Időt kezelő modellek és temporális logikák

Valósidejű rendszerek követelményeinek formalizálása és ellenőrzése

Majzik István

Budapesti Műszaki és Gazdaságtudományi Egyetem

Méréstechnika és Információs Rendszerek Tanszék

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

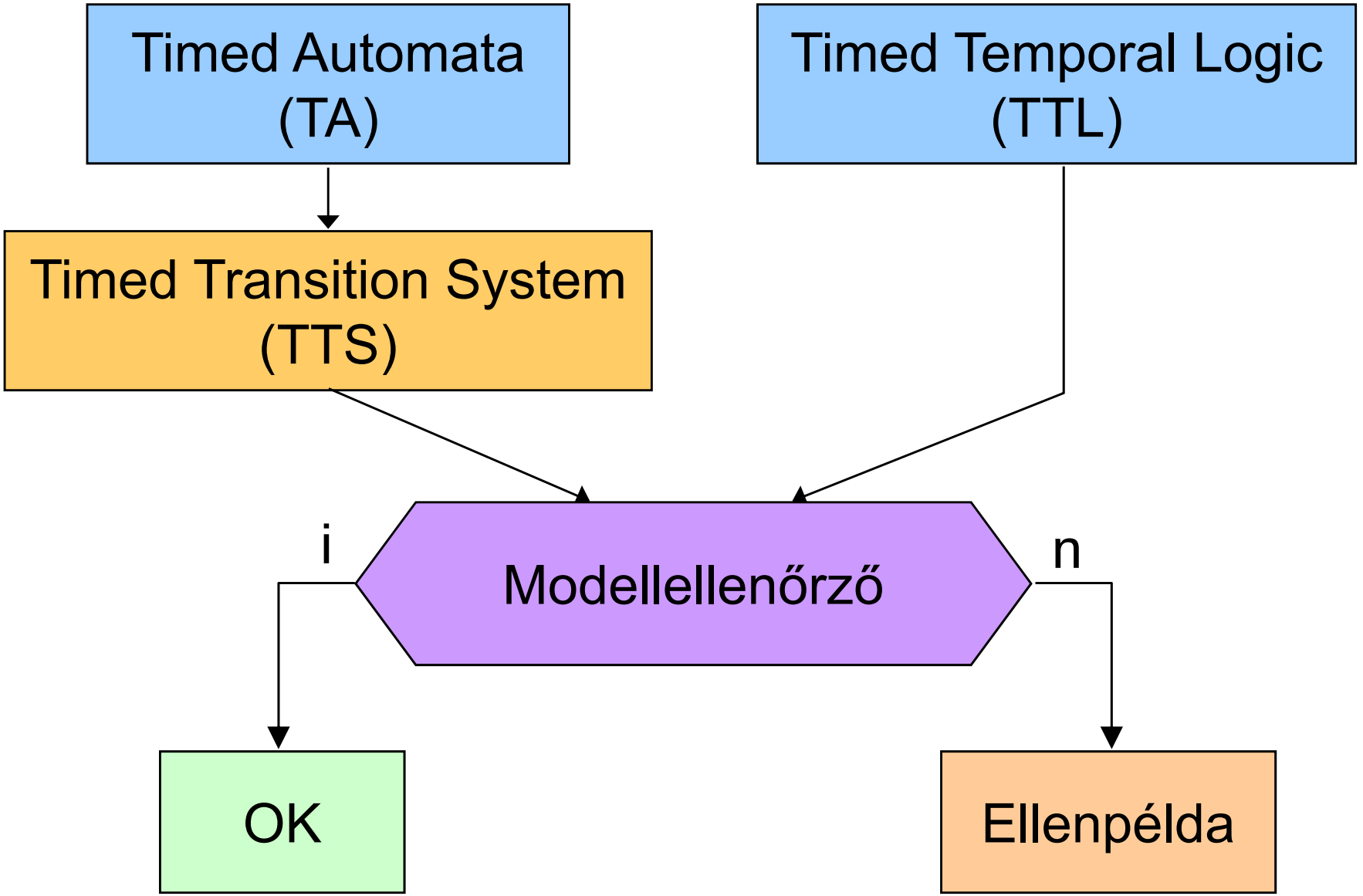
Valósidejű rendszerek modellezése

- Véges állapotú automata alapú leírások
  - Állapot-alapú, eseményvezérelt rendszerekhez
- Valós idejű órák az idő információ kifejezésére
  - Idő telik az állapotokban ill. az állapotátmenetek mentén
  - Feltételek az idő függvényében: Óra értékétől függően
  - Relatív időmérés: Óra resetelésével
- Tipikus ellenőrizendő követelmények
  - Adott időn belül adott tulajdonságú állapotba kerüljünk (határidő követelmény teljesítése)
    - Pl. kérésre adott időn belül válasz érkezzen
  - Adott idő után bizonyos tulajdonságú állapotba kerüljünk
  - Minden, adott időn belül elérhető állapotban igaz legyen egy adott tulajdonság

Megközelítés

- Mérnöki modell → Alapszintű formális modell
  - Az alapszintű formális modell mint a mérnöki modell „szemantikája” (leképzés a formalizáláshoz)
  - Modell ellenőrzés végrehajtása a formális modellen
- Minta:
  - UML állapottérkép → Kripke-struktúra (KS), ezen CTL követelmények
- Valósidejű modell ellenőrzéshez:
  - Timed Automata (TA) → Timed Transition System (TTS) ezen pedig Timed Temporal Logic (TL)

