Blockchain: Logički pogled

Zoran Ognjanović

zorano@mi.sanu.ac.rs

Matematički fakultet Beograd, 9. 4. 2024.

BlockChain

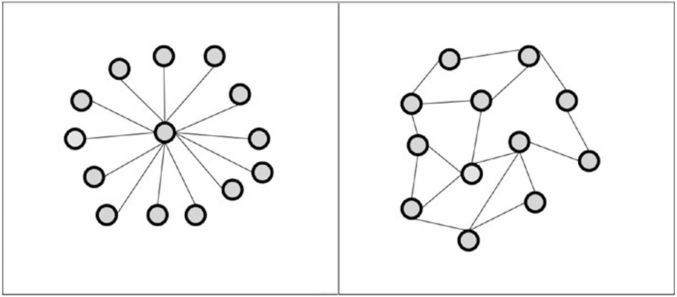
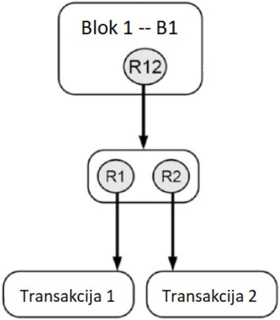
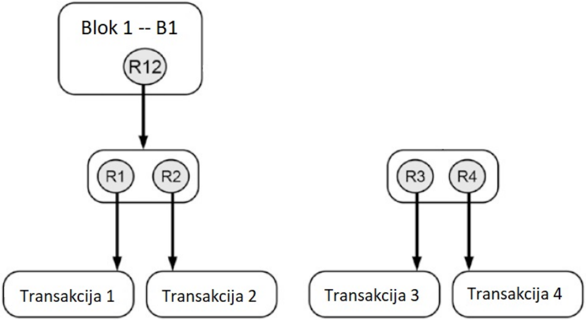


Figure: (De)centralizovana organizacija sistema

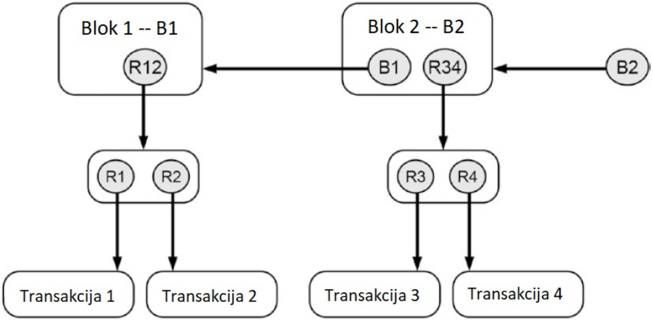
Ledger – lanac, računovodstvena knjiga



Ledger – lanac, računovodstvena knjiga



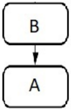
Ledger – lanac, računovodstvena knjiga



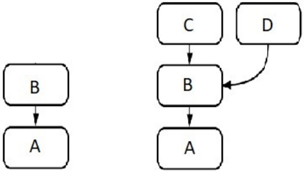
Težak kriptografski zadatak:

- Naći hash-vrednost koja počinje izvesnim brojem 0

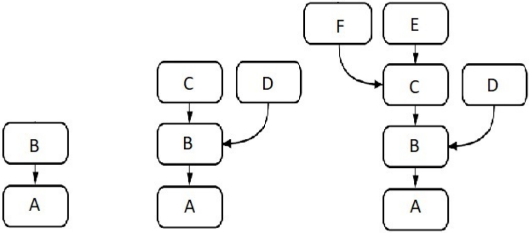
Fork: podela lanca



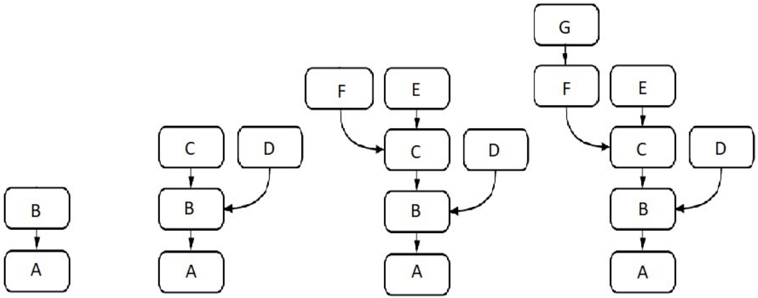
Fork: podela lanca



Fork: podela lanca



Fork: podela lanca



Kriterijum najduže grane:

- svaki čvor bira lanac blokova na kome radi, a čuva ostale
- kada jedan lanac postane najduži svi čvorovi prelaze na njega (ABCFG).

Motivacioni primeri

Čudno ostrvo: analiza istinitosti

- Putnik na ostrvu na kome stanovnici ili stalno lažu, ili stalno govore istinu, sreće osobe A_1 i A_2.
- A_1 kaže: "Obojica smo lažovi."
- Šta putnik zaključuje o njima?

Čudno ostrvo: analiza istinitosti

- Putnik na ostrvu na kome stanovnici ili stalno lažu, ili stalno govore istinu, sreće osobe A_1 i A_2.
- A_1 kaže: "Obojica smo lažovi."
- Šta putnik zaključuje o njima?

- Nije moguće da stanovnik ostrva kaže da je lažov:
  - ako stalno govori istinu, neće reći da je lažov (jer bi to bila laž),
  - ako je lažov, neće reći da je lažov (jer bi to bila istina).

Čudno ostrvo: analiza istinitosti

- Putnik na ostrvu na kome stanovnici ili stalno lažu, ili stalno govore istinu, sreće osobe A_1 i A_2.
- A_1 kaže: "Obojica smo lažovi."
- Šta putnik zaključuje o njima?

- Nije moguće da stanovnik ostrva kaže da je lažov:
  - ako stalno govori istinu, neće reći da je lažov (jer bi to bila laž),
  - ako je lažov, neće reći da je lažov (jer bi to bila istina).

- A_1 **je lažov**, jer da nije, ne bi lažno tvrdio da jeste.
- Kako je A_1 lažov, njegova izjava je lažna, pa nisu obojica lažovi.
- A_2 **govori istinu**.

Čudno ostrvo (2): formalna analiza

- Iskaz k_i: "Osoba A_i govori istinu"
- Neka A_i izjavi p_i. Ne znamo da li je p_i tačno, ali:
  - ako A_i govori istinu (tačno je k_i), onda p_i je tačno,
  - ako je p_i tačno, onda A_i govori istinu (tačno je k_i),
  - uvek važi:

$$k_i \leftrightarrow p_i$$

Čudno ostrvo (2): formalna analiza

- Iskaz k_i: "Osoba A_i govori istinu"
- Neka A_i izjavi p_i. Ne znamo da li je p_i tačno, ali:
  - ako A_i govori istinu (tačno je k_i), onda p_i je tačno,
  - ako je p_i tačno, onda A_i govori istinu (tačno je k_i),
  - uvek važi:

$$k_i \leftrightarrow p_i$$

- A_1 kaže p_1: "Obojica smo lažovi" $(\neg k_1 \wedge \neg k_2)$

$$k_1 \leftrightarrow (\neg k_1 \wedge \neg k_2)$$

Čudno ostrvo (3): istinitosna tablica

$I(k_1)$	$I(k_2)$	$I(\neg k_1)$	$I(\neg k_2)$	$I(\neg k_1 \wedge \neg k_2)$	$k_1 \leftrightarrow (\neg k_1 \wedge \neg k_2)$
$\top$	$\top$	$\bot$	$\bot$	$\bot$	$\bot$
$\top$	$\bot$	$\bot$	$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\top$	$\bot$	$\bot$	$\top$
$\bot$	$\bot$	$\top$	$\top$	$\top$	$\bot$

Čudno ostrvo (3): istinitosna tablica

$I(k_1)$	$I(k_2)$	$I(\neg k_1)$	$I(\neg k_2)$	$I(\neg k_1 \wedge \neg k_2)$	$k_1 \leftrightarrow (\neg k_1 \wedge \neg k_2)$
$\top$	$\top$	$\bot$	$\bot$	$\bot$	$\bot$
$\top$	$\bot$	$\bot$	$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\top$	$\bot$	$\bot$	$\top$
$\bot$	$\bot$	$\top$	$\top$	$\top$	$\bot$

- Formula je tačna samo kada je k_1 netačno i k_2 tačno (A_1 je lažov, A_2 govori istinu).
- Tautologija je

$$(k_1 \leftrightarrow (\neg k_1 \wedge \neg k_2)) \rightarrow (\neg k_1 \wedge k_2)$$

Čudno ostrvo (4): drugi primer

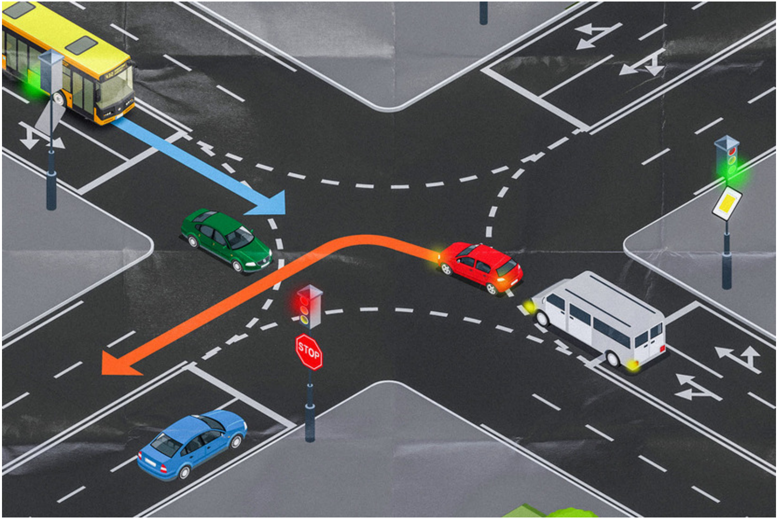
- A_1 kaže p_1: "Barem jedan od nas je lažov." $(\neg k_1 \vee \neg k_2)$

Čudno ostrvo (4): drugi primer

- A_1 kaže p_1: "Barem jedan od nas je lažov." $(\neg k_1 \vee \neg k_2)$

$I(k_1)$	$I(k_2)$	$I(\neg k_1)$	$I(\neg k_2)$	$I(\neg k_1 \vee \neg k_2)$	$k_1 \leftrightarrow (\neg k_1 \vee \neg k_2)$
$\top$	$\top$	$\perp$	$\perp$	$\perp$	$\perp$
$\top$	$\perp$	$\perp$	$\top$	$\perp$	$\top$
$\perp$	$\top$	$\top$	$\perp$	$\top$	$\perp$
$\perp$	$\perp$	$\top$	$\top$	$\top$	$\perp$

- Formula je tačna samo kada je k_1 tačno i k_2 netačno (A_1 govori istinu, A_2 je lažov).
- Tautologija je $(k_1 \leftrightarrow (\neg k_1 \vee \neg k_2)) \rightarrow (k_1 \wedge \neg k_2)$.


STOP

Matematička logika. Relacije posledice

Matematička logika. Relacije posledice

Formalni logički jezik, formule

Matematička logika. Relacije posledice

Formalni logički jezik, formule

- semantika
  (modeli, tačnost)

- semantičke posledice $T \models \alpha$

Matematička logika. Relacije posledice

Formalni logički jezik, formule

- semantika
  (modeli, tačnost)
- aksiomatski sistem
  (aksiome, pravila, dokazi)

- semantičke posledice $T \models \alpha$
- sintaksne posledice $T \vdash \alpha$

Matematička logika. Relacije posledice

Formalni logički jezik, formule

- semantika (modeli, tačnost)
- aksiomatski sistem (aksiome, pravila, dokazi)

- semantičke posledice $T \models \alpha$
- sintaksne posledice $T \vdash \alpha$

Potpunost: $T \models \alpha$ akko $T \vdash \alpha$

Neklasične logike

Neklasične logike

- Proširenja klasične logike:
  - Modalne logike
    - modalne logike (u užem smislu)
    - logike znanja,
    - temporalne logike,
    - verovatnosne logike, ...
- Zamena za klasičnu logiku:
  - Intuicionistička logika,
  - fuzzy logike,
  - default logike, ...

Modalne logike

- Mesec su osvojili vanzemaljci ili Novak Djoković je sportista.
- Danas je utorak ili danas nije utorak.

- Mesec su osvojili vanzemaljci ili Novak Djoković je sportista.
- Danas je utorak ili danas nije utorak.
- $\alpha \vee \beta$
- $\alpha \vee \neg\alpha$

Jezik

- Jezik klasične iskazne logike: $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, Var
- Unarni operator (veznik) nužno: $\Box$
- Unarni operator (veznik) moguće: $\Diamond\alpha =_{def} \neg\Box\neg\alpha$
- Primer formule: $\neg\Diamond\alpha \rightarrow \Box\Diamond\neg\alpha$

Shvatanja modalnih operatora

- $\Box\alpha$ – 'α je logički nužno',
  $\Diamond\alpha$ – 'α je logički moguće i ne protivreči logičkim zakonima',
- $\Box\alpha$ – 'agent zna α',
  $\Diamond\alpha$ – 'α nije u kontradikciji sa onim što se zna',
- $\Box\alpha$ – 'agent veruje u α',
- $\Box\alpha$ – 'α je dokazivo u nekom formalnom sistemu',
  $\Diamond\alpha$ – 'α nije u kontradikciji sa formalnim sistemom',
- $\Box\alpha$ – 'α je zakonska obaveza'
  $\Diamond\alpha$ – 'α je dozvoljeno',
- $\Box\alpha$ – 'α je tačno zauvek u budućnosti,
  $\Diamond\alpha$ – 'α će se ostvariti u budućnosti'

Zahtevi za modalne operatore

- modalni operatori nisu istinitosno funkcionalni, pa ni jedna od sledećih formula ne sme biti valjana:

$$\Box\alpha \leftrightarrow \neg\alpha,$$
$$\Box\alpha \leftrightarrow \alpha,$$
$$\Box\alpha \leftrightarrow (\alpha \vee \neg\alpha),$$
$$\Box\alpha \leftrightarrow (\alpha \wedge \neg\alpha)$$

- primerci klasično valjanih formula su nužno istiniti

- ako iskaz β nužno sledi iz iskaza α, tj. važi $\Box(\alpha \to \beta)$ i izkaz α je nužan, onda je nužan i iskaz β, odnosno valjana je formula

$$(\Box(\alpha \to \beta) \wedge \Box\alpha) \to \Box\beta$$

Kripkeovi modeli

Iskazni Kripkeovi modeli za modalne logike

Definition

Neka je Var skup iskaznih slova. Uredjena trojka

$$\mathcal{M} = \langle W, R, v \rangle$$

je *iskazni Kripkeov model* ako je:

- W je neprazan skup čije se elementi nazivaju *(modalni) svetovi* ili *stanja*,
- $R \subset W \times W$ je binarna relacija nad W koja se naziva *relacija dostižnosti (vidljivosti)*
- valuacija $v : W \times \text{Var} \to \{\top, \bot\}$ svakom svetu i svakom iskaznom slovu pridružuje $\top$ ili $\bot$.

