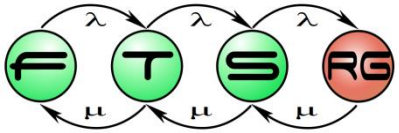
Valószínűségi modellellenőrzés Markov döntési folyamatokkal

Hajdu Ákos

Szoftver verifikáció és validáció

2015.12.09.

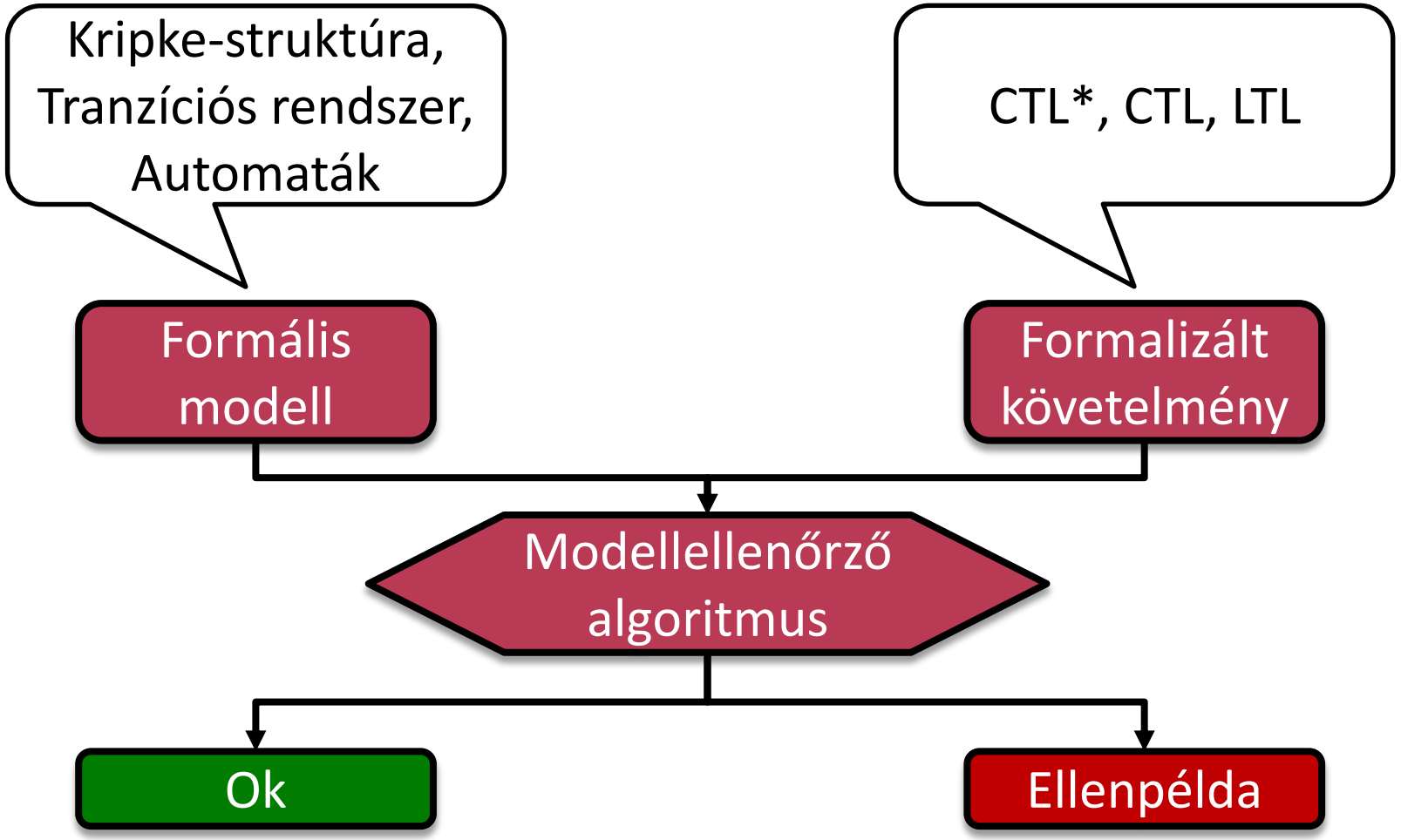


Forrás / Source

- Ez a prezentáció David Parker előadása alapján készült, amelyet az AVACS'15 iskolában mutatott be
- This presentation is mainly based on the lecture of David Parker presented in the AVACS'15 school