Modellellenőrzés



Alapszintű modell: Timed Transition System (TTS)

- Jelölések (állapotok és átmenetek tulajdonságai):
  - Atomi kijelentések: $AP = \{P, Q, \ldots\}$
  - Atomi akciók: $Act = \{a, b, c, \ldots\}$
  - Késleltetés akciók: $\Delta = \{\varepsilon(d) \mid d \in R_{\geq 0}\}$
- TTS definíció: $TTS = (S, s_0, \rightarrow, V)$ ahol
  - S állapotok halmaza
  - s_0 kezdőállapot
  - $\rightarrow \subseteq S \times L \times S$, ahol $L \in Act \cup \Delta$ (késleltetés is mint címke)
  - $V: S \rightarrow 2^{AP}$ állapotok címkézése

Mérnöki modell: Timed Automata (TA)

- Automata + órák
  - Konkurens (rendszer)órák
  - Azonos ütemben (rátával) haladnak
  - Értékük hozzáférhető feltételekben, invariánsokban
  - Resetelhetőek akciókban, egymástól függetlenül
- Jelölések:
  - C = {x, y, z, …} órák
  - B(C) óra-kifejezések, egy óra-kifejezés g-vel jelölve
    - Szintaxis: g ::= x~n | x-y~n | g $\wedge$ g
      ahol ~ $\in$ {$\leq$, $\geq$, =, <, >},
      és n természetes szám (konstans)

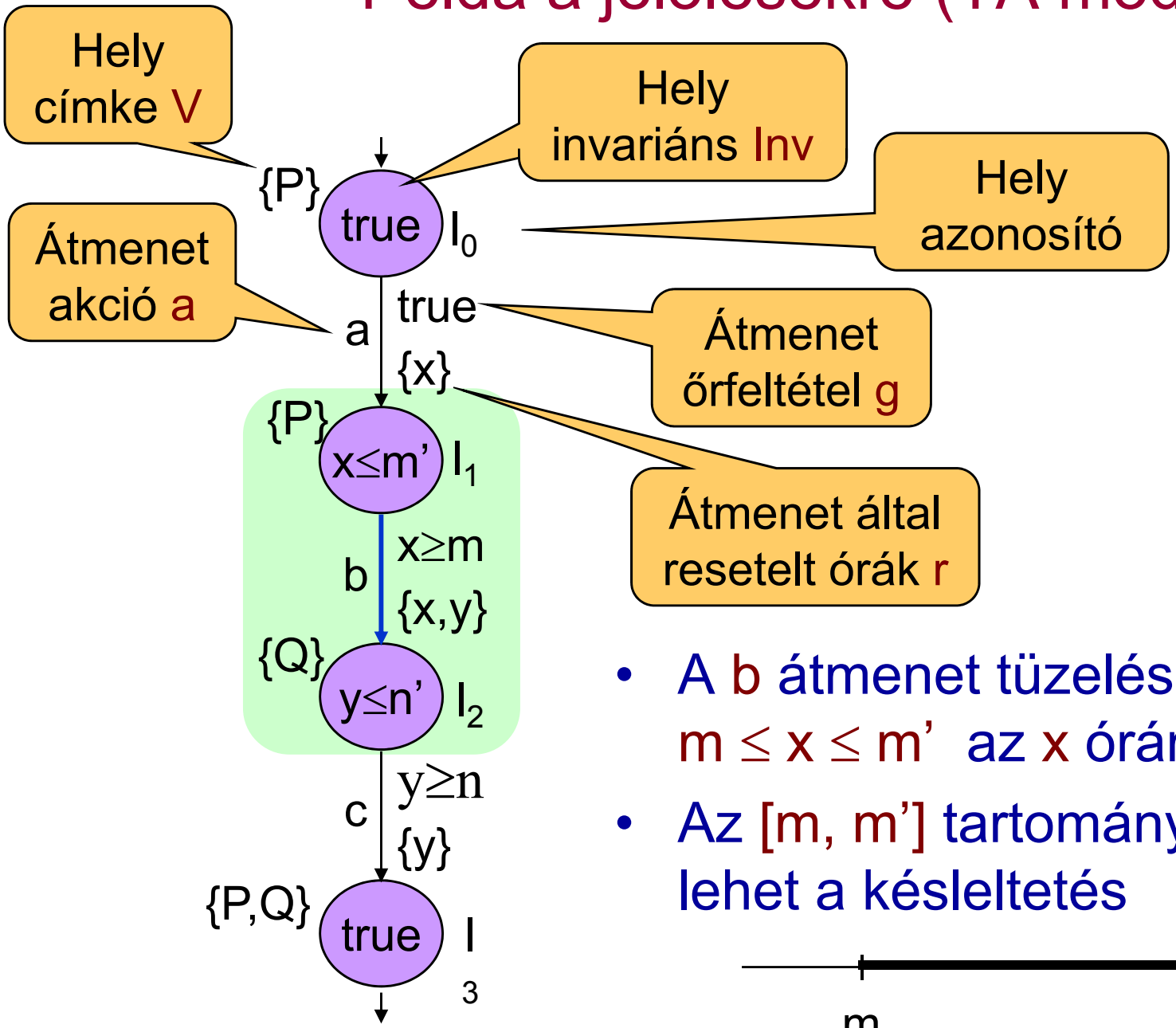
TA definíció

- Adott Act, AP, C mellett TA=(N, l_0, E, Inv, V) ahol
  - N vezérlési helyek (állapotok)
  - $l_0 \in N$ kezdeti hely – itt indul a rendszer, 0 az órák értéke
  - $E \subseteq N \times B(C) \times Act \times 2^C \times N$ élek halmaza, ahol egy él

    $$l \xrightarrow{g, a, r} l'$$

    itt
    - g: óra-kifejezés – ez mint engedélyező feltétel
    - a: akció – tevékenység az élhez rendelve
    - r: óra-halmaz – a resetelt órák halmaza
  - Inv: $N \rightarrow B(C)$ óra-invariánsok
    - Eddig növekedhetnek az órák az adott vezérlési helyen
  - V: $N \rightarrow 2^{AP}$ címkézés (a helyek tulajdonságai)

