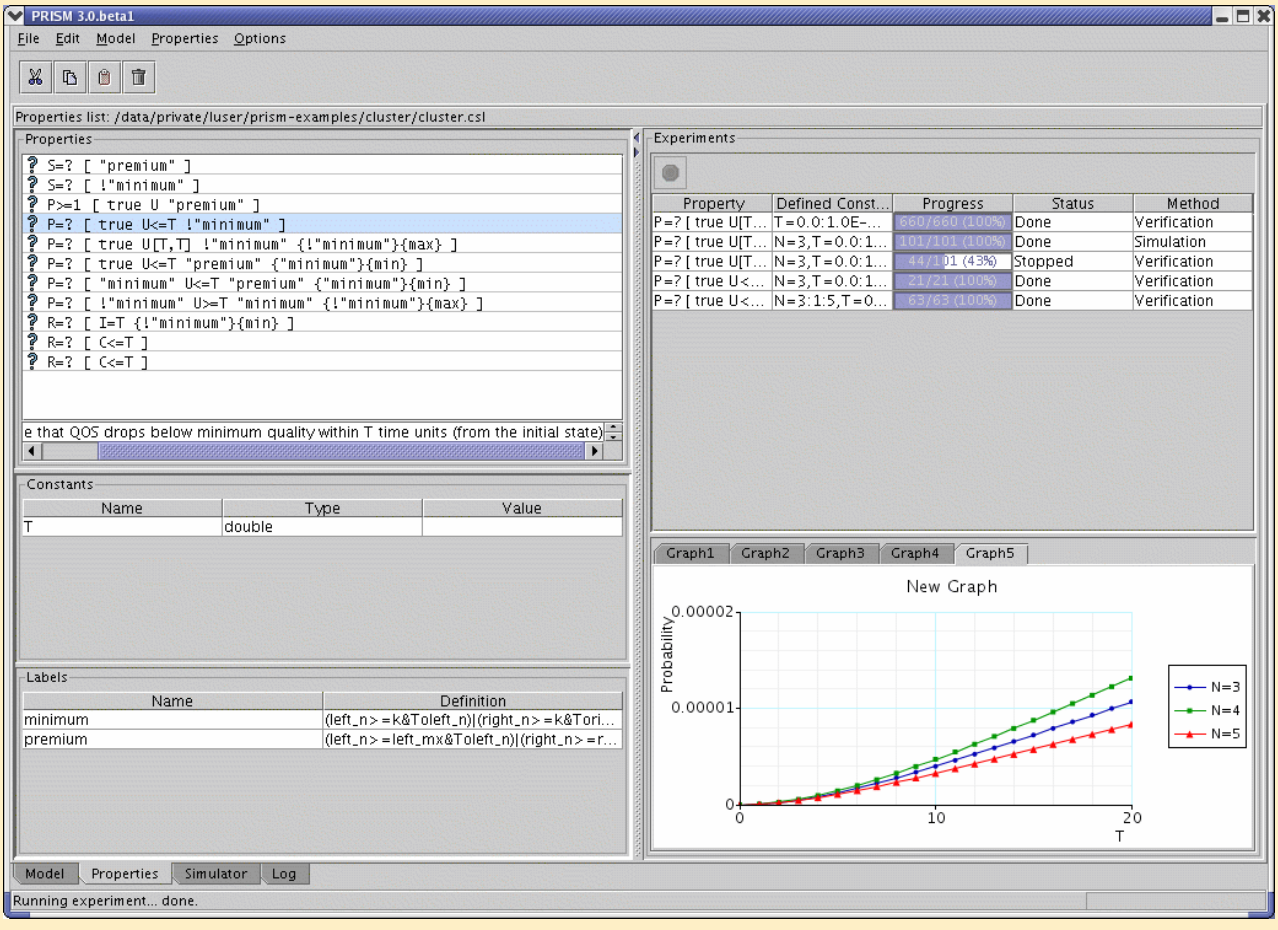
- ETMCC: Erlangen-Twente Markov Chain Checker (E|-MC^2)
  - Az első megvalósítás
  - Markov-láncok
  - Sztochasztikus processz algebrák
- PRISM: Probabilistic Symbolic Model Checker
  - GreatSPN kiterjesztés
  - BDD alapú reprezentációval kombinálva
- MRMC Markov Reward Model Checker
  - Diszkrét idejű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

ETMCC

CSL kifejezések

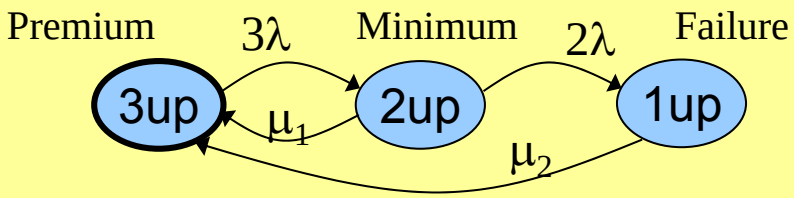


PRISM



CSL használata QoS formalizálására I.

TMR struktúra, AP={Premium, Minimum, Failure}



- Követelmények:
  - Hosszú távon legalább 70% valószínűséggel Premium szolgáltatás:

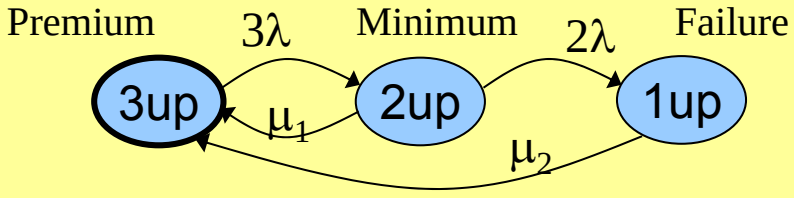
$$S_{\geq 0.7}(\text{Premium})$$

  - Hosszú távon kisebb a valószínűsége 5%-nál, hogy Minimum alatti szolgáltatás lesz:

$$S_{<0.05}(\text{Failure})$$

CSL használata QoS formalizálására II.

TMR struktúra, AP={Premium, Minimum, Failure}



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

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

  - 20%-nál kisebb valószínűséggel lesz 10 időegység múlva hibás:

$$P_{<0.2}(F^{[10,10]}\ \text{Failure})$$

  - Bármikor lehetőség van a Premium szolgáltatás szint visszaállítására:

$$P_{\geq 1}(F\ \text{Premium}) = P_{\geq 1}(\text{true}\ U^{(0,\infty)}\ \text{Premium})$$

CSL használata QoS formalizálására III.

- Annak a valószínűsége kisebb 10%-nál, hogy 85 időegység alatt a szolgáltatási szint Minimum alá csökken:

$$P_{<0.1}(F^{[0,85]}\ \text{Failure})$$

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

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

- Annak a valószínűsége legfeljebb 20%, hogy a hiba utáni helyreállítás több mint 15 időegységet vegyen igénybe:

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