http://prismmodelchecker.org/lectures/avacs15/

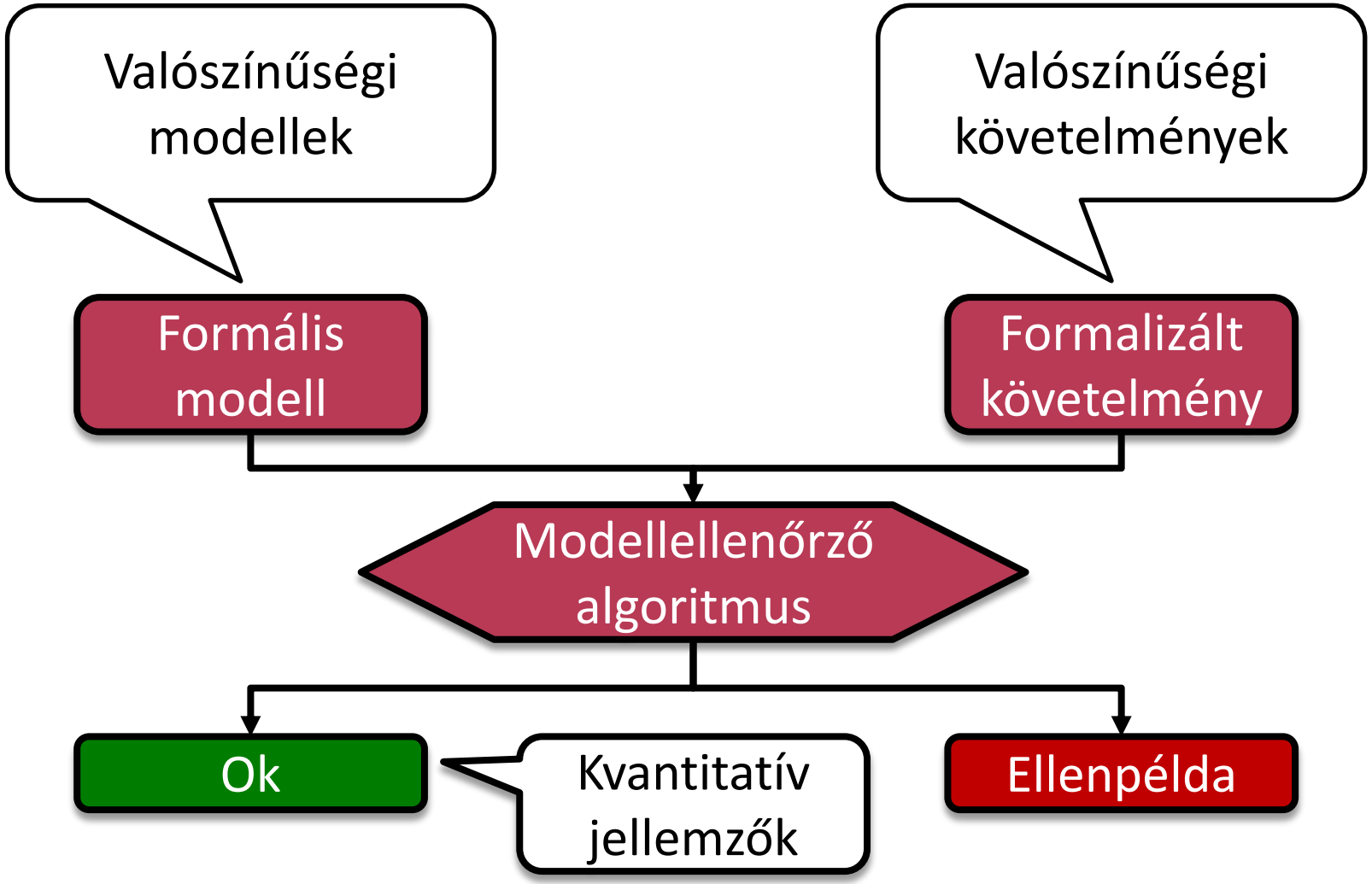
Ismétlés - modellellenőrzés



Motiváció

- Előre nem jelezhető, véletlenszerű viselkedés
  - Fizikai komponensek hibája
  - Üzenetvesztés
  - Megbízhatatlan szenzorok
  - Véletlenszerű back-off
- Kvantitatív jellemzők vizsgálata
  - Nem csak helyesség
    - Megbízhatóság, időzítés, teljesítmény
  - Pl.: *„Kisebb, mint 0,001 a valószínűsége, hogy a légzsák a trigger után 0,02 másodpercen belül nem nyílik ki.”*

Ismétlés - modellellenőrzés



Valószínűségi modellek

	Tisztán valószínűségi	Valószínűségi és nemdeterminisztikus
Diszkrét idő	Diszkrét idejű Markov-lánc (DTMC)	Markov döntési folyamat (MDP)
Folytonos idő	Folytonos idejű Markov-lánc (CTMC)	Folytonos idejű MDP, interaktív MC, valószínűségi időzített automata, sztochasztikus automata

