Sveučilište u Zagrebu
Prirodoslovno - matematički fakultet
Matematički odsjek

Modalna logika - seminar

Proširenje linearne temporalne logike operatorima prošlosti

Roberto Grabovac

Zagreb, rujan 2023.

Sadržaj

1 Uvod

Linearna temporalna logika (skraćeno: ***LTL***) je vrsta modalne, odnosno temporalne logike pogodne za izražavanje koncepta vremena. Naime, istinitost velike većine izjava ovisi o vremenskoj komponenti. Npr. izjava *"Svakog dana ću učiti"* nije univerzalno istinita ili lažna jer njezina (ne)istinitost nije ovisna samo o jednom stanju (danu), već o čitavom nizu stanja (dana) koji dolaze nakon te izjave. Upravo je glavno pitanje kako formalizirati vremensku komponentu, odnosno koji model vremena koristiti. U skladu s tim pitanjem, nastale su dvije vrste temporalne logike - linearna i granajuća. U linearnoj se polazi od tvrdnje da svaki trenutak u vremenu ima jedinstven trenutak koji iz njega slijedi u budućnosti (npr. deterministički programi), dok se u granajućoj smatra kako se svaki trenutak može razgranati u nekoliko alternativnih budućnosti (npr. nedeterministički programi). Sada se lako može zaključiti koje bi matematičke strukture bile pogodne za formalizaciju vremena u tim temporalnim logikama. Naravno, nizovi su prikladni za linearnu (npr. jedinstven ishod programa), a stabla (npr. nizovi mogućih ishoda programa) za granajuću temporalnu logiku. Kao što ćemo vidjeti u nastavku, LTL je proširenje propozicionalne logike ***temporalnim operatorima*** uz semantiku definiranu na ***linearnim modelima***, dok je granajuća temporalna logika pak proširenje LTL egzistencijalnim i univerzalnim kvantifikatorima. Tijekom 90ih godina prošlog stoljeća je fokus prvenstveno bio na granajuću temporalnu logiku, no on se vremenom sveo na linearnu jer je njezin jezik dovoljno intuitivan, praktičan i pogodan za formalnu verifikaciju za razliku od jezika granajuće temporalne logike. Upravo će jedan od ciljeva ovog rada biti taj da se prikaže koliko su sintaksa i semantika LTL intuitivne te se lako mogu formalizirati preko dosad dobro istraženih matematičkih struktura.

Primjer 1. *Temeljna ideja istinitosti izjava ovisnih o vremenskom konceptu (i modeliranje istog) lako je vidljiva iz primjera jednostavnog odsječka programa prikazanog na slici:*

```
while (x < 3) {
    print("hello");
    if (x == 1) print("hi");
    if (x == 2) x = 0;
            else x++;
}
```

Vidimo da je ponašanje programa određeno s vrijednosti varijable x pa je prirodno u ovisnosti o tome razlikovati stanja. Nadalje, zanima nas ponašanje

programa u tim stanjima pa je korisno definirati $p =$ *program ispisuje "hello",* $q =$ *program ispisuje "hi" te* $r = x$ *je paran broj. Pretpostavimo li da je inicijalna vrijednost varijable* x *jednaka 0, ponašanje programa modeliramo na sljedeći način:*

gdje npr. oznaka p, r *iznad prvog stanja po redu* $(x = 0)$ *znači da je* x *paran broj i da program ispisuje "hello". Oznake* p, q, r *će kasnije formalno biti definirane kao* ***propozicionalne varijable*** *(npr. svojstva programa u određenom stanju), a pojedino stanje i oznake nad njim (ako postoje) bit će zapravo elementi slike* ***funkcije označavanja****. Ako želimo opisati ponašanje programa (općenito: sigurnost, životnost, ispravnost...), to iziskuje promatranje* ***istinitosti formula*** *na pripadnom linearnom modelu koje izražavaju ono što nas u vezi programa zanima. Lako možemo vidjeti da vrijede sljedeće tvrdnje:* p *je* ***uvijek*** *istina; uvijek* p *povlači* $(q$ *ili* $r)$*;* ***nikad*** *ne vrijedi* $(q$ *i* $r)$*; uvijek će* ***nakon nekog vremena*** q *biti istina. Podebljane sintagme u prethodnim primjerima bit će semantička značenja* ***temporalnih operatora*** *u LTL.*

Navedeni primjer predstavlja zanimljivu analizu jednog jednostavnog programa, a za čitatelje koji pak žele znati nešto više o formalnoj verifikaciji znatno složenijih i važnijih programa, preporuka je pogledati drugo poglavlje u [6]. Specifičnost LTL-a ogleda se u tome da je za poznavanje budućnosti dovoljno znati informacije o trenutnom stanju. No, jasno je da iduće stanje nije nužno jednoznačno određeno samo trenutnim, već i stanjima koja su mu prethodila. Zbog toga se LTL proširuje operatorima prošlosti (eng. *past*) te tako dobivenu logiku označavamo s ***LTL+PAST***. Ipak, pokazuje se da su te dvije logike jednako ***ekspresivne*** (izražajne) pa se koncept prošlosti opravdano i zanemaruje. Naime, prilikom opisivanja ***tranzicijskih sustava*** nas ne zanima vrijedi li neko ponašanje (opisano formulom) u nekom od prethodnih stanja, već samo u budućima (ili trenutnom). Drugim riječima, zanima nas kako će se sustav ponašati, a ne kako se ponašao. Međutim, zanimljiv je fenomen koji proizlazi iz dokaza ekspresivnosti tih dviju logika. Naime, ispostavlja se da je LTL+PAST ***sažetija*** od LTL i to eksponencijalnog reda veličine. Intuitivno obrazloženje toga jest da postoje formule u LTL+PAST čija je ***veličina*** eksponencijalno manja od veličine njima ***ekvivalentnih formula*** u LTL. Upravo će dokaz te činjenice biti glavni cilj ovog rada u kojem će se, između ostalog, precizno definirati svi podebljani pojmovi koji su

s razlogom spomenuti i dodatno naglašeni u ovom uvodnom poglavlju kako bi se motivirala potreba za njihovim uvođenjem.

2 Sintaksa i semantika

Sintaksu i semantiku linearne temporalne logike dobivenu proširenjem operatorima prošlosti razradit ćemo u tri potpoglavlja. Prvo potpoglavlje bavi se posebnom vrstom modela - tranzicijski sustav s korijenom. Takvi modeli se upravo promatraju u LTL zbog čega je i nastala ta posebna vrsta temporalne logike čije su karakteristike glavni rezultat ovog seminara. U drugom potpoglavlju konačno precizno definiramo sintaksu i semantiku linearne temporalne logike, dok ju u trećem proširujemo operatorima prošlosti. Četvrto potpoglavlje predstavlja dodatno proširenje sintakse pojmom zatvarača formule i jednim semantičkim rezultatom potrebnim za dokaz sažetosti LTL+PAST nad LTL, a peto se bavi povezivanjem intuicije i semantičkog značenja svih temporalnih operatora.