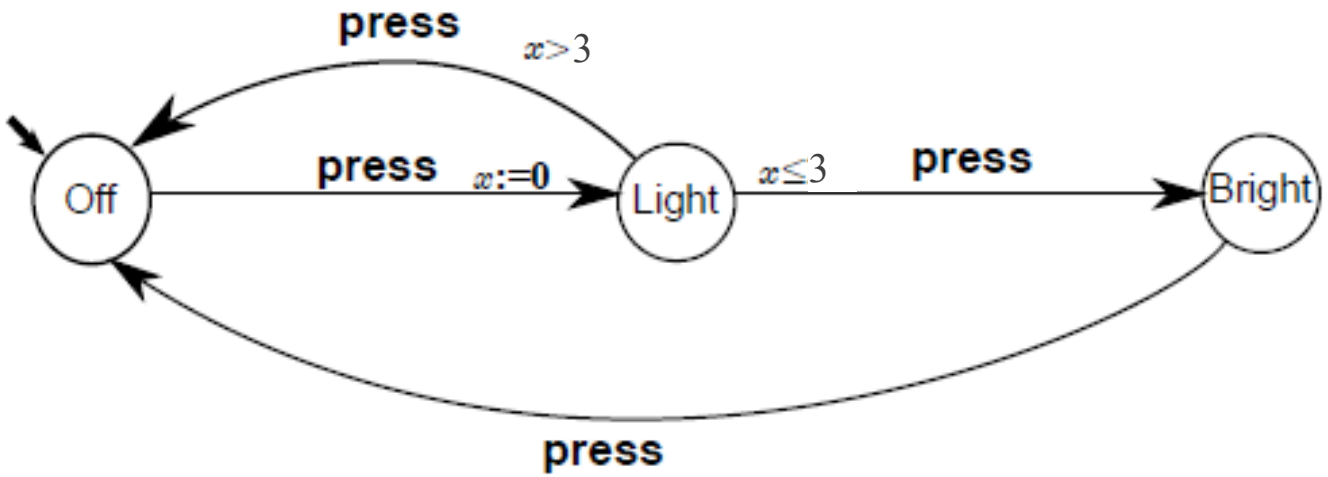
Példa a jelölésekre (TA modell)



- A b átmenet tüzelésének feltétele: $m \le x \le m'$ az x órára
- Az [m, m'] tartományban bárhol lehet a késleltetés

Egy egyszerű gyakorlati példa (TA modell)

- Villanykapcsoló
  - Kikapcsolt állapotban egy lenyomásra a halvány világítás bekapcsol
  - Ezután 3 másodpercen belüli újabb lenyomásra a fényes világítás bekapcsol, ezen időn túli lenyomásra kikapcsol
  - A fényes világítás állapotából lenyomásra mindig kikapcsol



TA szemantikája (1)

- Jelölések a szemantikához:
  - u: C $\rightarrow R_{\geq 0}$ óra-hozzárendelés
    - R^C a lehetséges óra-hozzárendelések halmaza C órahalmazhoz
    - $u \in R^C$ egy hozzárendelés, u(x) egy x óra értéke
  - u+d az óra-hozzárendelés növelése minden órára
    - Egy x óra esetén u(x)+d lesz az új érték
  - uv: hozzárendelések egyesítése órahalmazokra, ahol $u \in R^C$, $v \in R^K$ és K, C függetlenek: $C \cap K=0$
    - uv(x)=u(x) ha $x \in C$
    - uv(x)=v(x) ha $v \in K$
  - [C'$\rightarrow$0]u minden $x \in C'$ órára 0 lesz a hozzárendelés, egyébként marad az eredeti
  - g(u) egy g feltétel kiértékelése u hozzárendelés mellett
- TA *állapota*: (l, u) hely és óra-hozzárendelés

TA szemantikája (2)

- TA szemantikája egy TTS=(S, s_0, $\rightarrow$, V) ahol
  - S állapotok mint TA állapotai (l,u) alakúak
  - $s_0 = (l_0,u_0)$ kezdőállapot
  - $\rightarrow \subseteq S \times L \times S$ definiálható a következőképpen:
    - $(l,u) \rightarrow^a (l',u')$ lehetséges, ha van r, g úgy, hogy

$$l \xrightarrow{g,a,r} l' \text{ állapotátmenet van,}$$
$$g(u) \text{ őrfeltétel igaz,}$$
$$u' = [r \rightarrow 0]u \text{ az óra resetelés megtörténik}$$