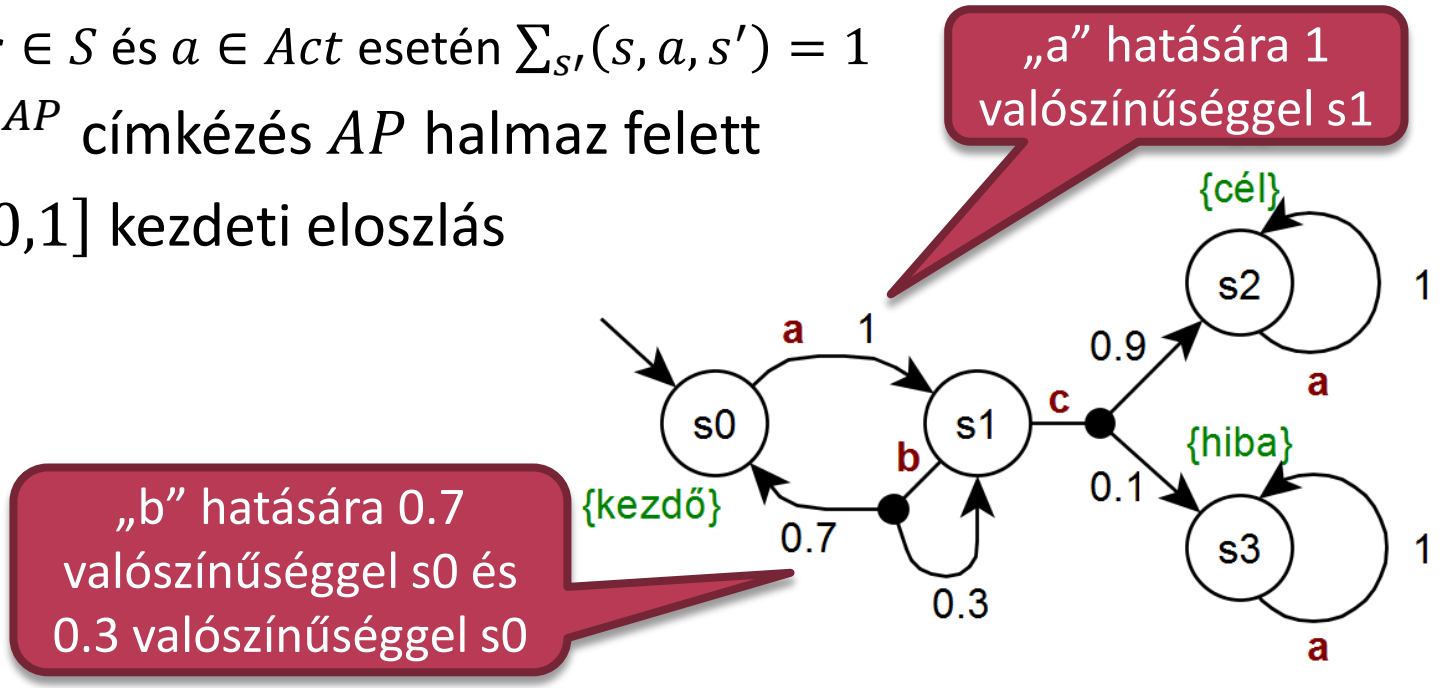
Valószínűségi követelmények

- Temporális logikák kiegészítése
  - Kvantitatív jellemzők: valószínűségek, időzítés, költség, jutalom
- Pl.: PCTL*: $\text{trigger} \rightarrow P_{\geq 0,999}[F^{\leq 20}\text{nyílás}]$
- Numerikus eredmények
  - $P_{\leq 0,1}[F\ \text{hiba}]$: *„Hiba valószínűsége kisebb, mint 0,1?”*
  - $P_{=?}[F\ \text{hiba}]$: *„Mennyi a hiba valószínűsége?”*
- Egzakt eredmények
  - Nem szimuláció

MARKOV DÖNTÉSI FOLYAMATOK (MDP)