Zadovoljivost

Definition

Neka je $\mathcal{M} = \langle W, R, v \rangle$ iskazni Kripkeov model. Relacija (*modalne*) *zadovoljivosti* ($\models$) je binarna relacija izmedju svetova modela i formula takva da za svaki svet $w \in W$ važi:

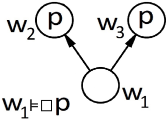
- ako je $p \in \Phi$, $w \models p$ ako i samo ako $v(w)(p) = \top$,
- $w \models \neg\alpha$ ako i samo ako nije $w \models \alpha$,
- $w \models (\alpha \wedge \beta)$ ako i samo ako $w \models \alpha$ i $w \models \beta$ i
- $w \models \Box\alpha$ ako i samo ako za svaki svet u dostižan iz w važi $u \models \alpha$.

Zadovoljivost

Definition

Neka je $\mathcal{M} = \langle W, R, v \rangle$ iskazni Kripkeov model. Relacija (*modalne*) *zadovoljivosti* ($\models$) je binarna relacija izmedju svetova modela i formula takva da za svaki svet $w \in W$ važi:

- ako je $p \in \Phi$, $w \models p$ ako i samo ako $v(w)(p) = \top$,
- $w \models \neg\alpha$ ako i samo ako nije $w \models \alpha$,
- $w \models (\alpha \wedge \beta)$ ako i samo ako $w \models \alpha$ i $w \models \beta$ i
- $w \models \Box\alpha$ ako i samo ako za svaki svet u dostižan iz w važi $u \models \alpha$.



Neka je

- $\mathcal{M} = \langle \{w_1, w_2\}, \{(w_1, w_1), (w_1, w_2), (w_2, w_1)\}, v\rangle$
- $v(w_1)(p) = \top$, $v(w_1)(q) = \top$, $v(w_2)(p) = \top$, $v(w_2)(q) = \bot$.

Sada je

- $w_1 \models p$, $w_1 \models q$, $w_1 \models p \wedge q$
- $w_2 \models p$, $w_2 \models \neg q$, $w_2 \not\models p \wedge q$
- $w_1 \models \Box p$, jer p važi u svim svetovima dostižnim iz w_1
- $w_2 \models \Box q$
- $w_1 \not\models \Box q$
- $w_1 \not\models \Box(p \wedge q)$
- $w_2 \models \Box(p \wedge q)$
- $w_2 \models \Box q$ iako nije $w_2 \models q$.

Neka je model $\mathcal{M}$ odredjen sa

- skupom svetova $W = \{w, u, t\}$,
- relacijom $R = \{(w, w), (w, u), (u, w), (u, u), (t, t)\}$ i
- valuacijom $v(w)(p) = v(t)(p) = \top$, $v(u)\ (p) = \bot$.

Neka je model $\mathcal{M}$ odredjen sa

- skupom svetova $W = \{w, u, t\}$,
- relacijom $R = \{(w, w), (w, u), (u, w), (u, u), (t, t)\}$ i
- valuacijom $v(w)(p) = v(t)(p) = \top$, $v(u)\ (p) = \bot$.

- $w \quad \Box p$ i
- $t \quad \Box p$.

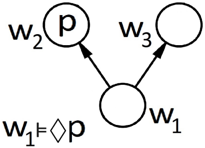
Neka je model $\mathcal{M}$ odredjen sa

- skupom svetova $W = \{w, u, t\}$,
- relacijom $R = \{(w, w), (w, u), (u, w), (u, u), (t, t)\}$ i
- valuacijom $v(w)(p) = v(t)(p) = \top$, $v(u)\ (p) = \bot$.

- $w \not\models \Box p$ i
- $t \models \Box p$.

- $\Diamond\alpha =_{def} \neg\Box\neg\alpha$
- $w \models \Diamond\alpha$ ako i samo ako u modelu

- $\Diamond\alpha =_{def} \neg\Box\neg\alpha$
- $w \models \Diamond\alpha$ ako i samo ako u modelu postoji svet u dostižan iz sveta w tako da je $u \models \alpha$



Razmotrimo formulu $\Box p \to \Box\Box p$ i model $\mathcal{M} = \langle W, R, v\rangle$, u kom je

- $W = \{w_1, w_2, w_3\}$,
- $R = \{(w_1, w_2), (w_2, w_3), (w_3, w_3)\}$ i
- $w_1 \models p$, $w_2 \models p$ i $w_3 \not\models p$.

Razmotrimo formulu $\Box p \to \Box\Box p$ i model $\mathcal{M} = \langle W, R, v\rangle$, u kom je

- $W = \{w_1, w_2, w_3\}$,
- $R = \{(w_1, w_2), (w_2, w_3), (w_3, w_3)\}$ i
- $w_1 \models p$, $w_2 \models p$ i $w_3 \not\models p$.

Zaključujemo da:

- $w_1 \models \Box p$, jer p važi u svim svetovima dostižnim iz w_1,
- $w_2 \not\models \Box p$, jer p ne važi u svetu w_3
- $w_1 \not\models \Box\Box p$, jer $\Box P$ ne važi u svetu w_2
- $w_1 \not\models \Box p \to \Box\Box p$

Razmotrimo formulu $\Box p \to p$, i model $\mathcal{M} = \langle W, R, v \rangle$, u kom je

- $W = \{w_1, w_2\}$,
- $R = \{(w_1, w_2), (w_2, w_2), \}$ i
- $w_1 \models \neg p$, $w_2 \models p$

Razmotrimo formulu $\Box p \to p$, i model $\mathcal{M} = \langle W, R, v \rangle$, u kom je

- $W = \{w_1, w_2\}$,
- $R = \{(w_1, w_2), (w_2, w_2), \}$ i
- $w_1 \models \neg p$, $w_2 \models p$

Zaključujemo da:

- $w_1 \models \Box p$, jer p važi u svim svetovima dostižnim iz w_1,
- $w_1 \not\models p$,
- $w_1 \not\models \Box p \to p$

Klase modela

Naziv klase modela	Uslovi za relaciju dostižnosti
K	bez uslova
T	refleksivnost
$K4$	tranzitivnost
KB	simetričnost
$S4$	refleksivnost i tranzitivnost
B	refleksivnost i simetričnost
$S5$	refleksivnost, simetričnost i tranzitivnost
D	idealizacija

Modalne aksiome i pravila izvodjenja

Osnovni sistem K – svi primerci klasičnih iskaznih teorema, plus:

(K) $\Box(\alpha \to \beta) \to (\Box\alpha \to \Box\beta)$

(MP) iz α i $\alpha \to \beta$ izvesti β i

(N) iz α izvesti $\Box\alpha$

Modalne aksiome i pravila izvodjenja

Osnovni sistem K – svi primerci klasičnih iskaznih teorema, plus:

(**K**) $\Box(\alpha \to \beta) \to (\Box\alpha \to \Box\beta)$

(**MP**) iz α i $\alpha \to \beta$ izvesti β i

(**N**) iz α izvesti $\Box\alpha$

Naziv klase modela	Uslovi za relaciju dostižnosti	Karakteristične aksiome
K	bez uslova	
T	refleksivnost	(**T**) $\Box\alpha \to \alpha$
$K4$	tranzitivnost	(**4**) $\Box\alpha \to \Box\Box\alpha$
KB	simetričnost	(**B**) $\alpha \to \Box\Diamond\alpha$
$S4$	refleksivnost i tranzitivnost	
B	refleksivnost i simetričnost	
$S5$	refleksivnost, simetričnost i tranzitivnost	(**5**) $\Diamond\alpha \to \Box\Diamond\alpha$
D	idealizacija	(**D**) $\Box\alpha \to \Diamond\alpha$

Modalne logike sa više verzija modalnog operatora $\Box$

- $\Box_1, \Box_2, \ldots, \Box_m$
- $M = \langle W, R_1, R_2, \ldots, R_m, v \rangle$
- $w \models \Box_i \alpha$ ako i samo ako za svaki svet u za koji je wR_iu važi $u \models \alpha$

Epistemička logika

Operator znanja, $\mathtt{K}$ $(= \Box)$

- Jezik klasične iskazne logike: $\mathrm{Var} = \{p, q, p_1, p_2, \ldots\}$, $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$
- Skup agenata $\mathbb{A} = \{a_1, \ldots, a_m\}$
- Epistemički operatori:
  - $\mathtt{K}_a$ $(a \in \mathbb{A})$, agent a zna
  - $\mathtt{C}$, common knowledge (opšte znanje)

Operator znanja, $\mathtt{K}$ ($= \Box$)

- Jezik klasične iskazne logike: $\mathrm{Var} = \{p, q, p_1, p_2, \ldots\}$, $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$
- Skup agenata $\mathbb{A} = \{a_1, \ldots, a_m\}$
- Epistemički operatori:
  - $\mathtt{K}_a$ ($a \in \mathbb{A}$), agent a zna
  - $\mathtt{C}$, common knowledge (opšte znanje)
  - $\mathtt{E}\alpha =_{def} \bigwedge_{a \in \mathbb{A}} \mathtt{K}_a\alpha$, grupa zna

Operator znanja, $\mathtt{K}$ $(= \Box)$

- Jezik klasične iskazne logike: $\mathsf{Var} = \{p, q, p_1, p_2, \ldots\}$, $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$
- Skup agenata $\mathbb{A} = \{a_1, \ldots, a_m\}$
- Epistemički operatori:
  - $\mathtt{K}_a$ $(a \in \mathbb{A})$, agent a zna
  - $\mathtt{C}$, common knowledge (opšte znanje)
  - $\mathtt{E}\alpha =_{def} \bigwedge_{a \in \mathbb{A}} \mathtt{K}_a\alpha$, grupa zna
- $\mathtt{C}\alpha \rightarrow (\mathtt{K}_a\alpha \wedge \mathtt{K}_a\mathtt{K}_b\alpha)$

Kripke modeli za epistemičku logiku

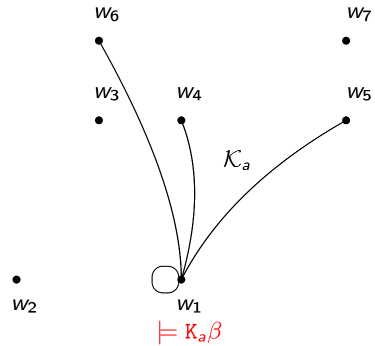
$\mathcal{M} = \langle \mathrm{W}, \mathcal{K}, v \rangle$:

- W je skup svetova (stanja),
- $\mathcal{K} = \{\mathcal{K}_a : a \in \mathbb{A}\}$ je skup relacija ekvivalencije na W,
- $v : W \times \mathrm{Var} \to \{\perp, \top\}$

Zadovoljivost u epistemičkoj logici

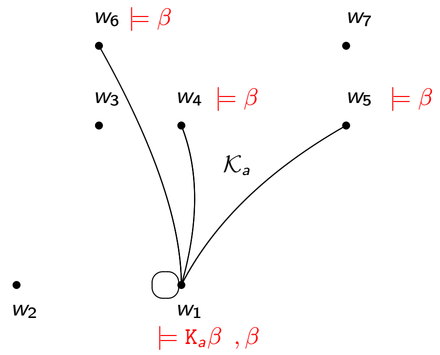
$$w_1 \models \mathtt{K}_a\beta \text{ akko } (\forall u)(w\mathcal{K}_a u \Rightarrow u \models \beta)$$

Zadovoljivost u epistemičkoj logici



$w_1 \models \mathtt{K}_a\beta$ akko $(\forall u)(w\mathcal{K}_a u \Rightarrow u \models \beta)$

Zadovoljivost u epistemičkoj logici

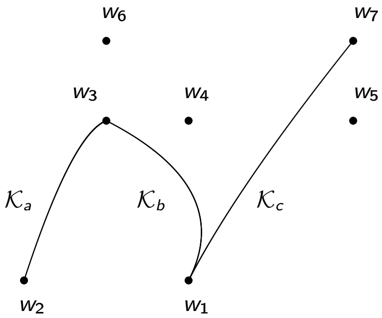


$w_1 \models \mathtt{K}_a\beta$ akko $(\forall u)(w\mathcal{K}_a u \Rightarrow u \models \beta)$

Zadovoljivost u epistemičkoj logici (2)

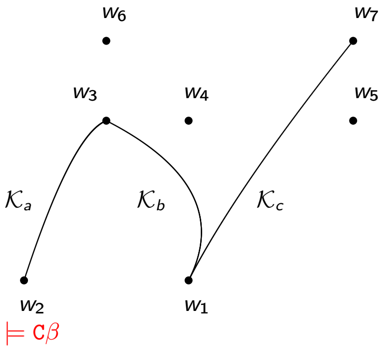
$w_2 \models \mathtt{C}\beta$ akko $(\forall u$ dostižan iz $w_2)(u \models \beta)$

Zadovoljivost u epistemičkoj logici (2)



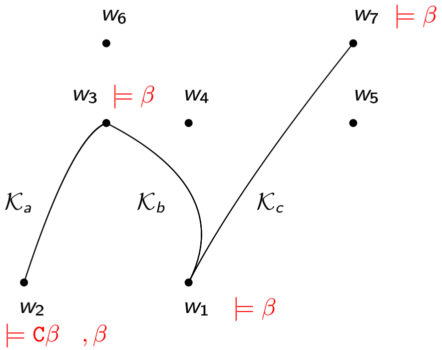
$w_2 \models \mathtt{C}\beta$ akko $(\forall u$ dostižan iz $w_2)(u \models \beta)$

Zadovoljivost u epistemičkoj logici (2)



$w_2 \models \mathtt{C}\beta$ akko $(\forall u$ dostižan iz $w_2)(u \models \beta)$

Zadovoljivost u epistemičkoj logici (2)



$w_2 \models \mathtt{C}\beta$ akko $(\forall u$ dostižan iz $w_2)(u \models \beta)$

Example

Osobe 1 i 2 sede jedna naspram drugoj i imaju kape na glavama. Osoba 1 vidi kapu osobe 2 i obrnuto, ali ni jedna osoba ne vidi svoju kapu. Ispitivač na početku **javno obaveštava** da se na nečijoj kapi nalazi nalepnica. Postavlja pitanje osobama da li je nalepnica baš na njihovoj kapi. Šta je odgovor?