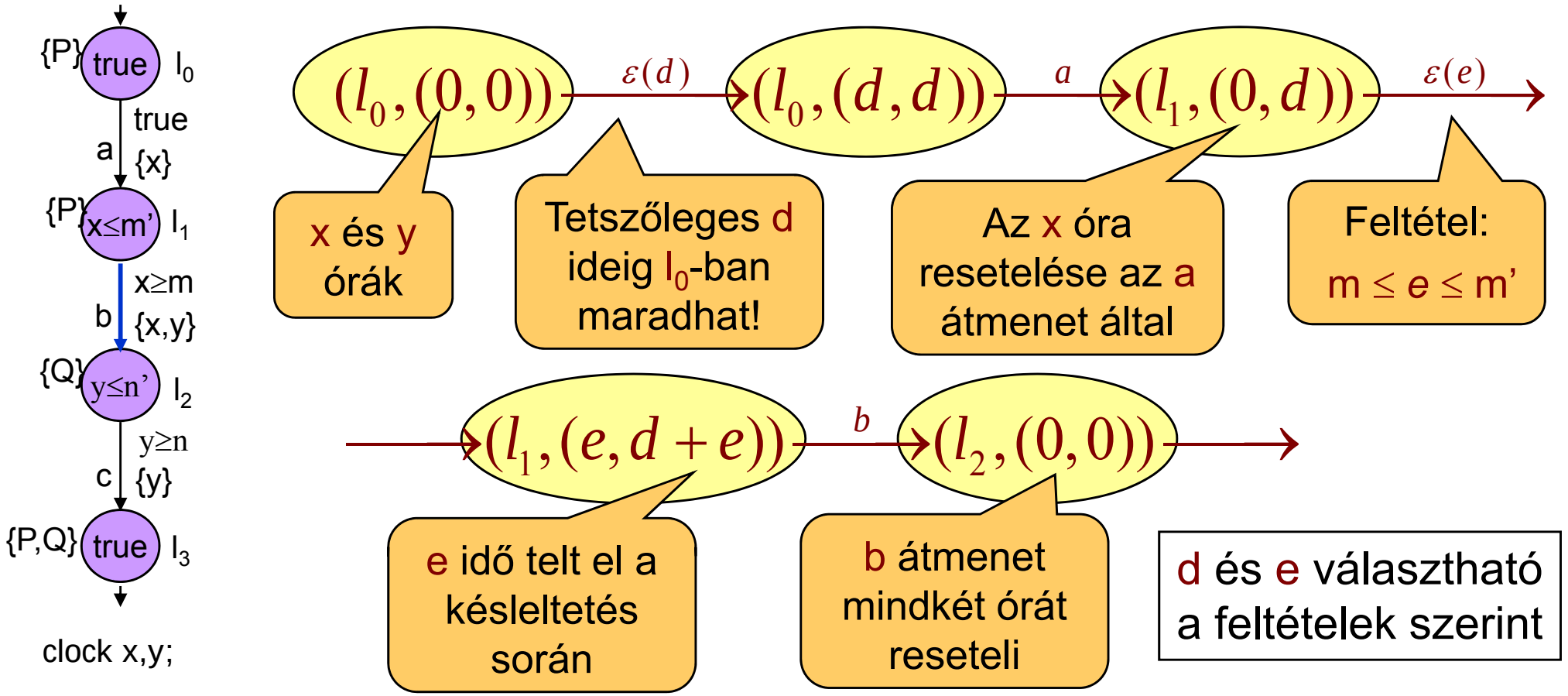
    - $(l,u) \rightarrow^{\varepsilon(d)} (l',u')$ lehetséges, ha

$$l = l' \text{ csomópont nem változik,}$$
$$u' = u + d \text{ eltelik } d \text{ idő,}$$
$$Inv(u') \text{ óra-invariáns teljesül}$$

  - V(l,u) = V(l) az állapotok címkézése

Példa a TA szemantikájára

- Egy TA esetén a szemantika egy TTS *halmaz!*
  - Ld. késleltetések értékei tartományokban (őrfeltételek és invariánsok szerint)
- Egy lehetséges TTS az előbbi TA esetén:



TA-k párhuzamos kompozíciója

- TA kompozíció: Automaták hálózata
  - Szinkronizáció az egyes automaták között
    - Együttlépő átmenetek
    - Tipikusan szinkron kommunikáció: Üzenet küldés és fogadás
  - Kompozíció általános meghatározása:
    - Milyen átmenetekre írjuk elő az együttlépést
    - Leírható: f szinkronizációs függvénnyel,
      ami akciókon (így implicit az átmeneteken) értelmezett
  - $TA_1 |_f TA_2$ kompozíció:
    - Szemantikája TTS-sel fejezhető ki
    - Előtte: TTS-ek kompozícióját kell áttekinteni

TTS-ek párhuzamos kompozíciója

- Paraméter: Szinkronizációs függvény f
  - f: $(Act \cup \{0\}) \times (Act \cup \{0\}) \rightarrow Act$
    ahol 0 a hiányzó akció helye (helyben maradáskor is)
- Kompozíció: $TTS_1 |_f TTS_2 = TTS_0$, ahol
  - $TTS_1=(S_1, s_{1,0}, \rightarrow_1, V_1)$, $TTS_2=(S_2, s_{2,0}, \rightarrow_2, V_2)$ és $TTS_0=(S, s_0, \rightarrow, V)$
  - $s_1 |_f s_2 \in S$ (a kompozíció szerint összeállított párok)
  - $s_0 = s_{1,0} |_f s_{2,0} \in S$ (kezdőállapot)
  - $\rightarrow$ induktívan definiálható:
    - $s_1 |_f s_2 \rightarrow^e s'_1 |_f s'_2$ ha $s_1 \rightarrow^a_1 s'_1$ és $s_2 \rightarrow^b_2 s'_2$ és f(a,b)=e
    - $s_1 |_f s_2 \rightarrow^{\varepsilon(d)} s'_1 |_f s'_2$ ha $s_1 \rightarrow^{\varepsilon(d)} s'_1$ és $s_2 \rightarrow^{\varepsilon(d)} s'_2$
  - $V(s_1 |_f s_2) = V_1(s_1) \cup V_2(s_2)$