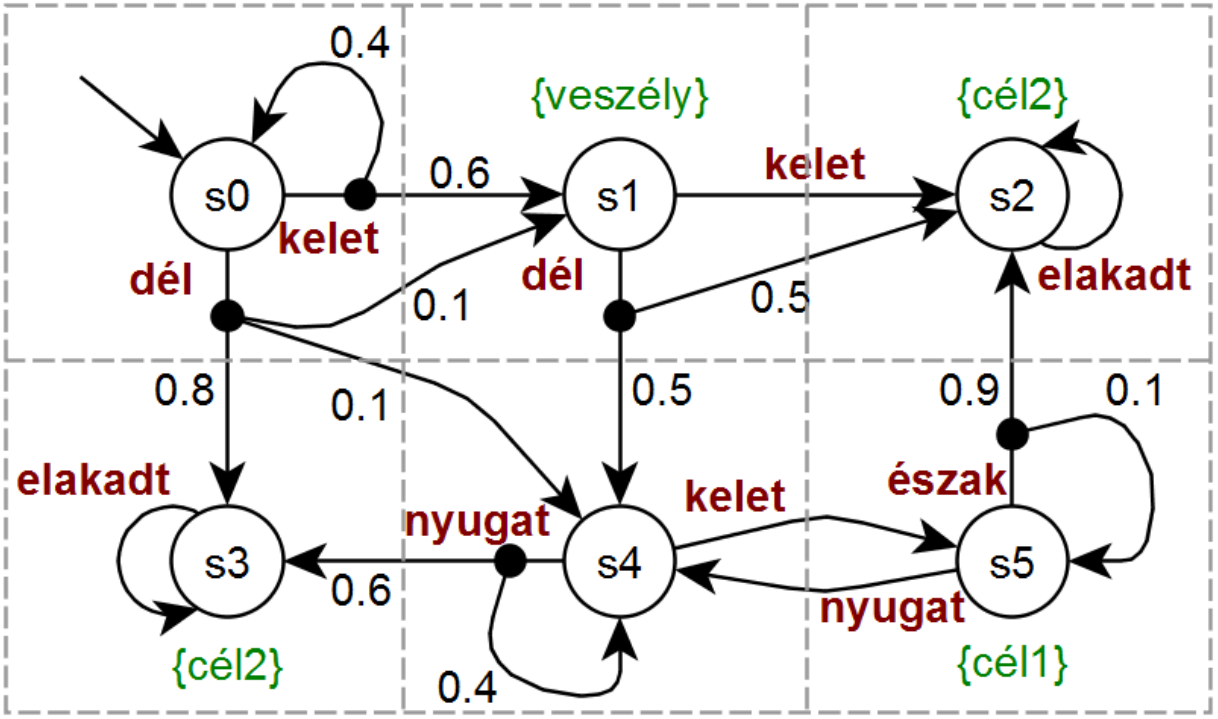
Markov döntési folyamatok

- DTMC kiegészítése nemdeterminizmussal
- Markov döntési folyamat $MDP = (S, Act, P, L, \mu)$
  - S: állapotok (véges) halmaza
  - Act: akciók (véges) halmaza
  - P: $S \times Act \times S \rightarrow [0,1]$ átmeneti valószínűség
    - Adott $s \in S$ és $a \in Act$ esetén $\sum_{s'}(s, a, s') = 1$
  - $L: S \rightarrow 2^{AP}$ címkézés AP halmaz felett
  - $\mu: S \rightarrow [0,1]$ kezdeti eloszlás