2.1 Tranzicijski sustav s korijenom

Prije formalne definicije tranzicijskog sustava s korijenom, potrebno je navesti intuitivno objašnjenje za uočavanje i potrebu svih pojmova koji ga definiraju.
Općenito, tranzicijski sustav predstavlja jednostavan, a opet izuzetno koristan formalizam u računalnoj znanosti. Svaki takav sustav sastoji se od niza konfiguracija (stanja) i skupa (relacije) prijelaza (akcije) koji zajedno opisuju dinamički proces. Primjerice, možemo promotriti igru šah - konfiguracije predstavljaju trenutno stanje igre (pozicije figura, igrač na potezu, vrijeme preostalo za izvršavanje poteza...), dok bi prijelazi između konfiguracija (akcije) bili dopustivi potezi igrača. Idući primjer je samo računalo koje sadrži složen mehanizam za stvaranje i ažuriranje sadržaja registara (konfiguracije/stanja) u skladu s instrukcijama koje su u njega ugrađene (prijelazi/akcije). Povezivanjem navedenog s matematičkom logikom, zaključujemo da trenutno stanje (konfiguraciju) mogu opisivati propozicionalne varijable. Matematički, tranzicijski sustavi mogu se shvatiti kao usmjereni grafovi koji opisuju potencijalno ponašanje nekog diskretnog sustava. Vrhovi predstavljaju stanja, a bridovi prijelaze između njih. Nadalje, postavlja se pitanje zašto je potrebno formalizirati neki proces. Odgovor je jednostavan - formaliziranje omogućava njegovu analizu kojom je moguće utvrditi svojstva koja ga karakteriziraju ili pak predvidjeti potencijalno ponašanje. Dva svojstva od najvećeg interesa su sigurnost i aktivnost sustava. Prvo svojstvo

se koristi kako bi se izrazilo da se u procesu ne može dogoditi ništa loše, odnosno nije moguće doći u neželjeno stanje. Drugo pak svojstvo osigurava da se u procesu ipak nešto i događa, odnosno da aktivno radi. Istaknimo da smo dosad intuitivno objasnili općeniti tranzicijski sustav, dok je njegova varijanta s korijenom specifična samo po tome što je jedno stanje istaknuto kao početno, korijensko.

Definicija 1. ***Tranzicijski sustav s korijenom*** *je uređena šestorka*

$$\mathcal{T} = (S, Act, \rightarrow, AP, L, s)$$

gdje je

- S *neprazan skup čije elemente nazivamo* ***stanja****,*
- Act *skup čije elemente nazivamo* ***akcije****,*
- $\rightarrow$ *podskup od* $S \times Act \times S$ *te ga nazivamo* ***relacija tranzicije****,*
- AP *skup* ***propozicionalnih varijabli****,*
- $L : S \rightarrow \mathcal{P}(AP)$ *je funkcija koju nazivamo* ***funkcija označavanja****,*
- s *je istaknuto početno,* ***korijensko stanje****.*

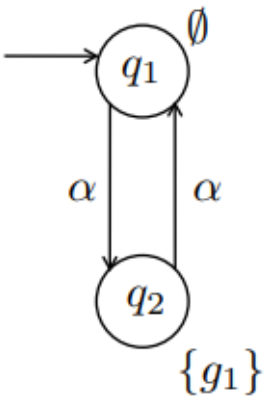
Primjer 2. *Pretpostavimo da imamo pojednostavljen model semafora u kojem nas jedino zanima je li trenutno svjetlo zeleno ili nije. Definiramo pripadni tranzicijski sustav s korijenom:*

$$\mathcal{T}_{TL} = (S_{TL}, Act_{TL}, \rightarrow_{TL}, AP_{TL}, L_{TL}, s_{TL})$$

gdje

- $S_{TL} = \{q_1, q_2\}$,
- $Act_{TL} = \{\alpha\}$,
- $\rightarrow_{TL} = \{(q_1, \alpha, q_2), (q_2, \alpha, q_1)\}$,
- $AP_{TL} = \{q_1\}$,
- $L_{TL}(q_1) = \emptyset$ *i* $L_{TL}(q_2) = \{q_1\}$,
- $s_{TL} = \{q_1\}$.

Oznaka $L_{TL}(q_1) = \emptyset$ *interpretira se tako da ako je sustav u stanju* q_1*, onda svjetlo nije zeleno. S druge strane,* $L_{TL}(q_2) = \{q_1\}$ *znači da je svjetlo zeleno ako je sustav u stanju* q_2*.*



Slika 1: Reprezentacija sustava $\mathcal{T}_{TL}$ usmjerenim grafom

Primjer 3. *Promotrimo logički dinamički sustav s varijablom stanja x, ulazom u i izlazom y:*

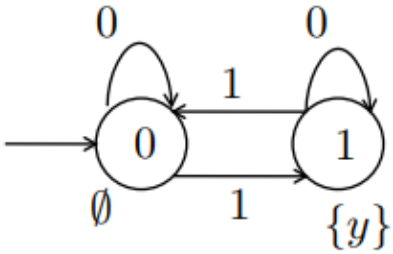
$$\begin{aligned} x[k+1] &= x[k] \oplus u[k], \\ y[k] &= x[k], \\ x[0] &= 0, \end{aligned}$$

gdje $x[k], y[k] \in \{0,1\}$ za sve $k \geq 0$, a $\oplus$ predstavlja XOR operator. Definiramo ovaj dinamički sustav kao tranzitivni s korijenom na sljedeći način:

$$\mathcal{T}_{LOG} = (S_{LOG}, Act_{LOG}, \rightarrow_{LOG}, AP_{LOG}, L_{LOG}, s_{LOG})$$

gdje

- $S_{LOG} = \{0,1\}$ *predstavlja skup stanja varijable x,*
- $Act_{LOG} = \{0,1\}$ *predstavlja vrijednosti ulaza u,*
- $(a,b,c) \in \rightarrow_{LOG}$ *ako i samo ako $c = a \oplus b$,*
- $AP_{LOG} = \{y\}$, *dok je pripadni partitivni skup dan s $\mathcal{P}(AP_{LOG}) = \{\emptyset, \{y\}\}$,*
- $L_{LOG}(0) = \emptyset, L_{LOG}(1) = \{y\}$ *što se redom interpretira kao $y = 0$, odnosno $y = 1$*
- $s_{LOG} = \{0\}$ *što odgovara činjenici da $x[0] = 0$.*



Slika 2: Reprezentacija sustava $\mathcal{T}_{LOG}$ usmjerenim grafom

2.2 LTL

Proučavanje bilo koje grane logike iziskuje definiranje njezinog jezika koji počiva na **alfabetu** - nepraznom skupu znakova. Konačni nizovi znakova alfabeta čine elemente jezika - **riječi**.