TA párhuzamos kompozíció szemantikája

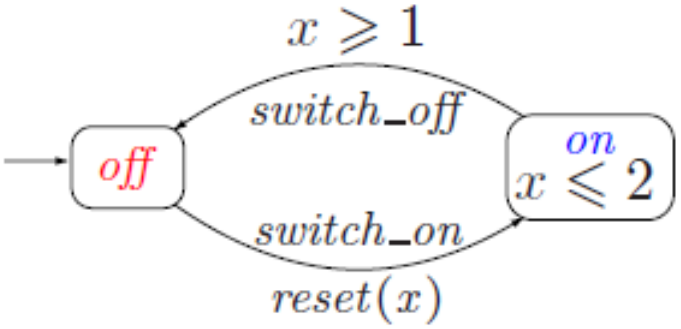
- $TA_1 |_f TA_2$ szemantikája $TTS_1 |_f TTS_2$ ahol
  - TA_1 szemantikája TTS_1, TA_2 szemantikája TTS_2
  - $TA_1 |_f TA_2$ egy jelölés automaták hálózatára (nem egy konkrét automata!)
    - Bár konstruálható olyan $TA_1 \otimes TA_2$ szorzat automata, hogy $TA_1 \otimes TA_2$ szemantikája $TTS_{TA1 \otimes TA2} \sim TTS_1 |_f TTS_2$ azaz biszimuláció ekvivalens (ld. később)
    - $TA_1 \otimes TA_2$ szorzat automata: állapotok: párosítás, invariánsok: konjunkció, órák: unió, élek: szinkronizálható élek
- UPPAAL esetén az f szinkronizációs fv:
  - f(a!,a?) együttes akció (a! „küldés” és a? „fogadás”)
  - f(a,0) egy automata akciója
  - f(0,a) egy automata akciója

Érdekességek időzített rendszerek modellezésében

- Nem realisztikus végrehajtási útvonalak: Megnehezítik az ellenőrzést
  - Idő konvergencia (time convergence): Végtelen késleltetés sorozat egy konkrét időponthoz konvergál
  - Időzár (timelock): Megáll az idő haladása
  - Zeno tulajdonság (zenoness): Végtelen sok akció végrehajtható véges idő alatt
- Kezelésük:
  - Az idő konvergenciára a modellellenőrzés során kell figyelni (lehetséges, de nem „fair” útvonalként kizárva)
  - Az időzár és a zeno tulajdonság a modell megfelelő kialakításával elkerülhetők

Idő konvergencia (time convergence)

- Példa modell:



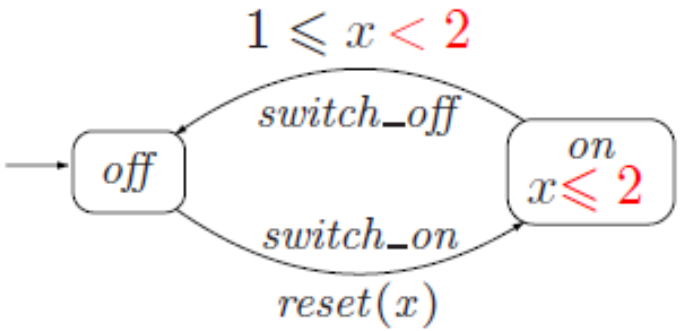
- Példa útvonal:

$$\langle off, 0\rangle \xrightarrow{2^{-1}} \langle off, 1-2^{-1}\rangle \xrightarrow{2^{-2}} \langle off, 1-2^{-2}\rangle \xrightarrow{2^{-3}} \langle off, 1-2^{-3}\rangle \ \ldots\ldots$$

- Idő konvergens útvonal általánosan:
  - Végtelen d_1, d_2, … késleltetés sorozat, ahol $d_1+d_2+\ldots$ összege d (konstans)
- Idő divergens útvonal:
  - Nem konstans végrehajtási idő (késleltetések összege)

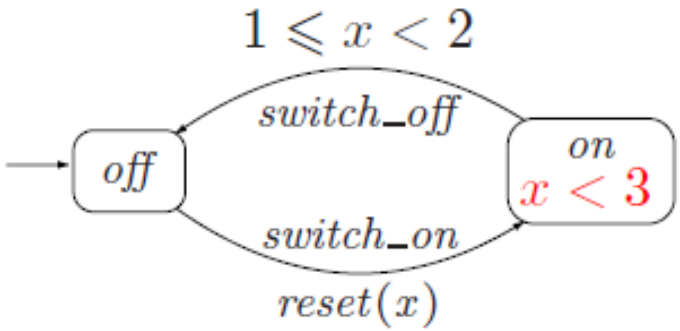
Időzár (timelock)

- Egy állapot időzárnak tekinthető, ha nincs belőle divergens útvonal
  - A kimenő útvonalakon nem „telhet tovább” az idő (a végtelenségig)
  - Terminális állapot
    - A végállapot nem feltétlenül jelent időzárat (pl. az invariáns true)
- Egy automata, ahol van időzár:
  - (on, 2) elérhető, és nincs belőle divergens útvonal



Időzár konvergens útvonallal

- A modell:

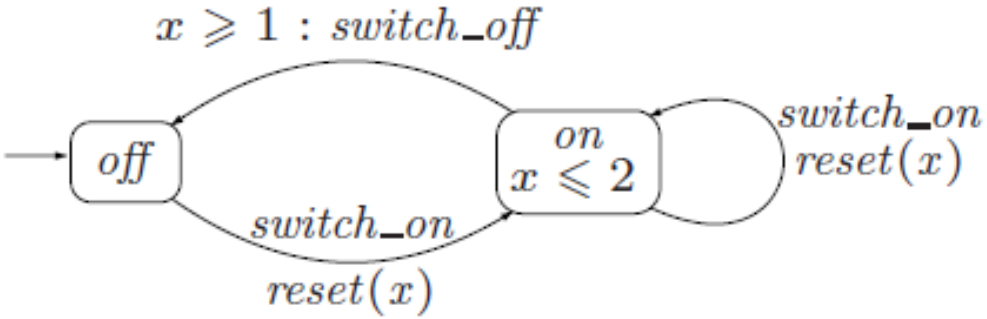


- Konvergens útvonal:

$$\langle on, 2\rangle \ \langle on, 2.9\rangle \ \langle on, 2.99\rangle \ \langle on, 2.999\rangle \ \langle on, 2.9999\rangle \ \ldots$$

Zeno tulajdonság

- Zeno útvonal:
  - Idő-konvergens, ugyanakkor
  - végtelenül sok $a \in Act$ akció végrehajtható
- Példa modell:



- Zeno útvonalak:

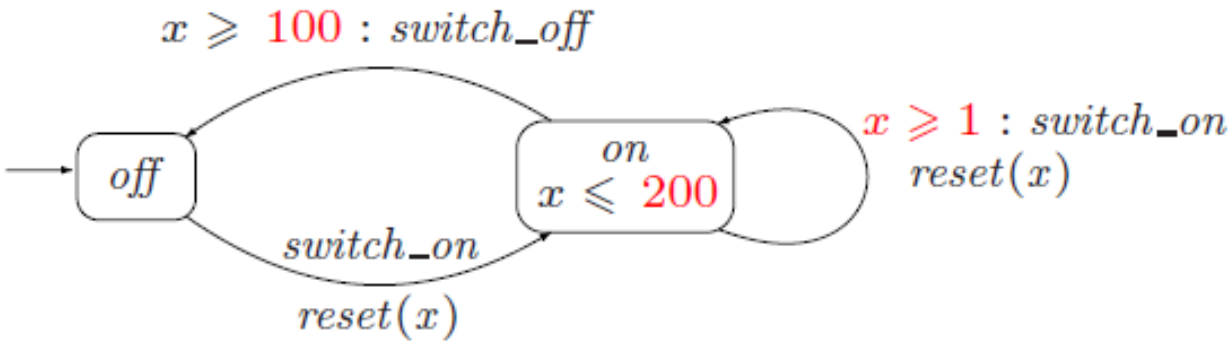
$$\langle off, 0\rangle \xrightarrow{sw\_on} \langle on, 0\rangle \xrightarrow{sw\_on} \langle on, 0\rangle \xrightarrow{sw\_on} \langle on, 0\rangle \xrightarrow{sw\_on} \ldots$$

$$\langle off, 0\rangle \xrightarrow{sw\_on} \langle on, 0\rangle \xrightarrow{0.5} \langle on, 0.5\rangle \xrightarrow{sw\_on} \langle on, 0\rangle \xrightarrow{0.25} \langle on, 0.25\rangle \xrightarrow{sw\_on} \ldots$$

Vannak késleltetések, de 1-et nem éri el ezek összege:
0,5 + 0,25 + 0,125 + …

A zeno tulajdonság elkerülése

- Az előző példa esetén:
  - (Minimális) késleltetés az egymás utáni switch_on akciók között
- A módosított példa modell:
  - Minimális késleltetés 1 egység (egész óra esetén)
  - Arányában megnövelve a vezérlés-specifikus késleltetés



Időzített logika (TL) bevezetése

- Elvárások:
  - Órák használata
  - Rekurzió megengedett
  - Elégséges a TA-n megfogalmazható leggyakoribb követelményekhez
  - Eldönthető a kifejezések igazsága
- Jelölések:
  - K óra-halmaz (formula-órák)
    - A modell óráival azonos rátával haladnak, de külön hivatkozhatók
  - Id azonosítók (formulában értékadáshoz – rekurzió)
    - $Z \in Id$ változó
    - D(Z) hozzárendelés Z változóhoz, $D(Z)=\varphi$, más alakban $Z:=\varphi$ (rekurzióhoz használandó)

TL szintaxis

- $\varphi ::= P \mid c \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \exists \varphi \mid \forall \varphi \mid \langle a \rangle \varphi \mid [a]\varphi \mid x \text{ in } \varphi \mid x+n \sim y+m \mid Z$

  ahol $P \in AP$, $c \in B(K)$, $a \in Act$, $x \in K$, és $Z \in Id$, $m,n \in N$

- Temporális operátorok informálisan:
  - $\exists \varphi$ – létezik olyan késleltetés, hogy φ igaz lesz
  - $\forall \varphi$ – minden késleltetésre φ igaz lesz
  - $x \text{ in } \varphi$ – x resetelésével φ igaz lesz
  - $x+n \sim y+m$ – óra-kifejezések összevetése
- TL értelmezhető (igazsága megállapítható) TA szemantikája, azaz TTS-ek felett
  - s: (l,u) lesznek a TTS állapotok TA-ból
  - (s,v) jelölés TTS-beli állapotra és formula-órára, $v \in R^K$