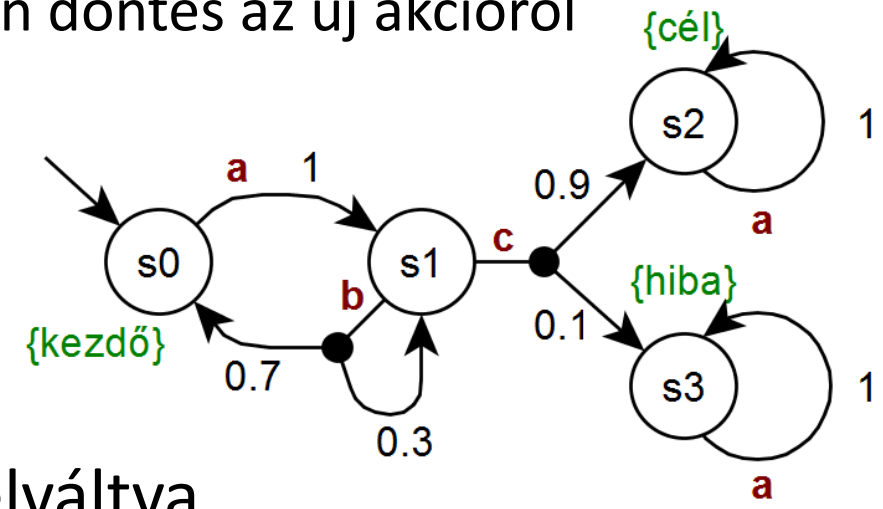
Markov döntési folyamatok

- Példa
  - Robot mozgása egy terepen
  - Akciók: robot döntései
  - Valószínűségek: környezeti hatások, zavarok