Definicija 2. ***Alfabet linearne temporalne*** *logike unija je skupova* A_1, A_2, A_3, A_4 *i* A_5 *pri čemu je:*

$A_1 = \{p_0, p_1, p_2...\}$ *prebrojiv skup čije elemente nazivamo* ***propozicionalnim varijablama***

$A_2 = \{\bot\}$ *logička konstanta* ***laž***

$A_3 = \{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$ *skup* ***logičkih veznika***

$A_4 = \{X, F, G, U\}$ *skup* ***temporalnih operatora***

$A_5 = \{(,)\}$ *skup pomoćnih simbola -* ***zagrade***

Sada možemo definirati pojam LTL-formule koji se definira na isti način kao i formule u propozicionalnoj logici, ali s dodatkom gore uvedenih temporalnih operatora.

Definicija 3. ***Atomarna LTL-formula*** *je svaka propozicionalna varijabla i logička konstanta* $\bot$*. Pojam* ***LTL-formule*** *definiramo rekurzivno na sljedeći način:*

1. *svaka atomarna LTL-formula je LTL-formula;*
2. *ako su* ϕ *i* ψ *LTL-formule, tada su LTL-formule i sljedeće riječi:* $(\neg\phi)$, $(\phi \wedge \psi), (\phi \vee \psi), (\phi \rightarrow \psi), (\phi \leftrightarrow \psi)$
3. *ako su* ϕ *i* ψ *LTL-formule, tada su LTL-formule i sljedeće riječi:* $(X\phi), (F\phi), (G\phi), (\phi U \psi)$*;*

4. *riječ alfabeta je LTL-formula ako je nastala primjenom konačno mnogo koraka 1., 2. i 3.*

Napomena 1. *Kako bismo osigurali preglednost prilikom pisanja LTL-formula, ponekad ćemo ispuštati zagrade kada nisu potrebne jer možemo koristiti prioritete logičkih veznika i temporalnih operatora. Unarni operatori imaju veći prioritet nad binarnima, dok su prioriteti binarnih veznika/operatora poredani uzlazno u sljedećem nizu:* $\leftrightarrow, \rightarrow, \wedge, \vee, U$.

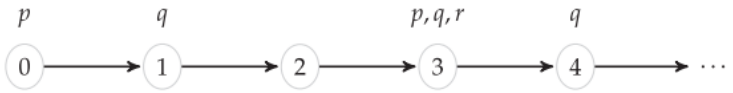
Primjer 4. *Ovdje navodimo nekoliko primjera formula te pri tome ističemo da one zasad nemaju nikakvo značenje jer nismo definirali semantiku. Primjeri:*

$$G(p_1), GFp_1 \rightarrow GFp_2, G(p_1 \rightarrow (\neg p_2 U p_3)), (p_1 \wedge p_2) \rightarrow F(p_3 \wedge p_2).$$

Za pridavanje potencijalnog značenja gornjim formulama u kontekstu računalne znanosti, pogledati 2.5.

Nakon definirane sintakse, dolazi potreba za semantikom. Prvo je potrebno definirati modele u LTL, a nakon toga relaciju istinitosti i istinitost formule na modelu. U nastavku slijedi definicija linearnog modela - posebnog slučaja tranzicijskog sustava s korijenom detaljno obrazloženog u prethodnom potpoglavlju.

Definicija 4. ***Linearni model*** *za LTL je svaki niz* $\sigma : \mathbb{N} \rightarrow \mathcal{P}(PROP)$. *Vrijednosti* $\sigma(j)$ *niza kratko ćemo nazivati* ***svojstvima*** *stanja* j.



Slika 3: Prefiks, odnosno restrikcija nekog linearnog modela na prvih 5 elemenata. Uočavamo da vrijedi: $\sigma(0) = \{p\}$, $\sigma(1) = \sigma(4) = \{q\}$, $\sigma(2) = \emptyset$ i $\sigma(3) = \{p, q, r\}$.

Napomena 2. *Uočimo zašto je linearni model specijalni slučaj tranzicijskog sustava s korijenom: vidimo da su imena akcija izostavljena, odnosno* $Act = \emptyset$, *a onda vrijedi da je* $\rightarrow$ *binarna relacija na* $S = \mathbb{N}$.

Definicija 5. *Neka su dani linearni model σ, pozicija $i \in \mathbb{N}$ i formule ϕ, ψ. Definiramo* ***relaciju istinitosti*** $\vDash$ *rekurzivno na sljedeći način:*

$\sigma, i \nvDash \bot$,

$\sigma, i \vDash p$ *akko* $p \in \sigma(i)$, *gdje je* p *propozicionalna varijabla,*

$\sigma, i \vDash \neg\phi$ *akko* $\sigma, i \nvDash \phi$,

$\sigma, i \vDash \phi \wedge \psi$ *akko* $\sigma, i \vDash \phi$ *i* $\sigma, i \vDash \psi$,

$\sigma, i \vDash \phi \vee \psi$ *akko* $\sigma, i \vDash \phi$ *ili* $\sigma, i \vDash \psi$,

$\sigma, i \vDash \phi \rightarrow \psi$ *akko* $\sigma, i \nvDash \phi$ *ili* $\sigma, i \vDash \psi$,

$\sigma, i \vDash \phi \leftrightarrow \psi$ *akko* $(\sigma, i \vDash \phi$ *i* $\sigma, i \vDash \psi)$ *ili* $(\sigma, i \nvDash \phi$ *i* $\sigma, i \nvDash \psi)$,

$\sigma, i \vDash X\phi$ *akko* $\sigma, i+1 \vDash \phi$,

$\sigma, i \vDash F\phi$ *akko postoji* $j \geq i$ *takav da* $\sigma, j \vDash \phi$,

$\sigma, i \vDash G\phi$ *akko za svaki* $j \geq i$ *vrijedi* $\sigma, j \vDash \phi$,

$\sigma, i \vDash \phi U \psi$ *akko postoji* $j \geq i$ *takav da* $\sigma, j \vDash \psi$ *i* $\sigma, k \vDash \phi$ *za sve* $k \in \mathbb{N}$ *takve da* $i \leq k < j$.

Definicija 6. *Kažemo da je formula ϕ* ***istinita na linearnom modelu*** *σ (oznaka: $\sigma \vDash \phi$) ako vrijedi $\sigma, 0 \vDash \phi$.*

Sada navodimo lemu koja će nam biti korisna u nastavku, a čiji se dokaz može pronaći u [5].