TL szemantika (1)

- $(s,v) \models P$ a.cs.a. $P \in V(s)$

  azaz P az állapot címkéi között van

- $(s,v) \models c$ a.cs.a. $c(v)$ igaz,

  azaz a v által meghatározott óra-hozzárendelés esetén igaz a c óra-kifejezés

- $(s,v) \models \varphi_1 \wedge \varphi_2$ a.cs.a. $(s,v) \models \varphi_1$ és $(s,v) \models \varphi_2$
- $(s,v) \models \varphi_1 \vee \varphi_2$ a.cs.a. $(s,v) \models \varphi_1$ vagy $(s,v) \models \varphi_2$
- $(s,v) \models \exists\varphi$ a.cs.a. $\exists d,s'$: $s \rightarrow^{\varepsilon(d)} s'$ és $(s',v+d) \models \varphi$

  azaz létezik olyan, (s,v)-ből késleltetéssel elérhető állapot, ahol igaz φ

- $(s,v) \models \forall\varphi$ a.cs.a. $\forall d,s'$: $s \rightarrow^{\varepsilon(d)} s' \Rightarrow (s',v+d) \models \varphi$

  azaz minden, (s,v)-ből késleltetéssel elérhető állapotban igaz φ

TL szemantika (2)

- $(s,v) \models \langle a \rangle \varphi$ a.cs.a. $\exists s'$: $s \rightarrow^a s'$ és $(s',v) \models \varphi$

  azaz létezik olyan, (s,v)-ből a akcióval elérhető állapot, ahol igaz φ

- $(s,v) \models [a]\varphi$ a.cs.a. $\forall s'$: $s \rightarrow^a s' \Rightarrow (s',v) \models \varphi$

  azaz minden, (s,v)-ből a akcióval elérhető állapotban igaz φ

- $(s,v) \models x$ in φ a.cs.a. $(s,v') \models \varphi$ ahol $v'=[\{x\}\rightarrow 0]v$

  azaz x reseteléssével igaz lesz φ

- $(s,v) \models x+n \sim y+m$ a.cs.a. $v(x)+n \sim v(y)+m$

  azaz az óra-változók állása megfelelő

- $(s,v) \models Z$ a.cs.a. $(s,v) \models D(Z)$

  azaz a Z-hez rendelt formula igaz

TL jellemzők

- Eredeti logika:
  $\varphi ::= c \mid P \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \exists \varphi \mid \forall \varphi \mid \langle a \rangle \varphi \mid [a]\, \varphi \mid$
  $x \text{ in } \varphi \mid x+n \sim y+m \mid Z$
- Alacsony szintű, nagyon egyszerű operátorok
  - Egzisztenciális és univerzális operátorok késleltetéssel illetve akcióval címkézett átmenetekre
  - „Alap logika” (hasonló szerepű, mint a μ-kalkulus)
  - Kifejezőképessége nagy (rekurzió is megengedett), de önmagában nehezen használható
- Továbblépés:
  - Összetett operátorok képzése az egyszerűbbekből
    - Közelebb állnak a gyakori követelményekhez: pl. invaráns, UNTIL, $\text{UNTIL}_{<t}$, BEFORE t
  - Korlátozások bevezetése az egyes modellellenőrzőkben a hatékonyabb ellenőrzési algoritmusok érdekében
    - pl. UPPAAL, KRONOS

Hasznos kifejezések

- INV(φ) invariáns, az a Z kifejezés

  ahol **Z := $\varphi \wedge \forall$Z $\wedge$ [Act]Z**

  ahol [Act]Z jelentése $[a_1]Z \wedge [a_2]Z \wedge \ldots \wedge [a_n]Z$ minden $a_i \in$Act-ra

A rekurzió miatt kell Z bevezetése

Hasznos kifejezések

- INV(φ) invariáns, az a Z kifejezés
  - ahol **Z := φ ∧ ∀Z ∧ [Act]Z**
    - ahol [Act]Z jelentése $[a_1]Z \wedge [a_2]Z \wedge \ldots \wedge [a_n]Z$ minden $a_i \in$ Act-ra

A rekurzió miatt kell Z bevezetése

Minden, késleltetéssel elérhető állapotban Z újra igaz lesz

Minden, akcióval elérhető állapotban Z újra igaz lesz

Általános „next” kifejezése

Hasznos kifejezések

- INV(φ) invariáns, az a Z kifejezés

  ahol **Z := $\varphi \wedge \forall$Z $\wedge$ [Act]Z**

  ahol [Act]Z jelentése $[a_1]Z \wedge [a_2]Z \wedge \ldots \wedge [a_n]Z$ minden $a_i \in$Act-ra

- φ_1 UNTIL $\varphi_2 \equiv$ Z „weak until”,

  ahol **Z := $\varphi_2 \vee (\varphi_1 \wedge \forall$Z $\wedge$ [Act]Z)**

Weak until: φ_2 nem feltétlenül kell teljesüljön

- φ_1 UNTIL$_{<n}$ $\varphi_2 \equiv$ x in (($\varphi_1 \wedge$ x<n) UNTIL φ_2)

  itt x resetelés után értékelendő ki, vagyis n relatív idő

- φ BEFORE n $\equiv$ true UNTIL$_{<n}$ φ
- at(l_i) BEFORE t az l_i hely elérése t előtt