Example

Osobe 1 i 2 sede jedna naspram drugoj i imaju kape na glavama. Osoba 1 vidi kapu osobe 2 i obrnuto, ali ni jedna osoba ne vidi svoju kapu. Ispitivač na početku **javno obaveštava** da se na nečijoj kapi nalazi nalepnica. Postavlja pitanje osobama da li je nalepnica baš na njihovoj kapi. Šta je odgovor?

- stanje modela (p_1, p_2),
  $p_i = 1$ na kapi osobe i je nalepnica

Example

Osobe 1 i 2 sede jedna naspram drugoj i imaju kape na glavama. Osoba 1 vidi kapu osobe 2 i obrnuto, ali ni jedna osoba ne vidi svoju kapu. Ispitivač na početku **javno obaveštava** da se na nečijoj kapi nalazi nalepnica. Postavlja pitanje osobama da li je nalepnica baš na njihovoj kapi. Šta je odgovor?

- stanje modela (p_1, p_2),
  $p_i = 1$ na kapi osobe i je nalepnica
- sva stanja modela: $(0, 0)$, $(0, 1)$, $(1, 0)$ i $(1, 1)$

Example

Osobe 1 i 2 sede jedna naspram drugoj i imaju kape na glavama. Osoba 1 vidi kapu osobe 2 i obrnuto, ali ni jedna osoba ne vidi svoju kapu. Ispitivač na početku **javno obaveštava** da se na nečijoj kapi nalazi nalepnica. Postavlja pitanje osobama da li je nalepnica baš na njihovoj kapi. Šta je odgovor?

- stanje modela (p_1, p_2),
  $p_i = 1$ na kapi osobe i je nalepnica
- sva stanja modela: $(0,0)$, $(0,1)$, $(1,0)$ i $(1,1)$
- $\mathcal{K}_1$ najmanja relacija ekvivalencije koja sadrži $\{((0,1),(1,1)),((0,0),(1,0))\}$,
- $\mathcal{K}_2$ najmanja relacija ekvivalencije koja sadrži $\{((0,0),(0,1)),((1,0),(1,1))\}$.

- $(0,1) \models \neg K_2 p_2$, jer
  $(0,0) \models \neg p_2$, $((0,1),(0,0)) \in \mathcal{K}_2$,
- $(1,0) \models \neg K_1 p_1$, jer
  $(0,0) \models \neg p_1$, $((1,0),(0,0)) \in \mathcal{K}_1$ i
- $(0,0) \models \neg(p_1 \vee p_2)$.

- $(0,1) \models \neg K_2 p_2$, jer
  $(0,0) \models \neg p_2$, $((0,1),(0,0)) \in \mathcal{K}_2$,
- $(1,0) \models \neg K_1 p_1$, jer
  $(0,0) \models \neg p_1$, $((1,0),(0,0)) \in \mathcal{K}_1$ i
- $(0,0) \models \neg(p_1 \vee p_2)$.
- ispitivačeva izjava: $C_{\{1,2\}}(p_1 \vee p_2)$

- $(0,1) \models \neg K_2 p_2$, jer
  $(0,0) \models \neg p_2$, $((0,1),(0,0)) \in \mathcal{K}_2$,
- $(1,0) \models \neg K_1 p_1$, jer
  $(0,0) \models \neg p_1$, $((1,0),(0,0)) \in \mathcal{K}_1$ i
- $(0,0) \models \neg(p_1 \vee p_2)$.
- ispitivačeva izjava: $C_{\{1,2\}}(p_1 \vee p_2)$
- odstraniti stanje $(0,0)$
  jer u njemu važi $\neg(p_1 \vee p_2)$.

- $(0,1) \models \neg K_2 p_2$, jer
  $(0,0) \models \neg p_2$, $((0,1),(0,0)) \in \mathcal{K}_2$,
- $(1,0) \models \neg K_1 p_1$, jer
  $(0,0) \models \neg p_1$, $((1,0),(0,0)) \in \mathcal{K}_1$ i
- $(0,0) \models \neg(p_1 \vee p_2)$.
- ispitivačeva izjava: $C_{\{1,2\}}(p_1 \vee p_2)$
- odstraniti stanje $(0,0)$
  jer u njemu važi $\neg(p_1 \vee p_2)$.
- $(0,1) \models K_2 p_2$, jer $(0,1) \models p_2$, a u novoj relaciji $\mathcal{K}_2$ svet $(0,1)$ je u relaciji samo sa samim sobom, i slično
- $(1,0) \models K_1 p_1$, jer je $(1,0) \models p_1$.

- Odgovor 'ne znam'
  (na pitanje ispitivača da li se nalepnica nalazi na njihovoj kapi)
  ponovo menja opšte znanje grupe i izgled modela

- Odgovor 'ne znam'
  (na pitanje ispitivača da li se nalepnica nalazi na njihovoj kapi)
  ponovo menja opšte znanje grupe i izgled modela

- eliminiše stanje $(1, 0)$, jer $(1, 0) \models K_1 p_1$
- eliminiše stanje $(0, 1)$, jer $(0, 1) \models K_2 p_1$

- Odgovor 'ne znam'
  (na pitanje ispitivača da li se nalepnica nalazi na njihovoj kapi)
  ponovo menja opšte znanje grupe i izgled modela

- eliminiše stanje $(1,0)$, jer $(1,0) \models K_1 p_1$
- eliminiše stanje $(0,1)$, jer $(0,1) \models K_2 p_1$

- $(1,1) \models K_1 p_1 \wedge K_2 p_2$.

- Odgovor 'ne znam'
  (na pitanje ispitivača da li se nalepnica nalazi na njihovoj kapi)
  ponovo menja opšte znanje grupe i izgled modela

- eliminiše stanje $(1, 0)$, jer $(1, 0) \models K_1 p_1$
- eliminiše stanje $(0, 1)$, jer $(0, 1) \models K_2 p_1$

- $(1, 1) \models K_1 p_1 \wedge K_2 p_2$.

- Na ponovno pitanje obe osobe odgovaraju: "**DA!**"

Operator verovanja, B

Logika verovanja:

- Veruje se i u ono što nije obavezno tačno.
- Model je $\mathcal{M} = \langle \mathrm{W}, \mathcal{B}, v \rangle$
  - relacije $\mathcal{B}_i$ su tranzitivne i simetrične, ali **ne moraju biti refleksivne**
- nije aksioma $\mathrm{B}\alpha \rightarrow \alpha$

Temporalne logike

Vremenski operatori

- Oblici $\Box$:
  uvek u budućnosti: $\mathtt{G}$
  uvek u prošlosti: $\mathtt{H}$

Vremenski operatori

- Oblici $\Box$:
  uvek u budućnosti: $\mathtt{G}$
  uvek u prošlosti: $\mathtt{H}$

- biće u budućnosti: $\mathtt{F} = \neg\mathtt{G}\neg$
- bilo je u prošlosti: $\mathtt{P} = \neg\mathtt{H}\neg$

Vremenski operatori

- Oblici $\Box$:
  uvek u budućnosti: $\mathtt{G}$
  uvek u prošlosti: $\mathtt{H}$

- biće u budućnosti: $\mathtt{F} = \neg\mathtt{G}\neg$
- bilo je u prošlosti: $\mathtt{P} = \neg\mathtt{H}\neg$

- $\mathtt{P}p \wedge \mathtt{PH}\neg p \rightarrow \mathtt{P}(\mathtt{GP}p \wedge \mathtt{H}\neg p)$

Modeli

Model $\mathcal{M} = \langle W, R, v \rangle$

- W – skup vremenskih trenutaka
- R – relacija 'biti ranije' ili 'ne biti kasnije'
- v – valuacija

Struktura skupa vremenskih trenutaka:

- prirodni brojevi $\mathbb{N}$
- racionalni brojevi $\mathbb{Q}$
- realni brojevi $\mathbb{R}$
- kružno vreme, linearno, razgranato . . .

Linearna temporalna logika LTL

Vreme za LTL:

- ima nulti trenutak (početak), ali nema kraj,
- diskretno je, za svaki trenutak postoji sledeći.

- Jezik klasične iskazne logike: Var, $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$

- Unarni temporalni operatori: $\bigcirc$, $\bullet$ (u sledećem/prethodnom trenutku)

- Binarni temporalni operatori: $\mathtt{U}$, $\mathtt{S}$ (sve dok nije/od kada je)

Linearna temporalna logika LTL

Vreme za LTL:

- ima nulti trenutak (početak), ali nema kraj,
- diskretno je, za svaki trenutak postoji sledeći.

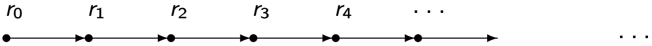
- Jezik klasične iskazne logike: Var, $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$

- Unarni temporalni operatori: $\bigcirc$, $\bullet$ (u sledećem/prethodnom trenutku)

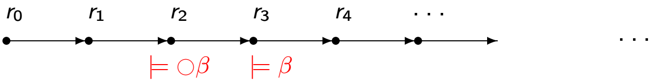
- Binarni temporalni operatori: $\mathtt{U}$, $\mathtt{S}$ (sve dok nije/od kada je)

- $\mathtt{F}\alpha =_{def} (\alpha \rightarrow \alpha)\mathtt{U}\alpha$, $\mathtt{G}\alpha =_{def} \neg\mathtt{F}\neg\alpha$, and
  $\mathtt{P}\alpha =_{def} (\alpha \rightarrow \alpha)\mathtt{S}\alpha$, $\mathtt{H}\alpha =_{def} \neg\mathtt{P}\neg\alpha$.

Satisfiability relation for LTL

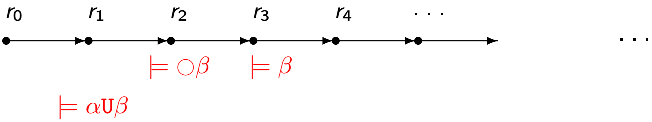


Satisfiability relation for LTL



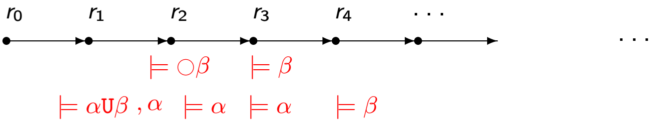
$r_2 \models \bigcirc\beta$ akko $r_3 \models \beta$

Satisfiability relation for LTL



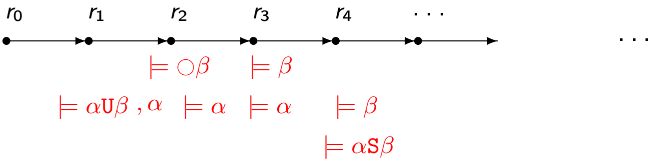
$r_1 \models \alpha \mathtt{U} \beta$ akko $(\exists j \geqslant 1)(r_j \models \beta \ \wedge (\forall k \in [1, j))(r_k \models \alpha))$
$r_2 \models \bigcirc\beta$ akko $r_3 \models \beta$

Satisfiability relation for LTL



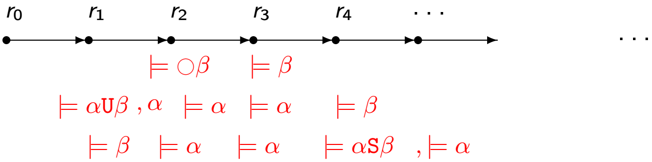
$r_1 \models \alpha \mathtt{U} \beta$ akko $(\exists j \geqslant 1)(r_j \models \beta \ \wedge (\forall k \in [1, j))(r_k \models \alpha))$
$r_2 \models \bigcirc\beta$ akko $r_3 \models \beta$

Satisfiability relation for LTL



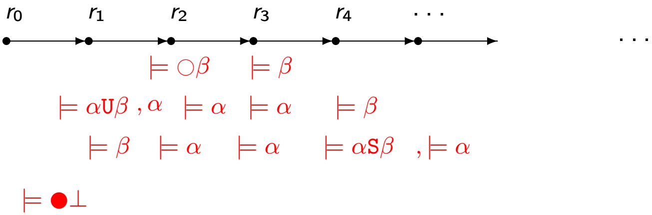
$$r_1 \models \alpha \mathtt{U} \beta \text{ akko } (\exists j \geqslant 1)(r_j \models \beta \ \wedge (\forall k \in [1, j))(r_k \models \alpha))$$
$$r_2 \models \bigcirc\beta \text{ akko } r_3 \models \beta$$
$$r_4 \models \alpha \mathtt{S} \beta \text{ akko } (\exists j \leqslant 4)(r_j \models \beta \ \wedge (\forall k \in (j, 4])(r_k \models \alpha))$$

Satisfiability relation for LTL



$r_1 \models \alpha \mathtt{U} \beta$ akko $(\exists j \geqslant 1)(r_j \models \beta \ \wedge (\forall k \in [1, j))(r_k \models \alpha))$
$r_2 \models \bigcirc \beta$ akko $r_3 \models \beta$
$r_4 \models \alpha \mathtt{S} \beta$ akko $(\exists j \leqslant 4)(r_j \models \beta \ \wedge (\forall k \in (j, 4])(r_k \models \alpha))$

Satisfiability relation for LTL



$r_0 \models \bullet\bot$

$r_1 \models \alpha \mathtt{U} \beta$ akko $(\exists j \geqslant 1)(r_j \models \beta \ \wedge (\forall k \in [1, j))(r_k \models \alpha))$

$r_2 \models \bigcirc\beta$ akko $r_3 \models \beta$

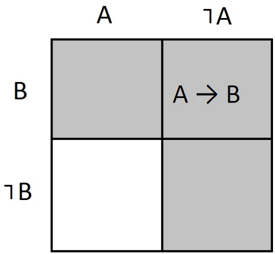
$r_4 \models \alpha \mathtt{S} \beta$ akko $(\exists j \leqslant 4)(r_j \models \beta \ \wedge (\forall k \in (j, 4])(r_k \models \alpha))$

Primeri formula

- $\alpha \rightarrow \mathtt{F}\beta$ – ako je α zadovoljena u nekom momentu, β će biti zadovoljena nakon tog momenta
- $\mathtt{G}(\alpha \rightarrow \mathtt{F}\beta)$ – posle svakog trenutka u kome važi α će postojati trenutak u kome važi β
- $\mathtt{FG}\alpha$ – α će nekom budućem momentu, početi da zauvek važi
- $\mathtt{G}(\alpha \rightarrow \mathtt{G}\alpha)$ – ako α bude važila u nekom trenutku, onda zauvek važi
- $\neg\beta\mathtt{U}\alpha$ – formula β neće važiti pre nego važi α

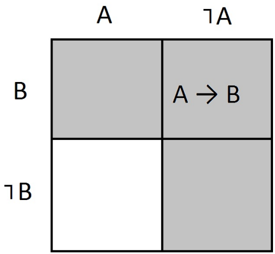
Verovatnosne logike

Zaključivanje u prisustvu neizvesnosti: verovatnosni MP



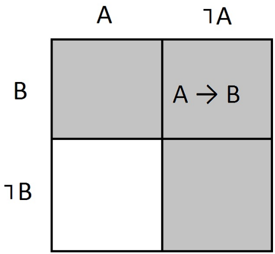
- $P(A) = r$, $P(A \rightarrow B) = s$, $P(B) = ?$

Zaključivanje u prisustvu neizvesnosti: verovatnosni MP



- $P(A) = r,\ P(A \to B) = s,\ P(B) = ?$
- $P(B) \leqslant P(A \to B)$
- $P(A \to B) \leqslant P(\neg A) + P(B)$

Zaključivanje u prisustvu neizvesnosti: verovatnosni MP



- $P(A) = r,\ P(A \to B) = s,\ P(B) =?$
- $P(B) \leqslant P(A \to B)$
- $P(A \to B) \leqslant P(\neg A) + P(B)$

$$P(A \to B) - (1 - P(A)) \leqslant P(B) \leqslant P(A \to B)$$

Zajedničke karakteristike

- Verovatnosne logike pružaju mogućnost formalnog rezovanja o verovatnoćama koristeći dobro definisanu sintaksu i semantiku.
- Formulu su tačne ili netačne.
- Formule nemaju numeričke istinitosne vrednosti.