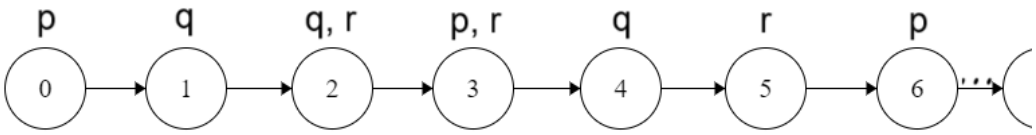
Napomena 3. *Neka je σ linearni model te $i, j \geq 0$. Za potrebe iskaza spomenute leme, uvodimo oznaku $\sigma[i, +\infty)$: linearni model dobiven iz σ odbacivanjem prvih i elemenata domene. Slično, $\sigma \backslash [i, j]$ predstavlja linearni model dobiven iz σ izbacivanjem podniza $\sigma(i), ..., \sigma(j)$.*

Lema 1. *Za svaku formulu ϕ i svaki linearni model σ te $i \in \mathbb{N}$ vrijedi sljedeća ekvivalencija:*

$$\sigma, i \vDash \phi \iff \sigma[i, +\infty) \vDash \phi.$$

Primjer 5. *Neka je linearni model σ definiran na sljedeći način: za svaki $k \in \mathbb{N}$,*

- $p \in \sigma(k)$ *akko* $k = 3l, l \in \mathbb{N}$,
- $q \in \sigma(k)$ *akko* $k = 2^l, l \in \mathbb{N}$,



Slika 4: Prvih 6 elemenata linearnog modela

- $r \in \sigma(k)$ *akko je* k *prost broj.*

Na opisanom linearnom modelu lako zaključujemo da vrijedi:

- $\sigma, 0 \vDash p \wedge XX\neg p$. *Zbog* $\sigma(0) = \{p\}$ *slijedi* $\sigma, 0 \nvDash q$ *i* $\sigma, 0 \nvDash r$*;*
- $\sigma, 1 \vDash F((q \wedge r) \vee \neg r)$ *te očito* $\sigma, 1 \nvDash Gr$*;*
- $\sigma, 4 \vDash (q \vee r)Up$ *gdje za* j *iz definicije 5 vrijedi* $j = 6$.

Kao što je već navedeno, glavni cilj ovog rada bit će dokazati sažetost LTL+PAST nad LTL u odnosu na veličinu formula pa je potrebno definirati i taj pojam.

Definicija 7. ***Veličina*** *formule* ϕ *(oznaka:* $|\phi|$*) je ukupan broj propozicionalnih varijabli, logičkih konstanti i veznika te temporalnih operatora i zagrada formule* ϕ*.*

2.3 LTL + PAST

Linearna temporalna logika (LTL) sadrži temporalne operatore koji se referiraju samo na budućnost. Proširenje LTL postiže se dodavanjem dualnih temporalnih operatora prošlosti. Godine 1980. izraelski logičar Dov M. Gabbay dokazao je da proširenje operatorima prošlosti ne povećava ekspresivnost LTL (objavljeno u [3]). Uz to, osmislio je i algoritam koji translatira LTL+PAST-formulu u njoj ekvivalentnu LTL-formulu. Pretvorba se odvija u nekoliko faza i pokazuje se da svaka od njih povećava formulu za najmanje eksponencijalni red veličine. Takav fenomen je u logici poznat pod nazivom **sažetost**, a njegovo intuitivno obrazloženje jest da postoje formule koje se mogu izraziti u dosta kraćoj formi u jednoj logici (ovdje: LTL+PAST), nego u drugoj (ovdje: LTL). Sve navedeno bit će puno preciznije obrađeno u poglavlju 3 koje ujedno predstavlja glavni cilj ovog seminara.
Sada je potrebno definirati gore spomenute temporalne operatore prošlosti i pojam LTL+PAST-formule, odnosno sintaksu, a potom i semantiku od LTL+PAST. No, ta je logika samo proširenje LTL pa se njezina sintaksa i

semantika dobivaju samo proširivanjem već viđenih definicija u potpoglavlju 2.2.

Definicija 8. ***Alfabet*** *LTL+PAST jednak je alfabetu LTL iz definicije 2 uz proširenje skupa A_4 dvama novim temporalnim operatorima Y i S, odnosno $A_4 = \{X, F, G, U, Y, S\}$.*

Definicija 9. ***Atomarna LTL+PAST formula*** *jednaka je pojmu atomarne LTL-formule, dok se rekurzivni dio definicije 3 proširuje sljedećim:*

- *ako su ϕ i ψ LTL+PAST-formule, tada su LTL+PAST-formule i sljedeće riječi: $(Y\phi), (\phi S\psi)$.*

Definicija 10. ***Relacija istinitosti*** $\vDash$ *promatra se i dalje nad linearnim modelima, a definicija 5 proširuje semantikom uvedenih temporalnih operatora prošlosti:*

- $\sigma, i \vDash Y\phi$ *akko* $\sigma, i-1 \vDash \phi$ *te* $i > 0$,
- $\sigma, i \vDash \psi S\phi$ *akko postoji* $j \in \mathbb{N}$ *takav da* $0 \leq j \leq i$ *te vrijedi* $\sigma, j \vDash \phi$ *i* $\sigma, k \vDash \psi$ *za sve* $j < k \leq i$.

Istinitost *LTL+PAST-formule definirana je identično kao istinitost LTL-formule iz definicije 6.*

Sada uvodimo novi pojam *inicijalno ekvivalentnih* formula koji daje prvu razliku između LTL i njezinog upravo definiranog proširenja. Ipak, prije toga je potrebno definirati logičku ekvivalentnost (općenitih) formula.

Definicija 11. *Dvije formule ϕ i ψ su* ***logički ekvivalentne*** *(oznaka: $\phi \equiv \psi$) ako za svaki model σ te svako stanje i tog modela vrijedi:*

$$\sigma, i \vDash \phi \iff \sigma, i \vDash \psi.$$

Definicija 12. *Neka su ϕ i ψ dvije LTL+PAST-formule. Kažemo da su ϕ i ψ* ***inicijalno ekvivalentne*** *(oznaka: $\phi \equiv_0 \psi$) ako za sve linearne modele σ vrijedi:*

$$\sigma, 0 \vDash \phi \iff \sigma, 0 \vDash \psi.$$

Sljedeća lema pokazuje da inicijalna ekvivalentnost nije od pretjeranog značaja za LTL, ali jest za LTL+PAST.

Lema 2.

1. *Za sve LTL-formule ϕ i ψ vrijedi: $\phi \equiv_0 \psi$ akko $\phi \equiv \psi$.*

2. *Postoje LTL+PAST-formule ϕ i ψ takve da $\phi \equiv_0 \psi$, ali ne vrijedi $\phi \equiv \psi$.*