  Itt jelölés: at(l_i) – az l_i helyen van az automata

Hatékonyabb kiértékelés

- Eredeti logika:

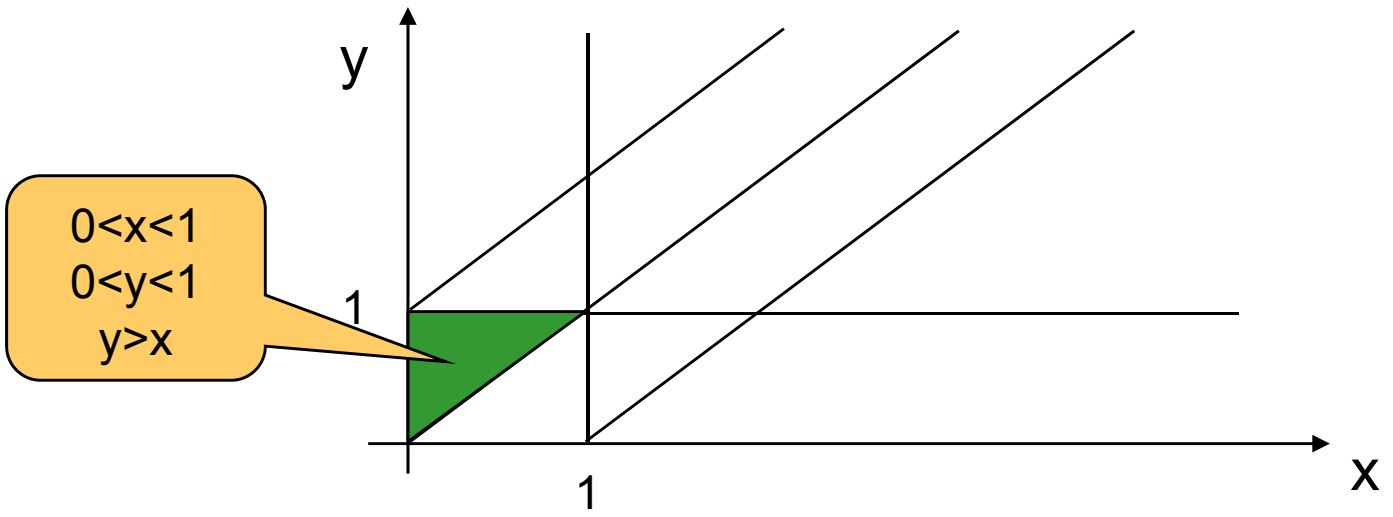
  $\varphi ::= c \mid P \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \exists \varphi \mid \forall \varphi \mid \langle a \rangle \varphi \mid [a]\, \varphi \mid$
  $x \text{ in } \varphi \mid x+n \sim y+m \mid Z$

- Biztonsági és kötött élőségi kritériumok ellenőrzése
  - $\exists \varphi$ kihagyva (késleltetéseken egzisztenciális kvantor)
  - $\langle a \rangle$ kihagyva (akciókon egzisztenciális kvantor)
  - $c \vee \varphi$ alakú formulák
  - $P \vee \varphi$ alakú formulák

  Invariáns, UNTIL, $\text{UNTIL}_{<n}$, BEFORE t kifejezhető

Modell ellenőrzés alapgondolata

- Régiók megállapítása,
  ahol azonosan értékelhetők ki a feltételek
  - A régiókon értelmezett a TL igazsága
    - Sokféle késleltetés tud igazzá tenni egy követelményt;
      ezeket az invariánsok és őrfeltételek határolják be;
    - Így alakulnak ki a régiók az óra-változókon
- Szemantika alapú modell ellenőrzés:
  - Kényszer-kielégítési problémára visszavezetve
  - Modellellenőrzés: Van-e olyan óra-hozzárendelés, hogy φ igaz?



UPPAAL modell ellenőrző

- Temporális logika:
  - Φ ::= A[] β | E<> β

    ahol β ::= a | β and β | β or β | β implies β | not β
    - itt a lehet A_i.l vagy x_i~n alakú,
    - A_i.l jelöli, hogy az A_i automata az l helyen van
  - Speciális operátor: --> („leadsto”)
    - a --> b egy rövidítés: A[] (a implies A<>b)
  - Speciális atomi kijelentés: deadlock
    - Arra az állapotra igaz, ahonnan nincs továbblépés
    - A[] not deadlock jellegzetes kritérium

KRONOS modell ellenőrző

- TA formalizmus használatos itt is
- TCTL temporális logika
  - $\exists\langle\rangle$ (EF-nek megfelelő)
  - $\forall[]$ (AG-nek megfelelő)
  - $\exists\langle\rangle_{=1}$ (egy időegység alatt elérhető)
  - $\forall[]_{\leq 5}$ (legfeljebb 5 időegység alatt elérhető)
- Érdekes követelmény:
  - $\forall[]\ \exists\langle\rangle_{=1}$ true
    - azaz minden állapotban igaz, hogy *telhet az idő* 1 egységet
    - a kritériumok nem azért teljesülnek, mert „megáll az idő”

Miről volt szó?

- Motiváció: Valósidejű rendszerek ellenőrzése
- Modellek
  - Timed Transition System (TTS)
  - Timed Automata (TA)
  - Leképzés: TA -> TTS
- Érdekességek valósidejű rendszerek modellezése során
  - Idő konvergencia, időzár, zeno tulajdonság
- Követelmények formalizálása
  - TL (Timed Temporal Logic)
- Modellellenőrzés
  - Korlátozások
  - Alapötlet