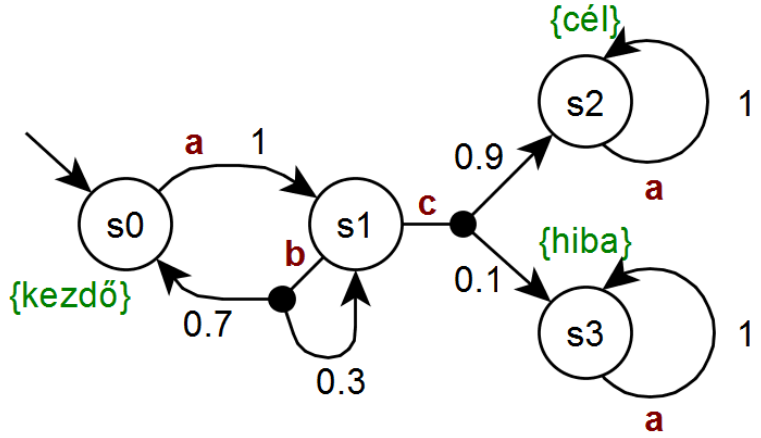
Markov döntési folyamatok

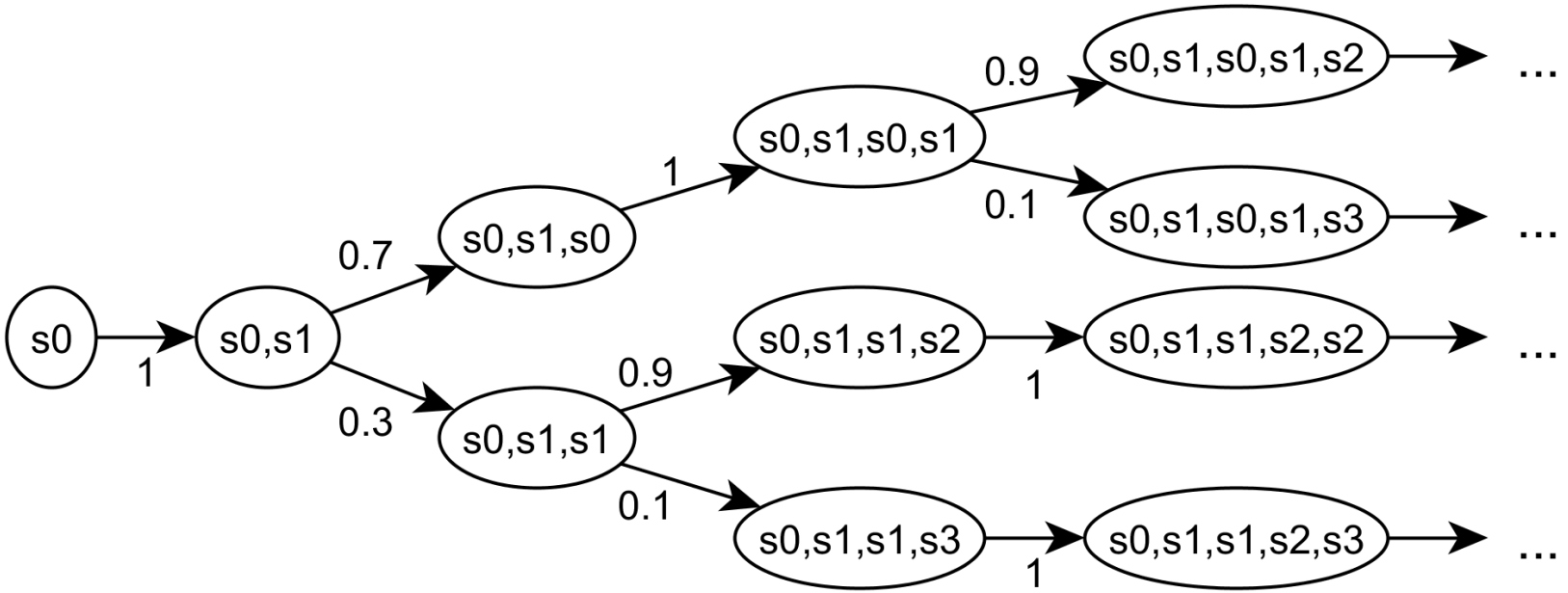
- Stratégia
  - Nemdeterminizmus feloldása
  - $D: S^* \rightarrow Act$
    - Eddigi állapotsorozat alapján döntés az új akcióról
  - Osztályozás
    - Memóriamentes
    - Véges memóriájú
    - Végtelen memóriájú
  - Példa: s1-ben „b” és „c” felváltva
    - Véges memória