Dokaz. (1) Neka su ϕ i ψ proizvoljne LTL-formule. Ako $\phi \equiv \psi$, onda očito $\phi \equiv_0 \psi$. Dokažimo sada obratni smjer. Pretpostavimo suprotno, tj. da vrijedi $\phi \equiv_0 \psi$ te da postoji model σ i stanje j takvo da $\sigma, j \vDash \phi$ i $\sigma, j \nvDash \psi$. Definiramo restrikciju linearnog modela σ sa $\sigma' = \sigma[j, +\infty)$. Iz $\sigma, j \nvDash \psi$ po lemi 1 slijedi $\sigma' \nvDash \psi$. Analogno, iz $\sigma, j \vDash \phi$ zaključujemo da $\sigma' \vDash \phi$. Kako su ϕ i ψ inicijalno ekvivalentne, vrijedi $\sigma', 0 \vDash \phi$ i $\sigma', 0 \vDash \psi$, a iz toga posebno $\sigma' \vDash \psi$ čime smo došli do kontradikcije.
(2) Definiramo $\phi = p_0 S p_1$ te $\psi = p_1$ gdje su p_0 i p_1 propozicionalne varijable. Očito $\phi \equiv_0 \psi$. Naime, ako je σ proizvoljan linearan model, onda iz $\sigma, 0 \vDash \phi$ i definicije istinitosti temporalnog operatora S nužno slijedi $\sigma, 0 \vDash p_1$, odnosno $\sigma, 0 \vDash \psi$. Obratno, ako $\sigma, 0 \vDash \psi$, onda ponovno iz definicije istinitosti slijedi $\sigma, 0 \vDash \phi$ zato što $i = j = 0$ pa uopće ne postoji k takav da $j < k \leq i$ nakon kojeg bi trebalo vrijediti $\sigma, k \vDash p_0$. No, definiramo li linearni model σ' takav da $\sigma'(0) = \{p_1\}$, $\sigma'(1) = \{p_0\}$ te $\sigma'(j) = \{\neg p_1\}$ za sve $j \in \mathbb{N}\backslash\{0\}$, onda vidimo da $\sigma', 1 \vDash \phi$, ali ne vrijedi $\sigma', 1 \vDash \psi$.

2.4 Zatvarač formule

Ideja zatvarača formule ϕ jest u tome da on predstavlja skup formula koje se koriste za provjeru istinitosti ili valjanosti formule ϕ. Takav skup je obično konačan i samo se formule iz njega mogu pojaviti u toj proceduri (algoritmu). Točna definicija zatvarača većinom ovisi o konkretnoj metodi za provjeru istinitosti/valjanosti, a u nastavku je dana najčešća verzija.

Definicija 13. ***Zatvarač formule*** *ϕ je skup (oznaka: $cl(\phi)$) koji sadrži sve potformule ψ od ϕ i njihove negacije $\neg\psi$ unutar kojeg poistovjećujemo ψ i $\neg\neg\psi$.*

Uočimo da naziv "zatvarač" za takav skup doista ima smisla jer su zadovoljena tri fundamentalna svojstva operatora zatvorenja:

1. $\phi \in cl(\phi)$,

2. $\Gamma \subseteq \Gamma' \implies cl(\Gamma) \subseteq cl(\Gamma')$,

3. $cl(cl(\Gamma)) = cl(\Gamma)$.

Napomena 4. *Za dani linearni model σ i formulu ϕ koristit ćemo oznaku $cl(\phi, \sigma, i)$ za skup svih formula iz $cl(\phi)$ koje su istinite na stanju i modela σ. Preciznije:*

$$cl(\phi, \sigma, i) := \{\psi \in cl(\phi) \mid \sigma, i \vDash \psi\}.$$

Pojam zatvarača formule je veoma bitan zbog sljedeće leme koja se koristi u dokazu sažetosti LTL+PAST nad LTL. Ukratko: ako uklonimo podniz između dvije pozicije u modelu na kojima su istiniti isti podskupovi iz $cl(\phi)$, onda se ne mijenja istinitost formula iz $cl(\phi)$ na preostalom dijelu modela. Dokaz se provodi indukcijom po formulama u $cl(\phi)$, a kako je vrlo sličan dokazu leme 1, ovdje ga izostavljamo.

Lema 3. *Neka je σ linearni model, ϕ LTL-formula, a i, j pozicije takve da $i < j$ te $cl(\phi, \sigma, i) = cl(\phi, \sigma, j)$. Dodatno definiramo $\sigma' := \sigma \backslash [i, j-1]$. Tada vrijedi:*

(I) $cl(\phi, \sigma', k) = cl(\phi, \sigma, k),\ \forall k \in [0, i-1]$.

(II) $cl(\phi, \sigma', k) = cl(\phi, \sigma, k + (j-i)),\ \forall k \geq i$.

2.5 Temporalni operatori - intuicija

Vidjeli smo da su LTL i njezino proširenje operatorima prošlosti zapravo ekstenzija propozicionalne logike temporalnim operatorima čija je semantika navedena u definiciji 5. Ipak, veoma je bitno razumjeti intuiciju oko tako definirane semantike te uvidjeti njihovu korist u primjeni. Stoga je u nastavku svaki takav operator detaljno obrazložen uz primjere i slike kojima će biti lakše shvatiti njihovo značenje.

- X: dolazi od engleskih riječi *"next time"*. Ako ϕ iskazuje svojstvo nekog sustava u trenutnom stanju, onda $X\phi$ znači da će i iduće stanje zadovoljavati ϕ. Koristan primjer formule je:

  $$upozorenje \rightarrow X zaustavljanje$$

  koja izražava da ako se u trenutnom stanju nekog sustava dogodi upozorenje, onda će se u sljedećem stanju sustav zaustaviti. Ponekad se koristi pokrata:

  $$X^n\phi = \underbrace{(X...X)}_{\text{n puta}}\phi.$$

  Uz gornju oznaku, činjenicu da je neko svojstvo ϕ istinito u trenutnom stanju i ostat će istinito u idućih n stanja izražavamo sljedećom formulom:

  $$\phi \wedge X\phi \wedge X^2\phi \wedge ... \wedge X^n\phi.$$

Slika 5: $\sigma, 0 \vDash X\varphi$

- F: dolazi od engleske riječi *"future"*, a $F\phi$ označava da će formula ϕ biti istinita u trenutnom ili nekom budućem stanju bez specificiranja tog stanja. Formula

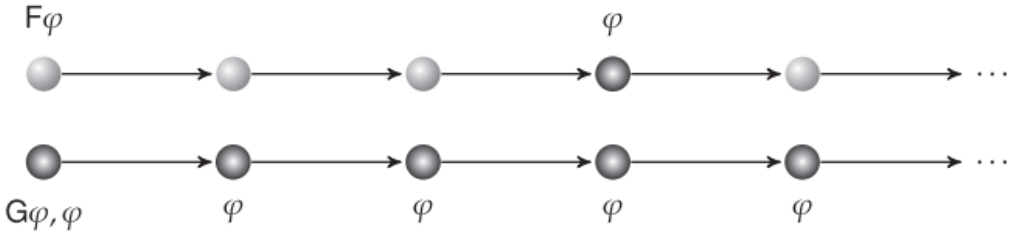
$$upozorenje \rightarrow Fzaustavljanje \tag{1}$$

  također predstavlja ponašanje nekih sustava: kada se dogodi upozorenje, sustav će se sigurno zaustaviti u nekom stanju koje mu slijedi, ali ne nužno u sljedećem kao kod operatora X.