Verovatnosni operatori $P_{\geqslant s}$

- Jezik klasične iskazne logike: $\mathrm{Var} = \{p, q, p_1, p_2, \dots\}$, $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$
- $P_{\geqslant s}, \quad s \in [0,1]_{\mathbb{Q}} \quad (= \mathbb{Q} \cap [0,1])$
- $P_{<s}\alpha$ je skraćenica za $\neg P_{\geqslant s}\alpha$, …

Verovatnosni operatori $P_{\geqslant s}$

- Jezik klasične iskazne logike: $\mathrm{Var} = \{p, q, p_1, p_2, \ldots\}$, $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$
- $P_{\geqslant s}, \quad s \in [0,1]_{\mathbb{Q}} \quad (= \mathbb{Q} \cap [0,1])$
- $P_{<s}\alpha$ je skraćenica za $\neg P_{\geqslant s}\alpha$, ...
- $P_{=1}((P_{\geqslant s}\alpha \wedge P_{<t}(\alpha \rightarrow \beta)) \rightarrow P_{=r}\beta)$

Verovatnosni modeli

$\mathcal{M} = \langle \mathrm{W}, Prob, v \rangle$:

- W je skup svetova
- $v : \mathrm{W} \times \mathrm{Var} \rightarrow \{\top, \bot\}$

- $Prob(w) = \langle \mathrm{W}(w), H(w), \mu(w) \rangle$ je verovatnosni prostor:
  - $\mathrm{W}(w) \subset W$,
  - $H(w)$ je algebra podskupova od $\mathrm{W}(w)$ i
  - $\mu(w) : H(w) \rightarrow [0, 1]$ je konačno aditivna verovatnoća.

Verovatnosni modeli

$$\mathcal{M} = \langle \mathrm{W}, \overbrace{Prob}^{\mathcal{K}}, v \rangle:$$

- W je skup svetova
- $v : \mathrm{W} \times \mathrm{Var} \rightarrow \{\top, \bot\}$

- $Prob(w) = \langle \mathrm{W}(w), H(w), \mu(w) \rangle$ je verovatnosni prostor:
  - $\mathrm{W}(w) \subset W$,
  - $H(w)$ je algebra podskupova od $\mathrm{W}(w)$ i
  - $\mu(w) : H(w) \rightarrow [0, 1]$ je konačno aditivna verovatnoća.

Verovatnosni modeli

$\mathcal{M} = \langle \mathrm{W}, Prob, v \rangle$:

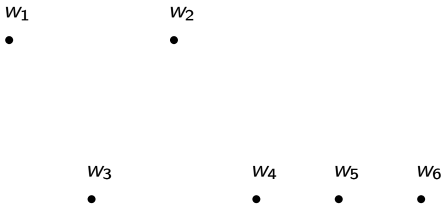
- W je skup svetova
- $v : \mathrm{W} \times \mathrm{Var} \to \{\top, \bot\}$

- $Prob(w) = \langle \mathrm{W}(w), H(w), \mu(w) \rangle$ je verovatnosni prostor:
  - $\mathrm{W}(w) \subset W$,
  - $H(w)$ je algebra podskupova od $\mathrm{W}(w)$ i
  - $\mu(w) : H(w) \to [0, 1]$ je konačno aditivna verovatnoća.

- Merljivi modeli: $[\alpha]_w = \{u \in \mathrm{W}(w) : u \models \alpha\} \in H(w),\ \forall w, \alpha$.

Verovatnosni modeli (2)

$\mu(w_1)(\{w_i\}) = \frac{1}{6}, \quad i \in \{1, \ldots, 6\}$



Verovatnosni modeli (2)

$$\mu(w_1)(\{w_i\}) = \frac{1}{6}, \quad i \in \{1, \ldots, 6\}$$

Verovatnosni modeli (2)

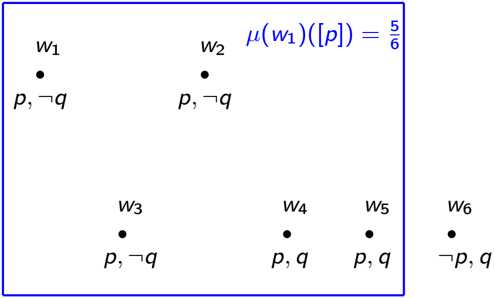
$$\mu(w_1)(\{w_i\}) = \frac{1}{6}, \quad i \in \{1, \dots, 6\}$$

w_1: $p, \neg q$ $\quad$ w_2: $p, \neg q$

w_3: $p, \neg q$ $\quad$ w_4: p, q $\quad$ w_5: p, q $\quad$ w_6: $\neg p, q$

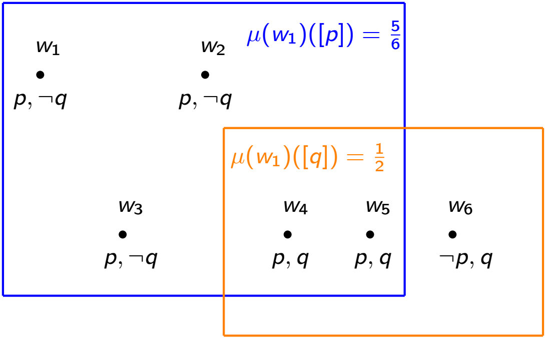
Verovatnosni modeli (2)

$$\mu(w_1)(\{w_i\}) = \frac{1}{6}, \quad i \in \{1, \dots, 6\}$$



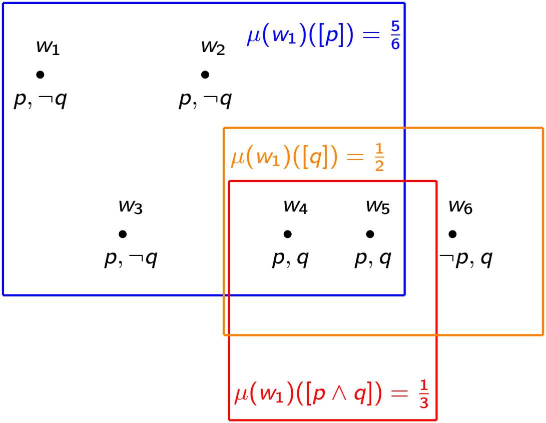
Verovatnosni modeli (2)

$$\mu(w_1)(\{w_i\}) = \frac{1}{6}, \quad i \in \{1, \ldots, 6\}$$



Verovatnosni modeli (2)

$$\mu(w_1)(\{w_i\}) = \frac{1}{6}, \quad i \in \{1, \dots, 6\}$$



Zadovoljivost

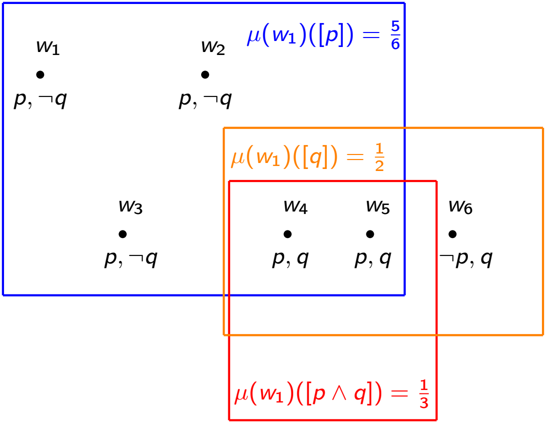
$\mathcal{M} = \langle \mathrm{W}, Prob, v \rangle$, $w \in \mathrm{W}$:

- ako $p \in \mathrm{Var}$, $w \models p$ akko $v(w)(p) = \top$,
- $w \models P_{\geqslant s}\alpha$ akko $\mu(w)([\alpha]_w) \geqslant s$
- $w \models \neg\alpha$ akko $w \not\models \alpha$,
- $w \models \alpha \wedge \beta$ akko $w \models \alpha$ and $w \models \beta$.

Skup formula $F = \{\alpha_1, \alpha_2, \ldots\}$ je zadovoljiv ako postoji svet $w \in \mathrm{W}$: $w \models \alpha_i$ za $i = 1, 2, \ldots$.

Zadovoljivost (2)

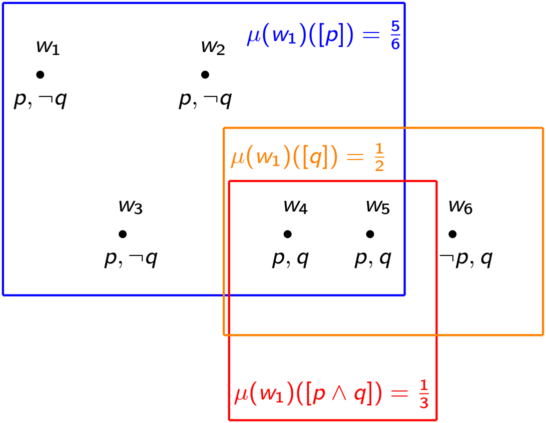
$$\mu(w_1)(\{w_i\}) = \frac{1}{6}, \quad i \in \{1, \ldots, 6\}$$



$w_1 \not\models q$

Zadovoljivost (2)

$\mu(w_1)(\{w_i\}) = \frac{1}{6}, \quad i \in \{1, \dots, 6\}$

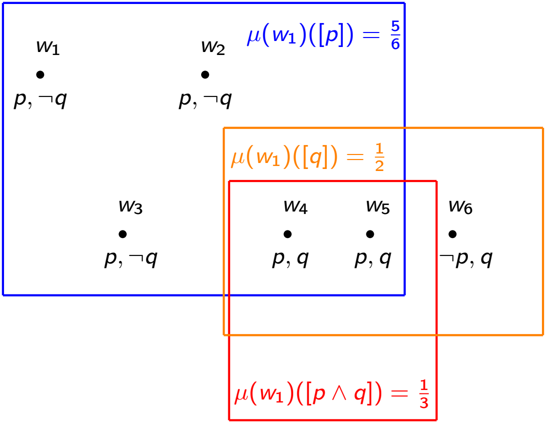


$w_1 \not\models q$

$w_1 \not\models p \wedge q$

Zadovoljivost (2)

$$\mu(w_1)(\{w_i\}) = \frac{1}{6}, \quad i \in \{1, \ldots, 6\}$$



$w_1 \not\models q$

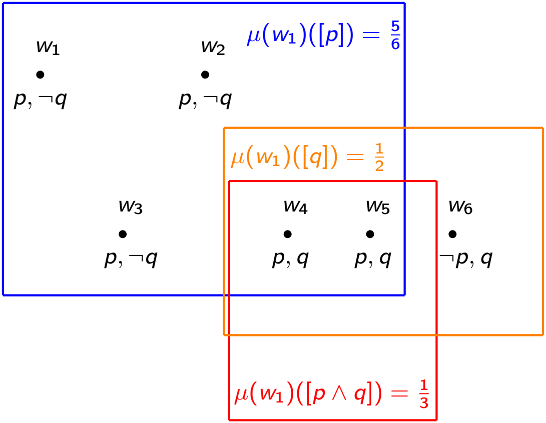
$w_1 \not\models p \wedge q$

$w_4 \models p \wedge q$

$w_5 \models p \wedge q$

Zadovoljivost (2)

$$\mu(w_1)(\{w_i\}) = \frac{1}{6}, \quad i \in \{1, \dots, 6\}$$



$w_1 \not\models q$

$w_1 \not\models p \wedge q$

$w_4 \models p \wedge q$

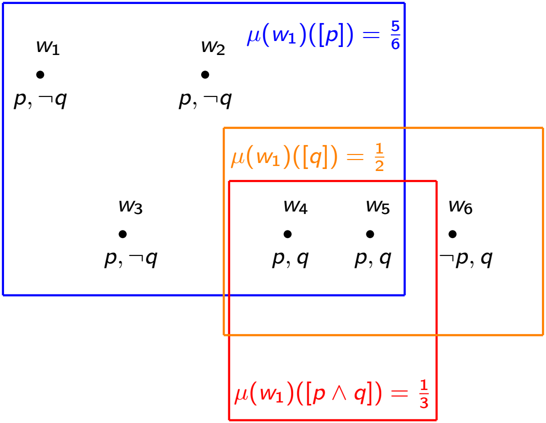
$w_5 \models p \wedge q$

$w_1 \models P_{\geqslant 0.5}\, p$

$w_1 \models P_{=1/3}(p \wedge q)$

Zadovoljivost (2)

$$\mu(w_1)(\{w_i\}) = \tfrac{1}{6}, \quad i \in \{1, \ldots, 6\}$$



$w_1 \not\models q$

$w_1 \not\models p \wedge q$

$w_4 \models p \wedge q$

$w_5 \models p \wedge q$

$w_1 \models P_{\geqslant 0.5}\, p$

$w_1 \models P_{=1/3}(p \wedge q)$

$w_1 \models P_{=1/3}(p \wedge q) \wedge P_{\leqslant 0.9}\, p$

Teorijski rezultati

- Nekompaktnost: $\{\neg P_{=0}p\} \cup \{P_{<1/n}p : n \in \mathbb{N}\}$

Teorijski rezultati

- Nekompaktnost: $\{\neg P_{=0} p\} \cup \{P_{<1/n} p : n \in \mathbb{N}\}$
- Jaka potpunost logike: $T \models \alpha$ akko $T \vdash \alpha$
- Ne postoji rekurzivna jako kompletna aksiomatizacija iskazne verovatnosne logike za realno vrednosne verovatnoće.
- Ne postoji nikakva rekurzivna kompletna aksiomatizacija predikatske verovatnosne logike za realno vrednosne verovatnoće.