Markov döntési folyamatok

- Stratégia
  - DTMC-vé alakít
  - Példa:
    - s1-ben „b” és „c” felváltva



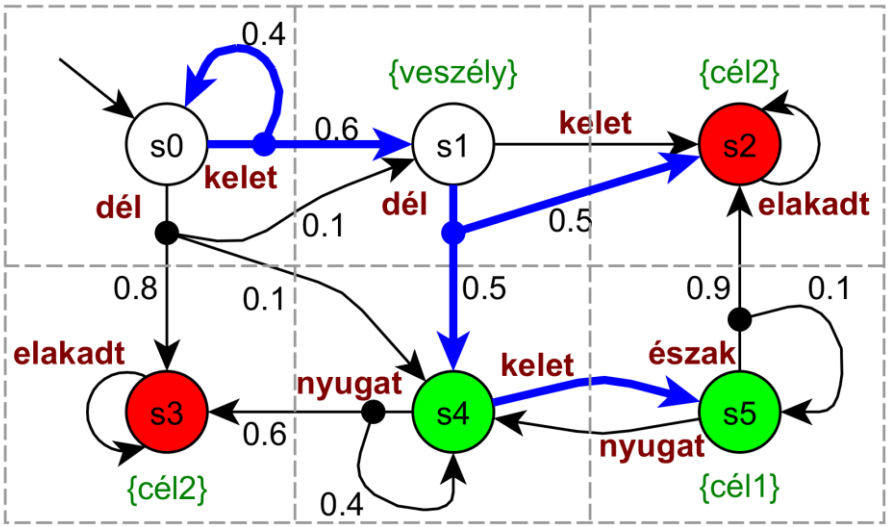


Valószínűségi modellellenőrzés

1. Verifikáció
   - Univerzális kvantálása a stratégiáknak
   - $P_{\leq 0,1}[F \text{ hiba}]$: *„Kisebb-e a hiba valószínűsége 0,1-nél az **összes** stratégia esetén?”*
2. Szintézis
   - Egzisztenciális kvantálása a stratégiáknak
   - $P_{>0,1}[F \text{ hiba}]$: *„**Van-e** olyan stratégia, amire a hiba valószínűsége 0,1-nél nagyobb?”*

- Duális problémák
  - Optimális értékekre (min/max) visszavezetés

Példa – Elérhetőség vizsgálata



Optimális stratégia:
s0: kelet
s1: dél
s2: -
s3: -
s4: kelet
s5: -

- $P_{\leq 0,6}[F \text{ cél1}]$ verifikáció
- $P_{\geq 0,4}[F \text{ cél1}]$ szintézis
- $P_{max=?}[F \text{ cél1}] = 0,5$
- Optimális stratégia
  - Memóriamentes
- Meghatározás
  - Gráf analízis
  - Numerikus módszerek

PLTL ellenőrzés

- PLTL: Probabilistic LTL
  - $P_{max=?}[(G\ \neg\text{veszély}) \wedge (GF\ \text{cél1})]$: *„Veszély elkerülése miközben cél1 látogatása végtelen sokszor.”*
  - $P_{max=?}[\neg\text{zóna3}\ U\ (\text{zóna1} \wedge F\ \text{zóna4})]$: *„Zóna1, majd zóna4 látogatása zóna3 nélkül.”*
- Ellenőrzés
  - φ formula átalakítása determinisztikus automatára: A_φ
  - $M \times A_\varphi$ konstruálása és megoldása
    - Elérhetőségre vezethető vissza
    - Optimális stratégia: véges memória

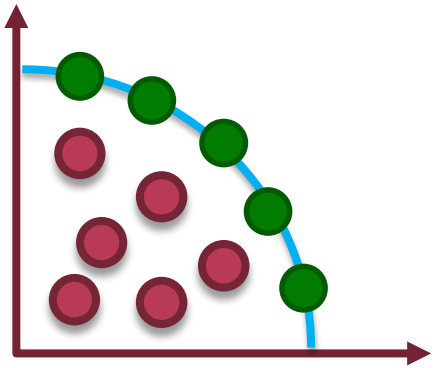
További tulajdonságok

- Költségek és jutalmak
  - Várható, akkumulált érték
    - $R_{min=?}[F\ \text{cél2}]$: *„Optimális lépésszám cél2 eléréséhez.”*
    - $R_{max=?}[F\ \text{vége}]$: *„Worst-case várható idő a protokoll befejezésére.”*
    - Elérhetőséghez hasonló
  - PLTL formula teljesítésének költsége
    - $R_{min=?}[\neg\text{zóna3}\ U\ (\text{zóna1}\ \wedge F\ \text{zóna4})]$: *„Zóna1, majd zóna4 meglátogatási idejének minimalizálása, közben zóna3 elkerülésével.”*
    - Automata módszer