- G: dolazi od engleske riječi *"globally"*, a predstavlja *"jaču"* varijantu operatora F: formula $G\phi$ znači da je ϕ istinita na trenutnom i svim stanjima nadalje. Primjerice,

$$G(upozorenje \rightarrow FXzaustavljanje)$$

  osigurava još veću sigurnost jer se njome postiže to da će sustav **uvijek** sadržavati stanje u kojem se zaustavlja nakon što se dogodilo upozorenje. Zanimljivo je uočiti dualnost operatora G i F: koje god svojstvo formula ϕ izražavala tako da je uvijek istinita, onda $\neg\phi$ nikad neće biti istinita, i obratno. Zbog toga formule $G\phi$ i $\neg F\neg\phi$ imaju ekvivalentno značenje.



Slika 6: $\sigma, 0 \vDash F\varphi$ i $\sigma, 0 \vDash G\varphi$; usporedba temporalnih operatora F i G

- U: dolazi od engleske riječi *"until"* te na još ekspresivniji način izražava budućnost od dosadašnjih operatora jer uključuje dvije formule. Intuitivno, formule $\phi U \psi$ znači da je ϕ istinita sve do stanja u kojem ψ postaje istinita. Sada prethodni primjer formule 1 može izražavati još realnije stanje sustava:

$$G(upozorenje \rightarrow (alarm U zaustavljanje)),$$

tj. svaki put će se nakon upozorenja upaliti alarm te se on neće ugasiti sve dok se sustav ne zaustavi. Drugi primjer bilo bi slanje poruke koja neće biti označena kao poslana sve dok ne stigne potvrda da je primljena:

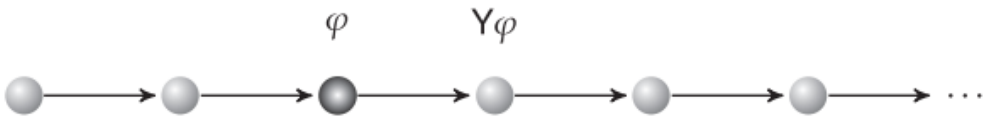
$$G(slanje \rightarrow \neg poslana U primljena).$$

Slika 7: $\sigma, 0 \vDash \varphi U \psi$

- Y: dolazi od engleske riječi *"yesterday"*, a njegovo je značenje analogno operatoru X: formula $Y\phi$ označava da je na prethodnom stanju ϕ bila istinita, a ako prethodnog stanja nema, onda je $Y\phi$ lažna. Primjer

$$zaustavljanje \rightarrow Y upozorenje$$

opisuje ishod nekog sustava, odnosno njegovom zaustavljanju prethodilo je upozorenje.

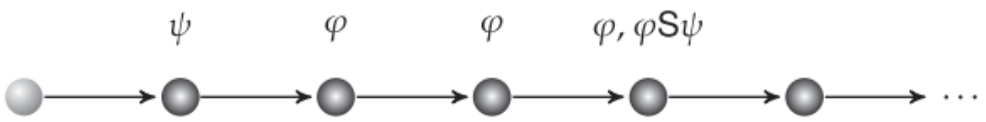


Slika 8: $\sigma, 3 \vDash Y\varphi$

- S: dolazi od engleske riječi *"since"*. Značenje formule $\phi S \psi$ je sljedeće: ψ je istinita na nekom od prethodnih stanja ili trenutnom, a od tog stanja

je onda istinita formula ϕ. Sada činjenicu da prije svakog odobrenja mora uslijediti zahtjev izražavamo sljedećom formulom:

$$G(odobrenje \rightarrow Y(\neg odobrenje S zahtjev)).$$



Slika 9: $\sigma, 4 \vDash \varphi S \psi$

3 Sažetost LTL+PAST

Težnja predviđanja budućnosti ne samo na osnovu trenutnog, već i na osnovu nekih prethodnih stanja modela potaknula je proširivanje linearne temporalne logike operatorima prošlosti. Naveli smo da se time ipak ne dobiva na *ekspresivnosti*, ali se pojedine klase formula mogu znatno kraće zapisati (eksponencijalnog reda veličine) korištenjem dodanih operatora čime LTL+PAST postaje *sažetija* logika nego LTL. Spominjemo pojmove ekspresivnosti i sažetosti logika koji su intuitivno jasni, ali unatoč tome, potrebno ih je precizno definirati.

Definicija 14. *Neka su $\mathcal{L}_1$ i $\mathcal{L}_2$ logike čija je semantika definirana nad tranzicijskim sustavom s korijenom. Kažemo da je logika $\mathcal{L}_1$* ***ekspresivnija*** *od logike $\mathcal{L}_2$ (oznaka: $\mathcal{L}_2 \sqsubseteq \mathcal{L}_1$) ako za svaku formulu ϕ u $\mathcal{L}_2$ vrijedi da postoji formula ϕ' u $\mathcal{L}_1$ takva da $\phi \equiv \phi'$. Kažemo da je logika $\mathcal{L}_1$* ***strogo ekspresivnija*** *od logike $\mathcal{L}_2$ (oznaka: $\mathcal{L}_2 \sqsubset \mathcal{L}_1$) ako vrijedi $\mathcal{L}_2 \sqsubseteq \mathcal{L}_1$ i $\mathcal{L}_1 \not\sqsubseteq \mathcal{L}_2$. Slično, logike $\mathcal{L}_1$ i $\mathcal{L}_2$ su* ***ekvivalentno ekspresivne*** *(oznaka: $\mathcal{L}_1 \equiv \mathcal{L}_2$) ako $\mathcal{L}_1 \sqsubseteq \mathcal{L}_2$ i $\mathcal{L}_2 \sqsubseteq \mathcal{L}_1$.*

Ekspresivnost je jako bitan pojam u logici jer predstavlja jedan od kriterija za usporedbu različitih logika te omogućuje njihovo povezivanje. Inutitivno obrazloženje gornje definicije proizlazi iz pitanja je li moguće sve što se može izraziti u jednoj, također izraziti i u drugoj logici. Naravno, definicija prirodno zahtjeva da se ekspresivnost promatra nad istim tipom modela (i objektima unutar istog) kod obje logike. Kao što je već navedeno, činjenicu da su LTL+PAST i LTL ekvivalentno ekspresivne nećemo dokazivati, a dokaz se može pronaći u [3] i [6].

Definicija 15. *Između dvije logike $\mathcal{L}_1$ i $\mathcal{L}_2$ postoji* ***eksponencijalna razlika sažetosti*** *ako postoji niz $\{\phi_n\}_{n\in\mathbb{N}}$ formula u $\mathcal{L}_1$ takav da za svaki niz $\{\psi_n\}_{n\in\mathbb{N}}$ formula u $\mathcal{L}_2$, a koji zadovoljava $\psi_n \equiv \phi_n$, $\forall n \in \mathbb{N}$, vrijedi da veličina formule ψ_n raste eksponencijalno u odnosu na veličinu formule ϕ_n.*

Sažetost jedne logike nad drugom zanimljiva je samo ako se promatra jedna cijela familija (niz) formula, odnosno asimptotski rast njihovih veličina. Dakle, to iziskuje potrebu za uvođenjem jednog dijela asimptotske notacije koji će biti potreban za dokaz sažetosti logike LTL+PAST.