Teorijski rezultati

- Nekompaktnost: $\{\neg P_{=0}p\} \cup \{P_{<1/n}p : n \in \mathbb{N}\}$
- Jaka potpunost logike: $T \models \alpha$ akko $T \vdash \alpha$
- Ne postoji rekurzivna jako kompletna aksiomatizacija iskazne verovatnosne logike za realno vrednosne verovatnoće.
- Ne postoji nikakva rekurzivna kompletna aksiomatizacija predikatske verovatnosne logike za realno vrednosne verovatnoće.
- Odlučivost: postoji procedura koja ya proiyvoljnu formulu u konačno mnogo koraka proverava da li je zadovoljiva ili ne.

Teorijski rezultati (2): Arhimedovo pravilo

Iz

$$\{P_{\geq s-\frac{1}{k}}p : k \in \mathbb{N}\}$$

izvesti

$$P_{\geq s}A$$

Teorijski rezultati (2): Arhimedovo pravilo

Iz

$$\{P_{\geq s-\frac{1}{k}}p : k \in \mathbb{N}\}$$

izvesti

$$P_{\geq s}A$$

- dokaz - prebrojiv niz formula
- teoreme jake potpunosti u iskaznom i predikatskom slučaju

Teorijski rezultati (3): Aksiomatizacija

- Aksiomatizacija klasične iskazne/predikatske logike

- Verovatnosne aksiome:
  - $P_{\geqslant 0}\alpha$
  - $P_{\leqslant r}\alpha \rightarrow P_{<s}\alpha$, $s > r$
  - $P_{<s}\alpha \rightarrow P_{\leqslant s}\alpha$
  - $(P_{\geqslant r}\alpha \wedge P_{\geqslant s}\beta \wedge P_{\geqslant 1}(\neg(\alpha \wedge \beta))) \rightarrow P_{\geqslant \min(1,r+s)}(\alpha \vee \beta)$
  - $(P_{\leqslant r}\alpha \wedge P_{<s}\beta) \rightarrow P_{<r+s}(\alpha \vee \beta)$, $r + s \leqslant 1$

- Verovatnosna pravila izvodjenja:
  - Necesitacija: Iz α izvesti $P_{\geq 1}\alpha$
  - Arhimedovo pravilo: Iz $\{\alpha \rightarrow P_{\geq s-\frac{1}{k}}\beta : k \in \mathbb{N}\}$ izvesti $\alpha \rightarrow P_{\geq s}\beta$.

Teorijski rezultati (4): Odlučivost

Odlučivost i složenost: PSAT je NP-kompletan.

Teorijski rezultati (4): Odlučivost

Odlučivost i složenost: PSAT je NP-kompletan.

$P_{\geqslant 0.35}(p \to q) \wedge P_{\geqslant 0.6}\, q$

Teorijski rezultati (4): Odlučivost

Odlučivost i složenost: PSAT je NP-kompletan.

$$P_{\geqslant 0.35}(p \to q) \wedge P_{\geqslant 0.6}\, q$$

$$P_{\geqslant 0.35}(\overbrace{\underbrace{(p \wedge q)}_{\text{atom}} \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q)}^{p \to q}) \wedge P_{\geqslant 0.6}(\overbrace{(p \wedge q) \vee (\neg p \wedge q)}^{q})$$

Teorijski rezultati (4): Odlučivost

Odlučivost i složenost: PSAT je NP-kompletan.

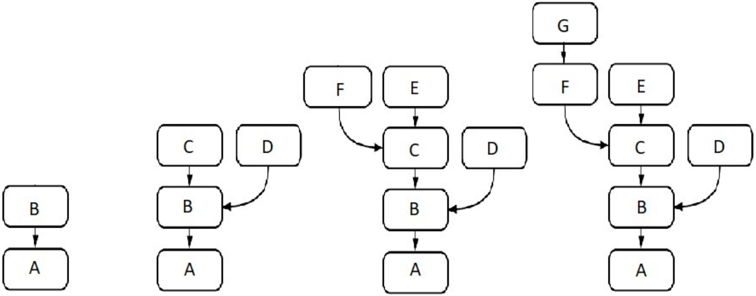
$$P_{\geqslant 0.35}(p \to q) \wedge P_{\geqslant 0.6}\, q$$

$$P_{\geqslant 0.35}(\overbrace{(\underbrace{(p \wedge q)}_{\text{atom}} \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q))}^{p \to q}) \wedge P_{\geqslant 0.6}(\overbrace{(p \wedge q) \vee (\neg p \wedge q)}^{q})$$

$$\mu(p \wedge q) + \mu(p \wedge \neg q) + \mu(\neg p \wedge q) + \mu(\neg p \wedge \neg q) = 1$$
$$\mu(p \wedge q) \geqslant 0,\ \mu(p \wedge \neg q) \geqslant 0,\ \mu(\neg p \wedge q) \geqslant 0,\ \mu(\neg p \wedge \neg q) \geqslant 0$$
$$\mu(p \wedge q) + \mu(\neg p \wedge q) + \mu(\neg p \wedge \neg q) \geqslant 0.35$$
$$\mu(p \wedge q) + \mu(\neg p \wedge q) \geqslant 0.6$$

BlockChain i verovatnosno-temporalno-epistemička logika (PTEL)

Fork: podela lanca



Kriterijum najduže grane:

- svaki čvor bira lanac blokova na kome radi, a čuva ostale
- kada jedan lanac postane najduži svi čvorovi prelaze na njega (ABCFG).

Formalni jezik za PTEL

- Skup agenata $\mathbb{A} = \{a_1, \ldots, a_m\}$
- Skup iskaznih slova $\mathrm{Var} = \{p, q, p_1, p_2, \ldots\}$,
- $\mathrm{A} = \{A_a | a \in \mathbb{A}\} \subset \mathrm{Var}$, A_a: "Agent a je aktivan",
- operatori:
  - klasični, temporalni, epistemički: $\neg$, $\wedge$, $\bigcirc$, $\mathtt{U}$, $\bullet$, $\mathtt{S}$, $\mathtt{K}_a$, $\mathtt{C}$,
  - verovatnosni: $\mathtt{P}_{\geqslant s}$, $\mathtt{P}_{a,\geqslant s}$, za $a \in \mathbb{A}$, $s \in [0, 1]_{\mathbb{Q}}$.

Formalni jezik za PTEL

- Skup agenata $\mathbb{A} = \{a_1, \ldots, a_m\}$
- Skup iskaznih slova $\mathsf{Var} = \{p, q, p_1, p_2, \ldots\}$,
- $\mathsf{A} = \{A_a | a \in \mathbb{A}\} \subset \mathsf{Var}$, A_a: “Agent a je aktivan”,
- operatori:
  - klasični, temporalni, epistemički: $\neg$, $\wedge$, $\bigcirc$, $\mathtt{U}$, $\bullet$, $\mathtt{S}$, $\mathtt{K}_a$, $\mathtt{C}$,
  - verovatnosni: $\mathtt{P}_{\geqslant s}$, $\mathtt{P}_{a,\geqslant s}$, za $a \in \mathbb{A}$, $s \in [0,1]_{\mathbb{Q}}$.
  - $\bigcirc^0 \alpha =_{def} \alpha$ and $\bigcirc^{n+1} \alpha = \bigcirc \bigcirc^n \alpha$, $n \geqslant 0$,

Formalni jezik za PTEL

- Skup agenata $\mathbb{A} = \{a_1, \ldots, a_m\}$

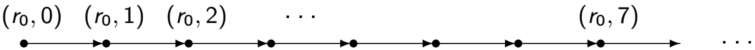
- Skup iskaznih slova $\mathrm{Var} = \{p, q, p_1, p_2, \ldots\}$,
- $\mathrm{A} = \{A_a | a \in \mathbb{A}\} \subset \mathrm{Var}$, A_a: "Agent a je aktivan",

- operatori:
  - klasični, temporalni, epistemički: $\neg$, $\wedge$, $\bigcirc$, $\mathtt{U}$, $\bullet$, $\mathtt{S}$, $\mathtt{K}_a$, $\mathtt{C}$,
  - verovatnosni: $\mathtt{P}_{\geqslant s}$, $\mathtt{P}_{a,\geqslant s}$, za $a \in \mathbb{A}$, $s \in [0,1]_{\mathbb{Q}}$.
  - $\bigcirc^0 \alpha =_{def} \alpha$ and $\bigcirc^{n+1}\alpha = \bigcirc \bigcirc^n \alpha$, $n \geqslant 0$,

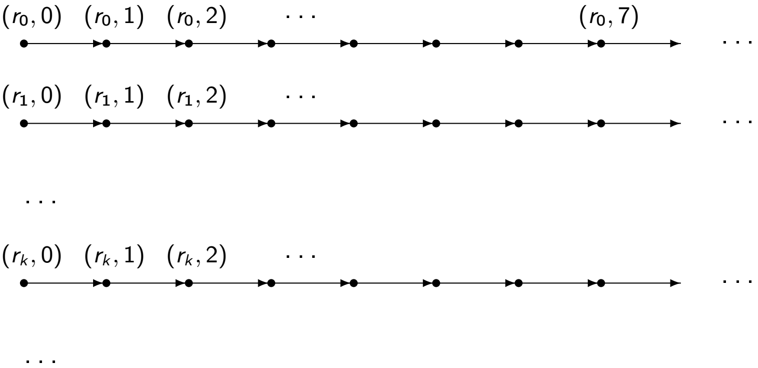
- $\mathtt{P}_{=s}(\mathtt{G}(\bigwedge_{a\in\mathbb{A}} \mathtt{K}_a \mathtt{P}_{b,\geqslant r}\alpha \to \bigcirc \mathtt{C}\mathtt{P}_{a,\geqslant r}\alpha))$

$(r_0, 0)$
$\bullet$

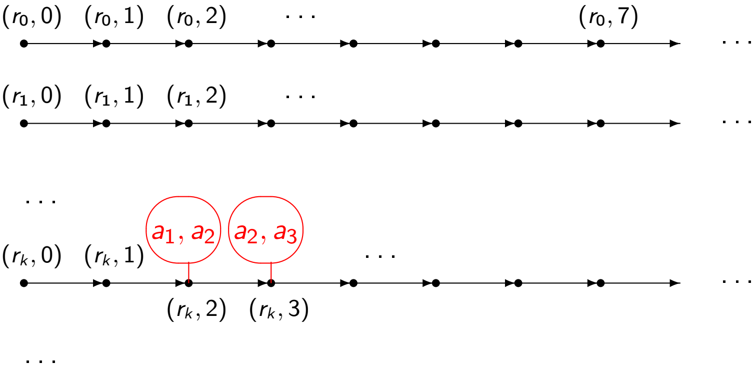
Tačka (svet, stanje) (r, t) – run r, vremenski trenutak t



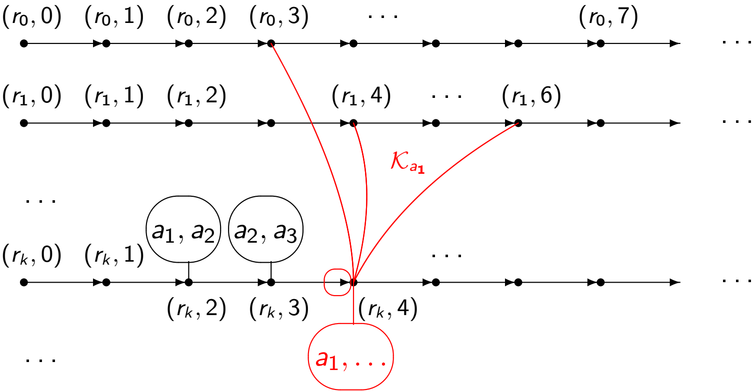
Run - jedno izvršavanje distribuiranog sistema



Distribuirani sistem – skup run-ova



Aktivni agenti



Relacija dostižnosti za a_1 u $(r_k, 4)$

Krajnje tačke (Dead-end points)

- Ako a nije aktivan u (r, n), tada $\neg\exists(r', n') \ \ (r, n)\mathcal{K}_a(r', n')$

Krajnje tačke (Dead-end points)

- Ako a nije aktivan u (r, n), tada $\neg\exists(r', n')\ \ (r, n)\mathcal{K}_a(r', n')$
- Ako a nije aktivan u (r, n), tada $(r, n) \models \mathtt{K}_a\bot$

Krajnje tačke (Dead-end points)

- Ako a nije aktivan u (r, n), tada $\neg\exists(r', n')\ \ (r, n)\mathcal{K}_a(r', n')$
- Ako a nije aktivan u (r, n), tada $(r, n) \models \mathtt{K}_a\bot$
- Zahtevi za relaciju dostižnosti:
    - simetričnost i tranzitivnost,
    - ako je a aktivan u (r, n), onda $(r, n)\mathcal{K}_a(r, n)$.

Merljivi skupovi objekata

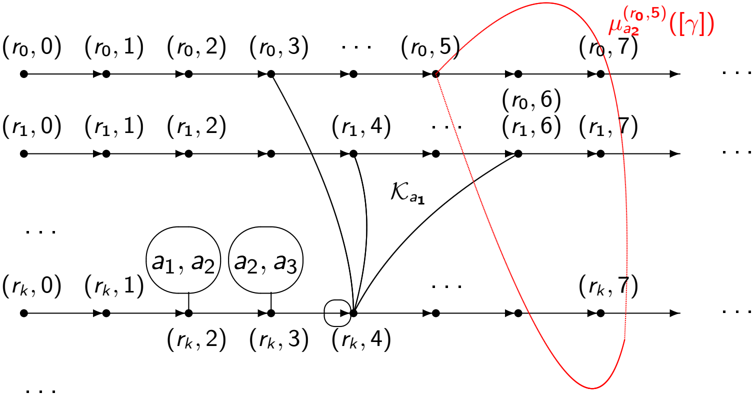
- Merljivi skupovi objekata su definabilni formulama
- Objekti: run-ovi, tačke

Merljivi skupovi objekata

- Merljivi skupovi objekata su definabilni formulama
- Objekti: run-ovi, tačke
- Verovatnoće:
  - lokalne koje daju agenti u sistemu i
  - globalna koju daje spoljašnji posmatrač (npr. dizajner sistema), nezavisno od agenata.