KITERJESZTÉSEK

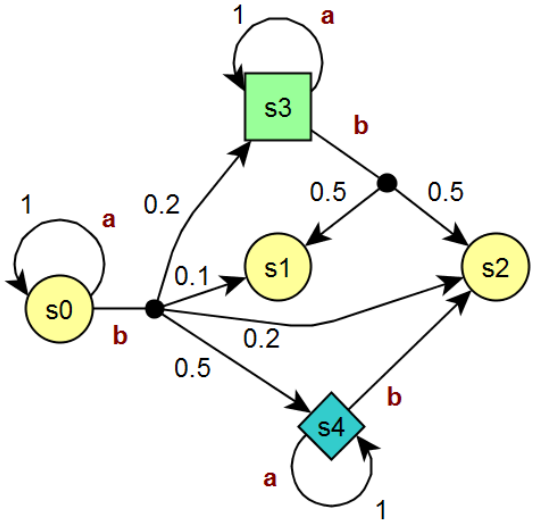
Többcélú modellellenőrzés

- „Trade-off” vizsgálata több cél között
- Megvalósíthatósági probléma
  - $multi\left(P_{>0,95}[F \text{ elküldve}], R^{idő}_{>10}\ [\text{akku}]\right)$
    - *„Van-e stratégia, ahol az üzenet 0,95 valószínűséggel el lesz küldve, miközben az akku élettartama több, mint 10 óra?”*
- Numerikus probléma
  - $multi\left(P_{max=?}[F \text{ elküldve}], R^{idő}_{>10}\ [\text{akku}]\right)$
    - *„Mi a max. valószínűsége az üzenet elküldésének, ha az akku élettartama több, mint 10 óra?”*
- Pareto probléma
  - $multi\left(P_{max=?}[F \text{ elküldve}], R^{idő}_{max=?}\ [\text{akku}]\right)$



Több játékos

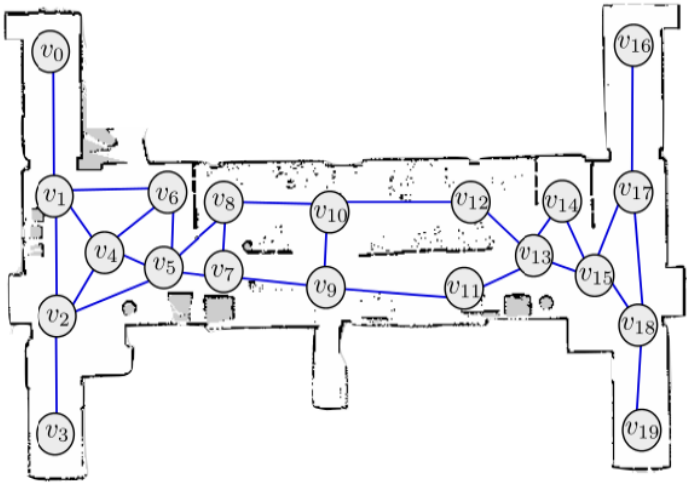
- Csomópontok játékosokhoz rendelve
  - Döntés az akcióról



- Követelmény: rPATL
  - Probabilistic alternating-time temporal logic with rewards
  - $\ll C \gg \varphi$: létezik-e a C-beli játékosoknak olyan stratégiája, hogy φ teljesül a többi játékostól függetlenül
  - $\ll \{1,2\} \gg P_{\geq 0,95}[F^{\leq 45}\text{vége}]$: *„Tud-e az 1-es és 2-es játékos úgy együttműködni, hogy 0,95 valószínűséggel 45 időegység alatt befejeződjön a protokoll a többiektől függetlenül?”*

Alkalmazás

- PRISM eszköz
  - Valószínűségi modellellenőrzés
- Alkalmazás
  - Robot navigáció
    - Bizonytalan környezet
    - Cél megfogalmazása PLTL-ben
    - Vezérlő szintézis



Hivatkozások

- Forejt, V., Kwiatkowska, M., Norman, G., & Parker, D. (2011). **Automated verification techniques for probabilistic systems.** In *Formal Methods for Eternal Networked Software Systems* (pp. 53-113). Springer Berlin Heidelberg.
- Kwiatkowska, M., Norman, G., & Parker, D. (2011, January). **PRISM 4.0: Verification of probabilistic real-time systems.** In *Computer aided verification* (pp. 585-591). Springer Berlin Heidelberg.
- Kwiatkowska, M., & Parker, D. (2013). **Automated verification and strategy synthesis for probabilistic systems.** In *Automated Technology for Verification and Analysis* (pp. 5-22). Springer International Publishing.
- http://www.prismmodelchecker.org/