Definicija 16. *Neka su $f(n)$ i $g(n)$ funkcije čija je domena skup nenegativnih cijelih brojeva.*

(a) Kažemo da je funkcija f ***ograničena odozgo*** *funkcijom g (oznaka: $f(n) \in \mathcal{O}(g(n))$) ako postoje realna konstanta $c > 0$ i cijeli broj $n_0 \geq 1$ tako da $f(n) \leq c \cdot g(n)$ za svaki cijeli broj $n \geq n_0$.*

(b) Kažemo da je funkcija f ***ograničena odozdo*** *funkcijom g (oznaka: $f(n) \in \Omega(g(n))$) ako postoje realna konstanta $c > 0$ i cijeli broj $n_0 \geq 1$ tako da $f(n) \geq c \cdot g(n)$ za svaki cijeli broj $n \geq n_0$.*

Uočimo da ako $f(n) \in \mathcal{O}(g(n))$, onda funkcija f ne raste brže od funkcije g, dok u slučaju $f(n) \in \Omega(g(n))$ funkcija f ne raste sporije od funkcije g. Primjerice, u dokazu sažetosti LTL+PAST će funkcija veličine formule predstavljati funkciju f, a cilj će biti ograničiti ju eksponencijalnom funkcijom g u određenom kontekstu, no više o tome u nastavku.
Nakon sljedeće dvije napomene vezane uz shvaćanje linearnih modela i pokratu operatora, konačno ćemo imati sve potrebno za dokazivanje sažetosti LTL+PAST.

Napomena 5. *Skup linearnih modela nad unaprijed danim skupom propozicionalnih varijabli $\Pi \subseteq A_1$ za LTL formulu ϕ takvu da $PROP(\phi) \subseteq \Pi$, može se shvatiti kao jezik nad abecedom $\mathcal{P}(\Pi)$:*

$$Mod_\Pi(\phi) := \{\sigma \in (\mathcal{P}(\Pi))^\omega \mid \sigma \vDash \phi\}.$$

Često, ali ne uvijek, možemo pretpostaviti da $\Pi = PROP(\phi)$, osim ako nije drugačije zadano. U tom slučaju ćemo $Mod_{PROP(\phi)}(\phi)$ označiti jednostavno s $Mod(\phi)$. Intuitivno, $Mod(\phi)$ predstavlja skup svih modela na kojima je formula ϕ istinita.

Napomena 6. *U skladu s operatorima budućnosti, prirodno je definirati operator F^{-1} na sljedeći način: $F^{-1}\phi := \top S \phi$, odnosno $F^{-1}\phi$ je istinita na*

trenutnom stanju ako i samo ako je istinita na tom stanju ili nekom od prethodnih. Slično, definiramo operator G^{-1}: $G^{-1}\phi := \neg F^{-1}\neg\phi$, odnosno $G^{-1}\phi$ je istinita na trenutnom stanju ako i samo ako je ϕ istinita na trenutnom i na svakom prethodnom stanju.

Kako bismo dokazali eskponencijalnu razliku sažetosti između LTL+PAST i LTL, definiramo dva jezika $Init_n$ i All_n, $n \geq 1$:

1. $Init_n := \{\sigma \in (\mathcal{P}(\{p_0, ..., p_n\})^\omega \mid \forall i \in \mathbb{N} :$ ako vrijedi $p_k \in \sigma(i) \iff p_k \in \sigma(0)\ \forall k \in [1, n]$ onda $p_0 \in \sigma(i) \iff p_0 \in \sigma(0)\}$,

2. $All_n := \{\sigma \in (\mathcal{P}(\{p_0, ..., p_n\})^\omega \mid \forall i, j \in \mathbb{N} :$ ako vrijedi $p_k \in \sigma(i) \iff p_k \in \sigma(j)\ \forall k \in [1, n]$ onda $p_0 \in \sigma(i) \iff p_0 \in \sigma(j)\}$.

Vidimo da se jezik $Init_n$ sastoji od linearnih modela koji zadovoljavaju sljedeće svojstvo: svako stanje modela koje se podudara s inicijalnim stanjem što se tiče istinitosti propozicionalnih varijabli $p_1, ..., p_n$, mora se s njim podudarati i na istinitosti propozicionalne varijable p_0. Slično, linearni modeli u All_n zadovoljavaju sljedeće: bilo koja dva stanja koja se podudaraju na istinitosti propozicionalnih varijabli $p_1, ..., p_k$, moraju se podudarati i na istinitosti propozicionalne varijable p_0.
Vezano uz ta dva definirana jezika, želimo dokazati sljedeće tvrdnje:

1. Jezik $Init_n$ se može izraziti u $LTL + PAST$ koristeći formule veličine $\mathcal{O}(n)$.

2. Ako se $Init_n$ može izraziti u LTL koristeći formule veličine $g(n)$, onda se All_n može također izraziti u LTL koristeći formule veličine $g(n) + 1$.

3. Ako se All_n može izraziti u LTL koristeći formule $\{\psi_n\}_{n\in\mathbb{N}}$, onda ψ_n mora imati veličinu $2^{\Omega(n)}$.

Definiramo li LTL+PAST-formulu ϕ_n na sljedeći način:

$$\phi_n := G\left(\left(\bigwedge_{i=1}^{n} \alpha_n\right) \to \beta\right), \tag{2}$$

$$\alpha_n := (p_i \to F^{-1}G^{-1}p_i) \wedge (\neg p_i \to F^{-1}G^{-1}\neg p_i), \tag{3}$$

$$\beta := (p_0 \to F^{-1}G^{-1}p_0) \wedge (\neg p_0 \to F^{-1}G^{-1}\neg p_0), \tag{4}$$

dokaz prve tvrdnje direktno slijedi iz sljedeće leme.

Lema 4. *Za svaki $n \geq 1$ vrijedi $Mod(\phi_n) = Init_n$.*

Dokaz. Slijedi direktno iz definicije jezika $Init_n$. Naime, antecedent u kondicionalu osigurava da se odgovarajuće stanje modela podudara s inicijalnim na istinitosti propozicionalnih varijabli $p_1, ..., p_n$ jer u linearnim modelima nad prirodnim brojevima (kakve ovdje promatramo), istinitost formule $F^{-1}G^{-1}\psi$ jamči istinitost formule ψ u korijenskom stanju. Nadalje, formula β konačno osigurava podudaranje na istinitosti propozicionalne varijable p_0 inicijalnog stanja i onog na kojem je antecedent kondicionala istinit.

Iduća lema iskazuje povezanost jezika $Init_n$ i All_n, a druga tvrdnja je njezina izravna posljedica.