Merljivi skupovi objekata (2)

- skupovi run-ova koje meri spoljašnji posmatrač
  $[\alpha] = \{r : (r, 0) \models \alpha\}$,
- skupovi tačaka koje mere agenti
  $[\alpha]_a^{*(r,n)} = \{(r', n') \ : \ (r', n') \in W_a^{(r,n)} \quad \text{and} \quad (r', n') \models \alpha\}$.



Verovatnoće koje daju agenti

- PTEL-model sadrži skup run-ova.
- Run je beskonačni niz tačaka, reprezentuje jedno izvršavanje sistema.
- Svaka tačka ima:
  - skup iskaznih slova koje su u njoj tačne,
  - skup agenata koji su u njoj aktivni,
  - skup relacija dostižnosti (za aktivne agente) i
  - skup verovatnoća koje mere skupove tačaka (run-ova).

PTEL-modeli, $\mathcal{M}$

Definition

PTEL-model $\mathcal{M} = \langle \mathrm{R}, \mathcal{A}, \mathcal{K}, \mathcal{P} \rangle$:

- R is a non-empty set of runs, where:
  - Every *run* r is a function from $\mathbb{N}$ to $\mathbb{P}(\mathrm{Var})$.
  - The pair (r, n), where $r \in \mathrm{R}$ and $n \in \mathbb{N}$, is called a *point*; the set of all points in $\mathcal{M}$ is denoted by W.
- $\mathcal{A} : \mathrm{W} \to \mathbb{P}(\mathbb{A})$, where:
  - $\mathcal{A}((r, n))$ denotes the set of *active agents* associated to the points (r, n), and
  - $a \in \mathcal{A}((r, n))$ iff $A_a \in r(n)$.
- $\mathcal{K} = \{\mathcal{K}_a : a \in \mathbb{A}\}$ is a set of symmetric and transitive *accessibility relations* on W, such that:
  - $a \notin \mathcal{A}((r, n))$ iff $(r, n)\mathcal{K}_a(r', n')$ is false for all (r', n').
  - $\mathcal{K}_a(r, n)$ denotes the set of all points *accessible*, according to the agent a, from (r, n).
- ...

PTEL-model, $\mathcal{M} = \langle \mathrm{R}, \mathcal{A}, \mathcal{K}, \mathcal{P} \rangle$

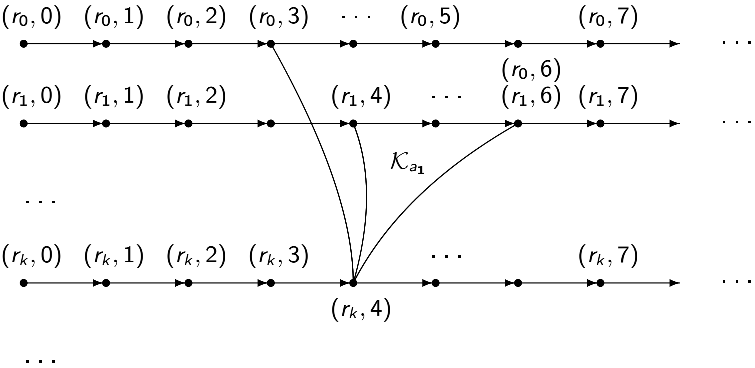
Definition

- ...
- $\mathcal{P}$ is a function defined on W, such that $\mathcal{P}((r, n))$ is a structure $\langle H^{(r,n)}, \mu^{(r,n)}, \{\mathcal{P}_a : a \in \mathbb{A}\}\rangle$, where
  - $H^{(r,n)}$ is an algebra of subsets of R,
  - $\mu^{(r,n)} : H^{(r,n)} \to [0, 1]$ is a finitely-additive probability measure on $H^{(r,n)}$,
  - $\{\mathcal{P}_a : a \in \mathbb{A}\}$ is the set of functions defined on W, where $\mathcal{P}_a((r, n))$ is a probability space $\langle \mathrm{W}_a^{(r,n)}, H_a^{(r,n)}, \mu_a^{(r,n)}\rangle$ such that:
    - $\mathrm{W}_a^{(r,n)}$ is a non-empty subset of W,
    - $H_a^{(r,n)}$ is an algebra of subsets of $\mathrm{W}_a^{(r,n)}$, and
    - $\mu_a^{(r,n)} : H_a^{(r,n)} \to [0, 1]$ is a finitely-additive probability measure.

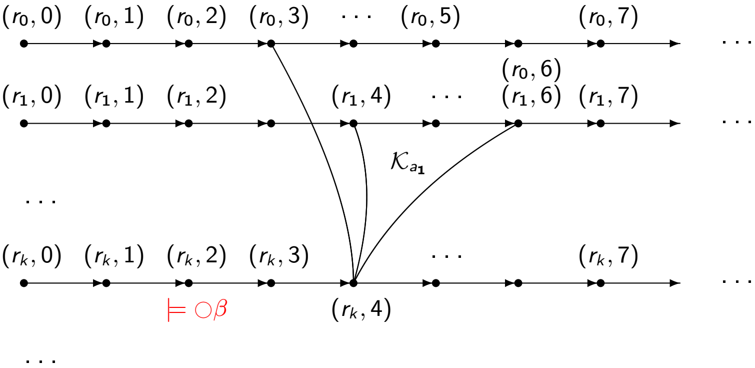
Zadovoljivost za PTEL, temporal deo

Definition

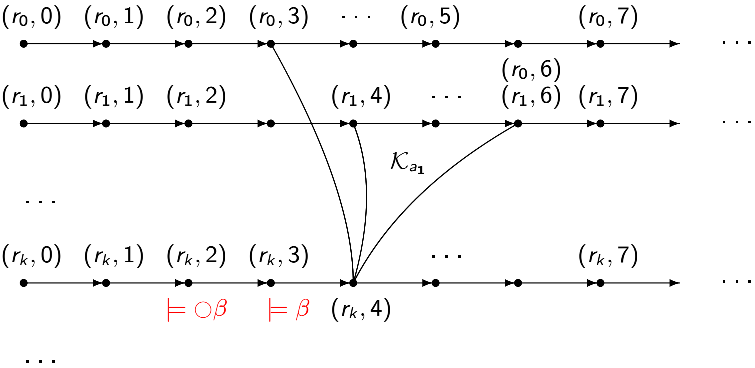
- if $p \in \mathrm{Var}$, $(r, n) \models p$ iff $p \in r(n)$,
- $(r, n) \models \alpha \wedge \beta$ iff $(r, n) \models \alpha$, $(r, n) \models \beta$,
- $(r, n) \models \neg\beta$ iff $(r, n) \not\models \beta$
- $(r, n) \models \bigcirc\beta$ iff $(r, n+1) \models \beta$,
- $(r, n) \models \alpha \mathtt{U} \beta$ iff $(\exists j \geqslant n)(r, j) \models \beta \ \wedge \ (\forall k \in [n, j))(r, k) \models \alpha$,
- $(r, n) \models \bullet\beta$ iff $n = 0$, or $n \geqslant 1$ i $(r, n-1) \models \beta$,
- $(r, n) \models \alpha \mathtt{S} \beta$ iff $(\exists j \in [0, n])(r, j) \models \beta \ \wedge \ (\forall k \in (j, n])(r, k) \models \alpha$,
- ...



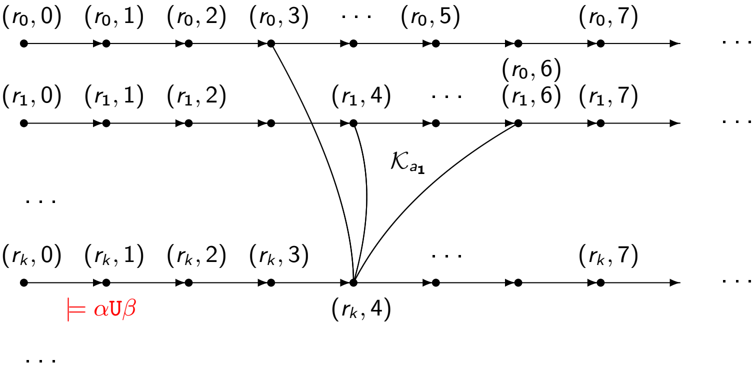
$(r_k, 2) \models \bigcirc\beta$ iff $(r_k, 3) \models \beta$



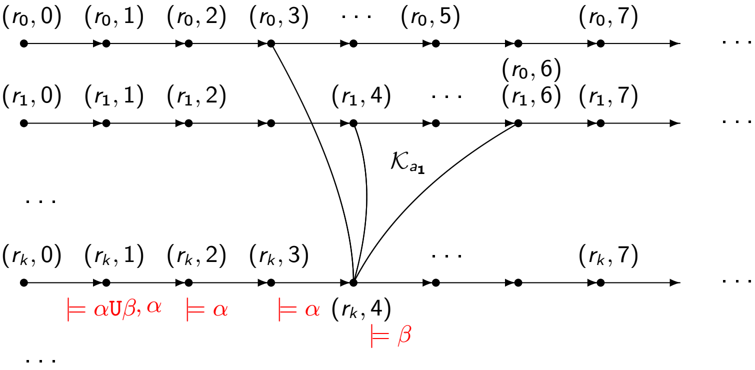
$(r_k, 2) \models \bigcirc\beta$ iff $(r_k, 3) \models \beta$



$(r_k, 2) \models \bigcirc\beta$ iff $(r_k, 3) \models \beta$



$(r_k, 1) \models \alpha \mathtt{U} \beta$

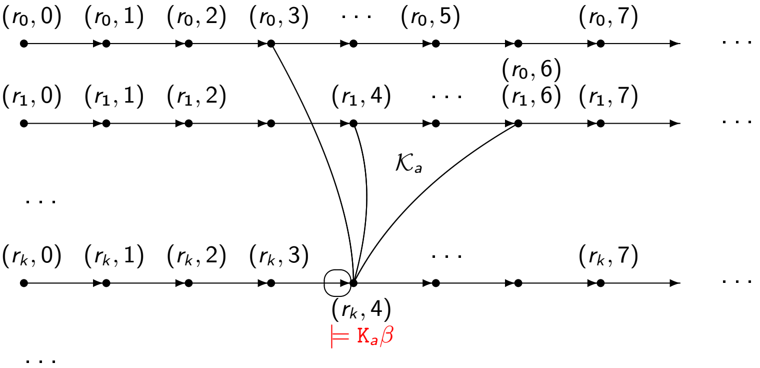


$(r_k, 1) \models \alpha \mathtt{U} \beta$

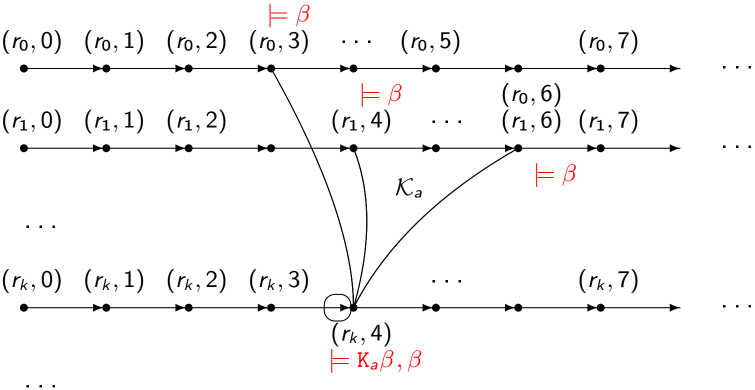
Zadovoljivost za PTEL (2), epistemički deo

Definition

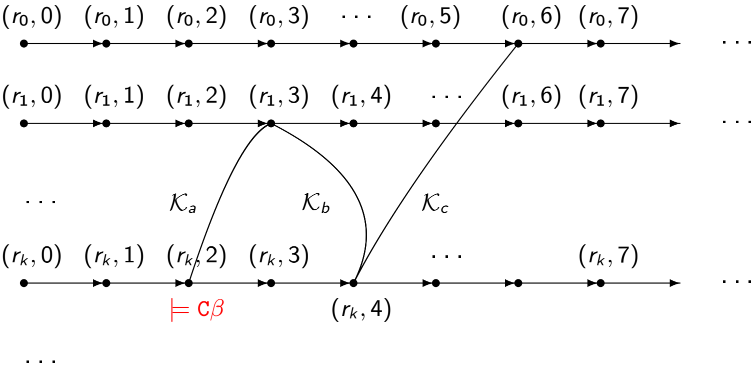
- ...
- $(r, n) \models \mathtt{K}_a\beta$ iff $(\forall(r', n') \in \mathcal{K}_a(r, n))(r', n') \models \beta$
- $(r, n) \models \mathtt{C}\beta$ iff $(\forall k \geqslant 0)(r, n) \models \mathtt{E}^k\beta$,
- or artenatively:
  - (r', k') is reachable from (r, k) if there is a sequence $(r, k) = (r_0, k_0), (r_1, k_1), \ldots, (r_m, k_m) = (r', k')$, such taht $(r_j, k_j)\mathcal{K}_{a_j}(r_{j+1}, k_{j+1})$, $j \in [0, m-1]$ and
  - $(r, n) \models \mathtt{C}\beta$ iff $(r', n') \models \beta$, $\forall(r', n')$ reachable from (r, n)
- ...



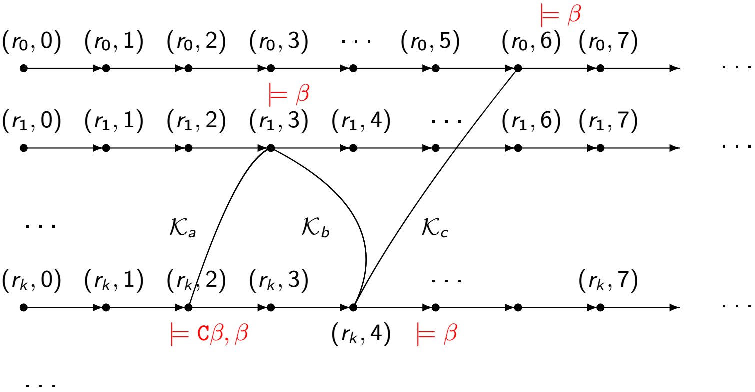
$(r_k,4) \models \mathtt{K}_a\beta$



$(r_k, 4) \models \mathtt{K}_a\beta$



$(r_k, 2) \models \mathtt{C}\beta$

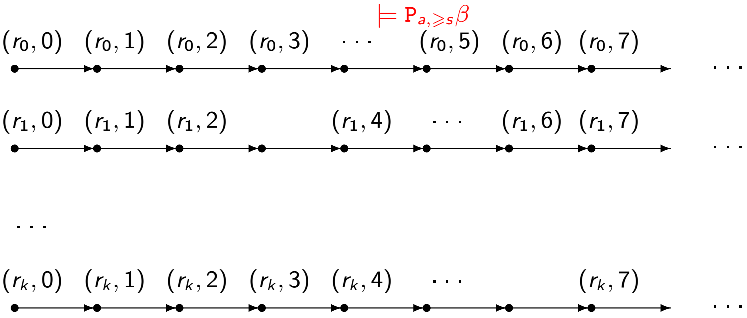


$(r_k, 2) \models \mathtt{C}\beta$

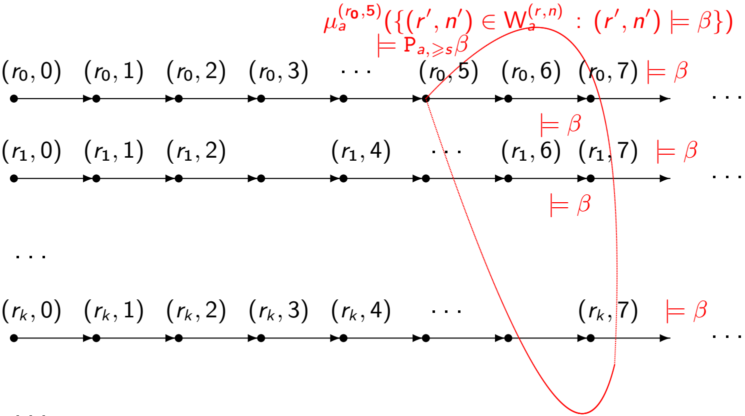
Zadovoljivost za PTEL (3), verovatnosni deo

Definition

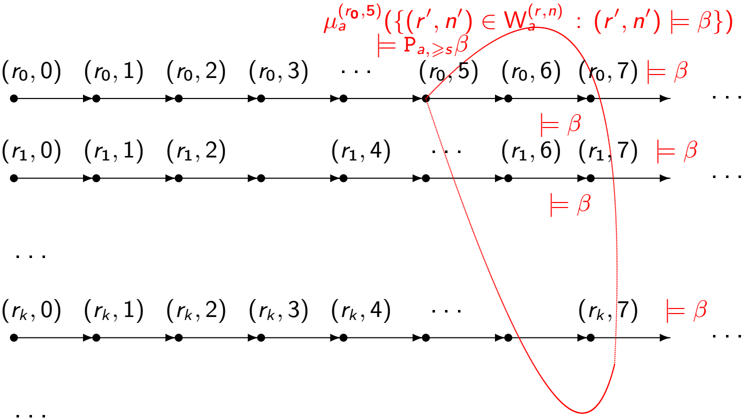
- ...
- $(r, n) \models \mathrm{P}_{\geqslant s}\beta$ iff $\mu_{\star}^{(r,n)}(\{r \in \mathrm{R} : (r, 0) \models \beta\}) \geqslant s$.
- $(r, n) \models \mathrm{P}_{a,\geqslant s}\beta$ iff $\mu_{\star,a}^{(r,n)}(\{(r', n') \in \mathrm{W}_a^{(r,n)} : (r', n') \models \beta\}) \geqslant s$. ■



$$(r_0,5) \models \mathrm{P}_{a,\geqslant s}\beta \text{ iff } \mu_a^{(r_0,5)}(\{(r',n') \in \mathrm{W}_a^{(r,n)} : (r',n') \models \beta\}) \geqslant s$$



$$(r_0,5) \models P_{a,\geqslant s}\beta \text{ iff } \mu_a^{(r_0,5)}(\{(r',n') \in W_a^{(r,n)} : (r',n') \models \beta\}) \geqslant s$$



$$(r_0,5) \models P_{\geqslant s}\beta \text{ iff } \mu^{(r_0,5)}(\{r' \in R : (r',0) \models \beta\}) \geqslant s$$
$$(r_0,5) \models P_{a,\geqslant s}\beta \text{ iff } \mu_a^{(r_0,5)}(\{(r',n') \in W_a^{(r,n)} : (r',n') \models \beta\}) \geqslant s$$

Valjane formule. Semantičke posledice

Definition

Formula α je

- vlajana u modelu, $\mathcal{M} \models \alpha$ ako za svaku tačku (r, n) iz $\mathcal{M}$, $(r, n) \models \alpha$.
- **valjana**, $\models \alpha$, ako za svaki model $\mathcal{M} \models \alpha$.

Skup formula F je zadovoljiv ako postoji tačka (r, n) iz nekog modela $\mathcal{M}$ tako da:

- $(r, n) \models \alpha$, za sve $\alpha \in$ F.
- Formula α je zadovoljiva ako je skup $\{\alpha\}$ zadovoljiv.

Formula α je semantička posledica skupa formula F, F $\models \alpha$, ako za svaki model $\mathcal{M}$ i svaku tačku (r, n) iz $\mathcal{M}$:

- ako $(r, n) \models$ F, onda $(r, n) \models \alpha$. ■

Logička pitanja (1)

- Kompletan aksiomatski sistem:
  - slaba potpunost (svaka konzistentna formula je zadovoljiva, $\models A$ akko $\vdash A$)
  - jaka potpunost (svaki konzistentan skup formula je zadovoljiv, $F \models A$ akko $F \vdash A$)
- Odlučivost:
  postoji procedura koja odlučuje da li je formula zadovoljiva/valjana.

Logička pitanja (1)

- Kompletan aksiomatski sistem:
  - slaba potpunost (svaka konzistentna formula je zadovoljiva, $\models A$ akko $\vdash A$)
  - jaka potpunost (svaki konzistentan skup formula je zadovoljiv, $F \models A$ akko $F \vdash A$)
- Odlučivost:
  postoji procedura koja odlučuje da li je formula zadovoljiva/valjana.
- Kompaktnost:
  skup formula je zadovoljiv akko je svaki njegov konačan podskup zadovoljiv.

Aksiome i pravila

Axioms and rules for:

- Classical reasoning
- Temporal reasoning
- Epistemic reasoning
- Probabilistic reasoning

I) Classical axioms and rules

Prop. Instances of classical tautologies

MP. $$\frac{\alpha, \alpha \to \beta}{\beta}$$ (Modus Ponens)

II) Temporal axioms and rules (1)

A$\bigcirc\neg$.	$\neg\bigcirc\alpha \leftrightarrow \bigcirc\neg\alpha$	
A$\bigcirc\rightarrow$.	$\bigcirc(\alpha \rightarrow \beta) \rightarrow (\bigcirc\alpha \rightarrow \bigcirc\beta)$	(Distribution Axiom for $\bigcirc$)
A$\mathtt{U}\bigcirc$.	$\alpha\mathtt{U}\beta \leftrightarrow \beta \vee (\alpha \wedge \bigcirc(\alpha\mathtt{U}\beta))$	
A$\mathtt{UF}$.	$\alpha\mathtt{U}\beta \rightarrow \mathtt{F}\beta$	
A$\bullet\neg$.	$\neg\bullet\neg\alpha \rightarrow \bullet\alpha$	
A$\bullet\rightarrow$.	$\bullet(\alpha \rightarrow \beta) \rightarrow (\bullet\alpha \rightarrow \bullet\beta)$	(Distribution Axiom for $\bullet$)
A$\bullet\wedge$.	$(\bullet\alpha \wedge \bullet\beta) \rightarrow \bullet(\alpha \wedge \beta)$	
A$\bigcirc\bullet$.	$\bigcirc\bullet\alpha \leftrightarrow \alpha$	(Inversion for $\bigcirc$ and $\bullet$)
A$\bigcirc\bullet$C$_1$.	$\bigcirc\bullet\alpha \rightarrow \bullet\bigcirc\alpha$	(Commutativity for $\bigcirc$ and $\bullet$)
A$\bigcirc\bullet$C$_2$.	$\neg\bullet(\gamma \wedge \neg\gamma) \rightarrow (\bigcirc\bullet\alpha \leftrightarrow \bullet\bigcirc\alpha)$	(Commutativity for $\bullet$ and $\bigcirc$)
A$\mathtt{S}\bullet$.	$\alpha\mathtt{S}\beta \leftrightarrow [\beta \vee (\neg\bullet(\alpha \wedge \neg\alpha) \wedge [\alpha \wedge \bullet(\alpha\mathtt{S}\beta)])]$	
A$\mathtt{P}\bullet$.	$\mathtt{P}\bullet\beta$	

II) Temporal axioms and rules (2)

R○N. $\dfrac{\alpha}{\bigcirc\alpha}$ (Necessitation for ○)

R●N. $\dfrac{\alpha}{\bullet\alpha}$ (Necessitation for ●)

RU. $$\frac{\{\Phi_{k,\mathrm{B},\mathrm{x}}(\neg((\bigwedge_{l=0}^{i-1}\bigcirc^{l}\alpha)\wedge\bigcirc^{i}\beta))\ :\ i\in\mathbb{N}\}}{\Phi_{k,\mathrm{B},\mathrm{x}}(\neg(\alpha\mathrm{U}\beta))}$$

RS. $$\frac{\{\Phi_{k,\mathrm{B},\mathrm{x}}(\neg((\bigwedge_{l=0}^{i-1}\bullet^{l}\alpha)\wedge(\bigwedge_{l=0}^{i}\neg\bullet^{l}(\alpha\wedge\neg\alpha))\wedge\bullet^{i}\beta))\ :\ i\in\mathbb{N}\}}{\Phi_{k,\mathrm{B},\mathrm{x}}(\neg(\alpha\mathrm{S}\beta))}$$

III) Epistemic axioms and rules

AK→.	$\mathtt{K}_a(\alpha \to \beta) \to (\mathtt{K}_a\alpha \to \mathtt{K}_a\beta)$	(Distribution Axiom for $\mathtt{K}_a$)
AKR.	$A_a \to (\mathtt{K}_a\alpha \to \alpha)$	(Reflexivity for $\mathtt{K}_a$)
AKA.	$A_a \to \mathtt{K}_a A_a$	(Self awareness for $\mathtt{K}_a$)
AKDE.	$\neg A_a \to \mathtt{K}_a(\alpha \wedge \neg\alpha)$	(Dead end)
AKS.	$\mathtt{K}_a\neg\alpha \to \mathtt{K}_a\neg\mathtt{K}_a\alpha$	(Symmetry for $\mathtt{K}_a$)
AKT.	$\mathtt{K}_a\alpha \to \mathtt{K}_a\mathtt{K}_a\alpha$	(Transitivity for $\mathtt{K}_a$)
ACE.	$\mathtt{C}\alpha \to \mathtt{E}^m\alpha,\ m \in \mathbb{N}$	
R$\mathtt{K}_a$N.	$\dfrac{\alpha}{\mathtt{K}_a\alpha}$	(Knowledge Necessitation)
RC.	$\dfrac{\{\Phi_{k,\mathrm{B},\mathrm{X}}(\mathtt{E}^i\alpha)\ :\ i \in \mathbb{N}\}}{\Phi_{k,\mathrm{B},\mathrm{X}}(\mathtt{C}\alpha)}$	

IV) Probability axioms and rules (for runs)

AGP1.	$P_{\geqslant 0}\alpha$	
AGP2.	$P_{\leqslant r}\alpha \to P_{<t}\alpha,\ t > r$	
AGP3.	$P_{<t}\alpha \to P_{\leqslant t}\alpha$	
AGP4.	$(P_{\geqslant r}\alpha \wedge P_{\geqslant t}\beta \wedge P_{\geqslant 1}\neg(\alpha \wedge \beta)) \to P_{\geqslant \min(1, r+t)}(\alpha \vee \beta)$	
AGP5.	$(P_{\leqslant r}\alpha \wedge P_{<t}\alpha) \to P_{<r+t}(\alpha \vee \beta),\ r + t \leqslant 1$	
AGP●.	$P_{\geqslant 1}\bullet(\alpha \wedge \neg\alpha)$	
RGPN.	$\dfrac{\alpha}{P_{\geqslant 1}\alpha}$	(Probabilistic Necessitation)
RGA.	$\dfrac{\{\Phi_{k,B,X}(P_{\geqslant r - \frac{1}{i}}\alpha) \ :\ i \geqslant \frac{1}{r}\}}{\Phi_{k,B,X}(P_{\geqslant r}\alpha)},\ r \in (0,1]_{\mathbb{Q}}$	(Archimedean rule)

V) Probability axioms and rules (for points)

AP1. $P_{a,\geqslant 0}\alpha$

AP2. $P_{a,\leqslant r}\alpha \rightarrow P_{a,<t}\alpha,\ t > r$

AP3. $P_{a,<t}\alpha \rightarrow P_{a,\leqslant t}\alpha$

AP4. $(P_{a,\geqslant r}\alpha \wedge P_{a,\geqslant t}\beta \wedge P_{a,\geqslant 1}\neg(\alpha \wedge \beta)) \rightarrow P_{a,\geqslant \min(1,r+t)}(\alpha \vee \beta)$

AP5. $(P_{a,\leqslant r}\alpha \wedge P_{a,<t}\alpha) \rightarrow P_{a,<r+t}(\alpha \vee \beta),\ r + t \leqslant 1$

RPN. $\dfrac{\alpha}{P_{a,\geqslant 1}\alpha}$ (Probabilistic Necessitation)

RA. $\dfrac{\{\Phi_{k,\mathrm{B},\mathrm{X}}(P_{a,\geqslant r-\frac{1}{i}}\alpha) \mid i \geqslant \frac{1}{r}\}}{\Phi_{k,\mathrm{B},\mathrm{X}}(P_{a,\geqslant r}\alpha)},\ r \in (0,1]_{\mathbb{Q}}$ (Archimedean rule)

Infinitary rules: RU, RS, RC, RGA, RA

- RGA:

$$\frac{\{\Phi_{k,\mathrm{B},\mathrm{X}}(P_{\geqslant r-\frac{1}{i}}\alpha)\ :\ i \geqslant \frac{1}{r}\}}{\Phi_{k,\mathrm{B},\mathrm{X}}(P_{\geqslant r}\alpha)}$$

Infinitary rules: RU, RS, RC, RGA, RA

- RGA:

$$\frac{\{\Phi_{k,\mathrm{B},\mathrm{X}}(\mathrm{P}_{\geqslant r-\frac{1}{i}}\alpha)\ :\ i \geqslant \frac{1}{r}\}}{\Phi_{k,\mathrm{B},\mathrm{X}}(\mathrm{P}_{\geqslant r}\alpha)}$$

- RGA':

$$\frac{\{\mathrm{P}_{\geqslant r-\frac{1}{i}}\alpha\ :\ i \geqslant \frac{1}{r}\}}{\mathrm{P}_{\geqslant r}\alpha}$$

Infinitary rules: RU, RS, RC, RGA, RA

- RGA:

$$\frac{\{\Phi_{k,\mathrm{B},\mathrm{X}}(\mathrm{P}_{\geqslant r-\frac{1}{i}}\alpha) \ : \ i \geqslant \frac{1}{r}\}}{\Phi_{k,\mathrm{B},\mathrm{X}}(\mathrm{P}_{\geqslant r}\alpha)}$$

- RGA':

$$\frac{\{\mathrm{P}_{\geqslant r-\frac{1}{i}}\alpha \ : \ i \geqslant \frac{1}{r}\}}{\mathrm{P}_{\geqslant r}\alpha}$$

$$\begin{tikzcd}
P_{\geqslant r-\frac{1}{k}}\alpha \arrow[dr] & P_{\geqslant r-\frac{1}{k+1}}\alpha \arrow[d] & \dots & \dots \arrow[dl] \\
& P_{\geqslant r}\alpha & &
\end{tikzcd}$$

Proofs. Syntactic consequences

Definition

A formula α is a *theorem*, denoted by $\vdash \alpha$, if there are $\alpha_0, \alpha_1, \ldots, \alpha_{\lambda+1}$ (λ is a finite or countable ordinal):

- $\alpha_{\lambda+1} = \alpha$, and
- every α_i is an instance of some axiom schema or is obtained from the preceding formulas by an application of an inference rule.

A formula α is a *syntactic consequence* of T if there are $\alpha_0, \alpha_1, \ldots, \alpha_{\lambda+1}$:

- $\alpha_{\lambda+1} = \alpha$, and
- every α_i is an instance of some axiom schema or a formula from the set T, or it is obtained from the previous formulas by an application of an inference rule,with the exception that the **premises of R$\bigcirc$N, R$\bullet$N, R$\mathbb{K}_a$N, RGPN and RPN must be theorems**.

$\alpha_0, \alpha_1, \ldots, \alpha_{\lambda+1}$ is a *proof* for α (from the set T).

$$F = \{\neg P_{=0} p\} \cup \{P_{\leqslant 1/n} p : n \in \mathbb{N}\}$$

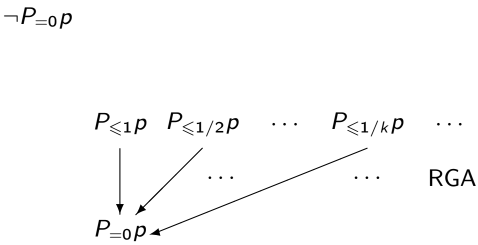
$$F = \{\neg P_{=0}p\} \cup \{P_{\leqslant 1/n}p : n \in \mathbb{N}\}$$

$\neg P_{=0}p$

1. $F \vdash \neg P_{=0}p$
2. $F \vdash P_{\leqslant 1/n}p,\ n \in \mathbb{N}$

$P_{\leqslant 1}p \quad P_{\leqslant 1/2}p \quad \cdots \quad P_{\leqslant 1/k}p \quad \cdots$

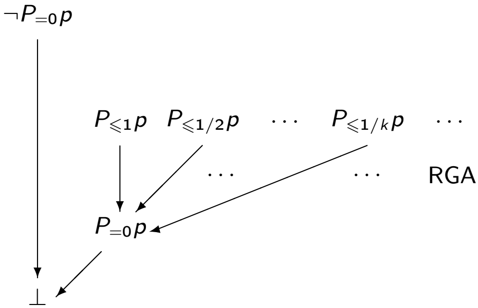
$$F = \{\neg P_{=0}p\} \cup \{P_{\leqslant 1/n}p : n \in \mathbb{N}\}$$



1. $F \vdash \neg P_{=0}p$
2. $F \vdash P_{\leqslant 1/n}p$, $n \in \mathbb{N}$
3. $F \vdash P_{\leqslant 0}p$, by Rule RGA
4. $F \vdash P_{=0}p$, from (4)

$$F = \{\neg P_{=0}p\} \cup \{P_{\leqslant 1/n}p : n \in \mathbb{N}\}$$

1. $F \vdash \neg P_{=0}p$
2. $F \vdash P_{\leqslant 1/n}p,\ n \in \mathbb{N}$
3. $F \vdash P_{\leqslant 0}p$, by Rule RGA
4. $F \vdash P_{=0}p$, from (4)
5. $F \vdash \perp$, from (1) and (4)



Strong completeness

- Deduction theorem

Strong completeness

- Deduction theorem
- Lindenbaum's theorem
- Strong necessitation: If $\mathsf{T} \vdash \gamma$, then
  - $\bigcirc\mathsf{T} \vdash \bigcirc\gamma$, $(\bigcirc\mathsf{T} = \{\bigcirc\alpha \ : \ \alpha \in \mathsf{T}\})$,
  - $\bullet\mathsf{T} \vdash \bullet\gamma$, and
  - $\mathtt{K}_a\mathsf{T} \vdash \mathtt{K}_a\gamma$, for every $a \in \mathsf{A}$.

Strong completeness

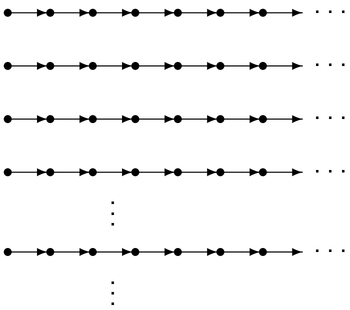
- Deduction theorem
- Lindenbaum's theorem
- Strong necessitation: If $\mathsf{T} \vdash \gamma$, then
  - $\bigcirc\mathsf{T} \vdash \bigcirc\gamma$, $(\bigcirc\mathsf{T} = \{\bigcirc\alpha \ : \ \alpha \in \mathsf{T}\})$,
  - $\bullet\mathsf{T} \vdash \bullet\gamma$, and
  - $\mathtt{K}_a\mathsf{T} \vdash \mathtt{K}_a\gamma$, for every $a \in \mathsf{A}$.
- The canonical model $\mathcal{M}^*$ is constructed using maximal consistent sets so that
  - A formula is satisfied in a point of the canonical model iff it belongs to the maximal consistent set of formulas which corresponds to the considered point, and
  - A set T of formulas is $\mathtt{Ax}_{\mathsf{PTEL}}$-consistent iff it is satisfiable.

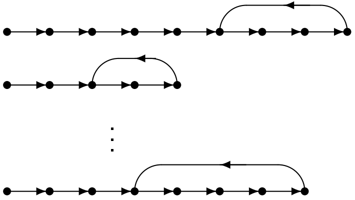
Odlučivost

- PTEL-zadovoljivost formula α se može redukovati na proveru zadovoljivosti u klasi konačno *predstavljivih* struktura.
- Veličina svake takve strukture je ograničena rekurzivnom funkcijom veličine formule α, pa se zadovoljivost α može proveriti u konačno mnogo koraka.

Odlučivost

- PTEL-zadovoljivost formula α se može redukovati na proveru zadovoljivosti u klasi konačno *predstavljivih* struktura.
- Veličina svake takve strukture je ograničena rekurzivnom funkcijom veličine formule α, pa se zadovoljivost α može proveriti u konačno mnogo koraka.





t-konzistentnost

t-konzistentnost:

- Za svaki $t \in \mathbb{N}$ u svakoj rundi izvršenja protokola

  sa visokom verovatnoćom (funkcijom od t) prefiksi lanca agenata (svi sem poslednjih t blokova) se poklapaju i zauvek ostaju u lancu.

Plan:

- U jeziku PTEL formulisati osnovne osobien protokola Blockchain (kao aksiome) i t-konzistentnost.
- Doakzati da u PTEL sa novim aksiomam formula za t-konzistentnost je teorema.

BlockChain-aksiome i pomoćne oznake

- $\mathrm{POW} \;:=\; \{\mathrm{pow}_a | a \in \mathbb{A}\}$, pow_a: a proizvodi PoW,
- $\mathrm{ACC} \;:=\; \{\mathrm{acc}_{a,b} | a, b \in \mathbb{A}\}$, $acc_{a,b}$: a prihvata PoW koji je proizveo b,
- $\mathrm{LDG} \;:=\; \{\mathrm{ldg}_{a,b,k} \;:\; a, b \in \mathbb{A}, k \in \mathbb{N}, k \geq 1\}$, $\mathrm{ldg}_{a,b,k}$: prvih k blokova u lancima a i b se poklapaju,
- $e_a \;:=\; \bigwedge_{b \in \mathbb{A}} (A_b \to \mathrm{acc}_{b,a})$, svaki aktivan agent prihvata PoW koji je proizveo a,
- $\mathrm{ech}_b \;:=\; \bigvee_{a \in \mathbb{A}} \mathrm{acc}_{b,a}$, b prihvata neki PoW,
- $(\mathrm{pow} = k) \;:=\; \bigvee_{\mathsf{X} \subset \mathbb{A}, |\mathsf{X}| = k} (\bigwedge_{a \in \mathsf{X}} \mathrm{pow}_a \wedge \bigwedge_{b \notin \mathsf{X}} \neg \mathrm{pow}_b)$, tačno k agenata proizvelo je PoW.

$\mathtt{Ax}_{\mathrm{BC}}$: BlockChain-aksiome (2)

AB1	$\bigvee_{a \in \mathbb{A}} \mathrm{pow}_a$	In each round at leats one agent produces proof-of-work.
AB2	$\mathrm{pow}_a \to A_a$	Only active agents can produce proofs-of-work.
AB3	$\mathrm{acc}_{b,a} \to \mathrm{pow}_a$	One can only accept proof-of-work that has been produced.
AB4	$\mathrm{acc}_{b,a} \to \neg \mathrm{acc}_{b,c}$, for each $c \neq a$	An agent accepts at most one proof-of-work for a given round.
AB5	$A_a \to \mathrm{ech}_a$	Each active agent must accept one of the produced proofs-of-work. Note that we do not have any assumption on how an agent accepts a proof.
AB6	$\mathrm{P}_{\leqslant 1-\varepsilon} \bigcirc^{i} (\mathrm{pow} > 1)$	The probability that more than one agent create proof-of-work for a round is bounded from above.

$\mathtt{Ax}_{\mathrm{BC}}$: BlockChain-aksiome (3)

AB7	$\bigwedge_{i\in Y} P_{\geqslant s_i}\bigcirc^i(\mathrm{pow}=k_i) \rightarrow P_{\geqslant s}\bigwedge_{i\in Y}\bigcirc^i(\mathrm{pow}=k_i)$ $s=\prod_{a\in X} s_a,\ k_i\in\{1,\dots,\lvert\mathbb{A}\rvert\}$	Necessary condition for independence of ($\mathrm{pow}=k$)'s in different rounds. (Y is a finite subset of $\mathbb{N}$)
AB8	$\bigwedge_{i\in Y} P_{\leqslant s_i}\bigcirc^i(\mathrm{pow}=k_i) \rightarrow P_{\leqslant s}\bigwedge_{i\in Y}\bigcirc^i(\mathrm{pow}=k_i)$ $s=\prod_{a\in X} s_a,\ k_i\in\{1,\dots,\lvert\mathbb{A}\rvert\}$	Necessary condition for independence of ($\mathrm{pow}=k$)'s in different rounds. (Y is a finite subset of $\mathbb{N}$)
AB9	$(\bullet^{n+1}\bot\wedge\neg\bullet^{n}\bot)\rightarrow \mathrm{ldg}_{a,a,k}$, $k\leqslant n+1$	Reflexivity for equality of ledgers.
AB10	$\mathrm{ldg}_{a,b,k}\rightarrow \mathrm{ldg}_{b,a,k}$	Symmetry for equality of ledgers.
AB11	$\mathrm{ldg}_{a,b,k}\wedge \mathrm{ldg}_{b,c,k}\rightarrow \mathrm{ldg}_{a,c,k}$	Transitivity for equality of ledgers.
AB12	$\mathrm{ldg}_{a,b,k}\rightarrow \mathrm{ldg}_{a,b,j}$, $j\leq k$	Soundness: equality of prefixes of equal ledgers.
AB13	$\bullet\bot\wedge\bigcirc^k \mathrm{acc}_{a,b}\rightarrow \mathrm{ldg}_{a,b,k+1}$	Accepting of a pow in the k-th round implies the acceptance of the corresponding ledger.
AB14	$\bullet\bot\ \wedge\ \bigcirc^k e_a\ \wedge\ \bigcirc^{k+j}A_b\ \rightarrow \mathrm{ldg}_{b,a,k+1}$	Persistence: once achieved consensus cannot be changed in the future.

Tvrdjenja o BlockChain-protokolu

Theorem

Skup T *formulas je* $\mathtt{Ax}_{\mathrm{BC}}$*-konzistentan akko je* $\mathtt{Mod}_{BC}$*-zadovoljiv.*

Tvrdjenja o BlockChain-protokolu

Theorem

Skup T *formulas je* $\mathtt{Ax}_{\mathrm{BC}}$*-konzistentan akko je* $\mathtt{Mod}_{BC}$*-zadovoljiv.*

Lemma

Sledeće važi:

- $\vdash_{\mathtt{Ax}_{\mathrm{BC}}} \bigvee_{b \in \mathbb{A}} A_b$
- $\vdash_{\mathtt{Ax}_{\mathrm{BC}}} e_a \to \neg e_c,\ a \neq c$
- *Ako svi aktivni agenti prihvate isti PoW u rundi* k*, tada će zauvek imati identičnih prvih* $k+1$ *blokova u svojim lancima.*

Tvrdjenja o BlockChain-protokolu (2)

Theorem

Neka je ε predefinisani prag verovatnoće i $z \in \mathbb{N}$ dužina lanca. Tada:

$$\vdash_{\mathtt{Ax}_{BC}} \mathtt{C}\ \mathtt{P}_{\geqslant 1-(1-\varepsilon)^{z+1}} \bigvee_{i=0}^{z} \bigcirc^{i} \bigvee_{a \in \mathbb{A}} e_a.$$

Z. Ognjanović, N. Krdžavac, *Uvod u teorijsko računarstvo* (glave 7 i 8), Beograd, 2004.

http://www.mi.sanu.ac.rs/~zorano/ti/2012/TeorijskoRacunarstvo.pdf