Lema 5. *Neka je $(\psi_n)_{n\in\mathbb{N}}$ niz LTL-formula takvih da $Mod(\psi_n) = Init_n, \forall n \geq 1$. Tada $Mod(G\psi_n) = All_n, \forall n \geq 1$.*

Dokaz. Neka je σ linearni model i $n \in \mathbb{N}$ proizvoljan. Ako $\sigma \in Mod(G\psi_n)$, onda vrijedi $\sigma, i \vDash \psi_n$ za svako stanje i tog modela. Neka su sada k i j dva proizvoljna stanja modela σ koja se podudaraju na istinitosti propozicionalnih varijabli $p_1, ..., p_n$. Bez smanjenja općenitosti možemo pretpostaviti da $k < j$ te potom dodatno definiramo $\sigma_k = \sigma[k, +\infty)$. Kako $\sigma, k \vDash \psi_n$, onda iz leme 1 slijedi $\sigma_k \vDash \psi_n$. Zbog $Mod(\psi_n) = Init_n, \forall n \geq 1$ znamo da $\sigma_k \in Init_n$, a onda iz pretpostavke da se stanja k i j podudaraju na istinitosti propozicionalnih varijabli $p_1, ..., p_n$ konačno slijedi $\sigma_k, k \vDash p_0 \iff \sigma_k, j \vDash p_0$, odnosno $\sigma, k \vDash p_0 \iff \sigma, j \vDash p_0$. Time smo dokazali $\sigma \in All_n$, odnosno $Mod(G\psi_n) \subseteq All_n$. Dokažimo sada drugu inkluziju. Neka je $\sigma \in All_n$. Pretpostavimo suprotno, tj. $\sigma \notin Mod(G\psi_n) \iff \sigma \nvDash G\psi_n \iff \sigma, 0 \nvDash G\psi_n \iff$ postoji neko stanje $k \geq 0$ takvo da $\sigma, k \nvDash \psi_n$. Ponovno definiramo $\sigma_k = \sigma[k, +\infty)$ te koristeći lemu 1 slijedi $\sigma_k \nvDash \psi_n \iff$ postoji stanje $j \geq k$ koje se podudara na istinitosti propozicionalnih varijabli $p_1, ..., p_n$ s inicijalnim stanjem u modelu σ_k, ali se s njim ne podudara na istinitosti propozicionalne varijable p_0. No, time smo zapravo dobili da u modelu σ postoje dva stanja k i j koja se podudaraju na istinitosti propozicionalnih varijabli $p_1, ..., p_n$, ali ne vrijedi $\sigma, k \vDash p_0 \iff \sigma, j \vDash p_0$ što je kontradikcija s pretpostavkom da $\sigma \in All_n$. Dakle, dobili smo $All_n \subseteq Mod(G\psi_n)$ čime smo dokazali jednakost skupova $Mod(G\psi_n)$ i All_n.

Prije dokazivanja treće tvrdnje potrebno je uvesti nekoliko oznaka. Uočimo kako postoji $N := 2^n$ međusobno različitih funkcija označavanja L obzirom na istinitost propozicionalnih varijabli $p_1, ..., p_n$ nad nekim fiksnim stanjem s. Definiramo konačan niz v_n na sljedeći način (prikazano je samo jedno moguće uređenje od $\mathcal{P}(\{p1, ..., p_n\})$):

$$v_n := (\emptyset, \{p_1\}, \{p_2\}, \{p_1, p_2\}, \{p_3\}, ..., \{p_1, ..., p_n\}).$$

gdje za svako stanje i vrijedi $\sigma_n, i \vDash p_j \iff p_j \in v_n(i)$, $j \in \{1, 2, ..., n\}$ gdje je σ_n linearni model sa skupom stanja $\{0, 1, ..., 2^n - 1\}$. Nadalje, za bilo koji skup pozicija $T \subseteq [1, 2^n]$[1] definiramo ω_n^T koji se dobiva iz v_n dodavanjem p_0 svim pozicijama u T i samo njima, odnosno

$$\omega_n^T(i) = \begin{cases} v_n(i) \cup \{p_0\}, \ i \in T \\ v_n(i), \ i \notin T \end{cases}.$$

Uočimo da takvih različitih skupova pozicija ima ukupno $2^N = 2^{2^n}$. Fiksirajmo jedan takav skup T_0 i promotrimo linearne modele $\rho_n^T := (\omega_n^T)^\omega$ i $\sigma_n^T := \omega_n^{T_0} \cdot \rho_n^T$, $\forall T \subseteq [1, 2^n]$. Jasno je da $\rho_n^T \in All_n$ za svaki $T \subseteq [1, 2^n]$, dok $\sigma_n^T \in All_n \iff T = T_0$. Sada smo spremni dokazati sljedeću lemu iz koje slijedi treća tvrdnja.

Lema 6. *Neka je ψ_n familija LTL-formula takvih da za svaki $n \geq 1$ imamo $Mod(\psi_n) = All_n$. Tada $|\psi_n| = 2^{\Omega(n)}$.*

Dokaz. Neka je σ_n^T definiran kao i ranije za svaki $T \in \mathcal{P}([1, 2^n])$. Promatramo formule koje se nalaze u zatvorenju od ψ_n, a koje su istinite na stanjima 0 i 2^n modela σ_n^T. Pretpostavimo da su skupovi takvih formula jednaki, odnosno $cl_{LTL}(\psi_n, \sigma_n^T, 0) = cl_{LTL}(\psi_n, \sigma_n^T, 2^n)$. Iz leme 3 slijedi da možemo maknuti stanja od 0 do $2^n - 1$ iz σ_n^T što rezultira modelom ρ_n^T, a nakon čega imamo

$$\sigma_n^T \vDash \psi_n \iff \rho_n^T \vDash \psi_n. \tag{5}$$

Dakle, dobili smo da ako $cl_{LTL}(\psi_n, \sigma_n^T, 0) = cl_{LTL}(\psi_n, \sigma_n^T, 2^n)$, onda vrijedi 5. No, $\rho_n^T \in All_n = Mod(\psi_n)$ za svaki T, a $\sigma_n^T \notin All_n$ za gotovo svaki T, tj. za njih točno $2^{2^n} - 1$. Sada iz obrata po kontrapoziciji dobivene implikacije slijedi da mora postojati barem $2^{2^n} - 1$ različitih podskupova skupa $cl_{LTL}(\psi_n)$ što je jedino moguće ako $|\psi_n| = 2^{\Omega(n)}$.

Kombinacijom te tri dokazane tvrdnje, odnosno lema 4, 5 i 6 dobivamo teorem kojim konačno dokazujemo eksponencijalnu razliku sažetosti LTL+PAST nad LTL.

Teorem 1. *Postoji niz LTL+PAST-formula $(\phi_n)_{n \in \mathbb{N}}$ takvih da za svaku familiju ψ_n LTL-formula za koje vrijedi $\psi_n \equiv \phi_n$, $\forall n \geq 1$ imamo: $|\psi_n| = 2^{\Omega(|\phi_n|)}$.*

Dokaz. Niz LTL+PAST-formula definiramo s 2. Iz leme 4 znamo da $Mod(\psi_n) = Init_n$, dok lema 5 govori da za svaku familiju ψ_n LTL-formula takvih da $Mod(\psi_n) = Init_n$, odnosno $\psi_n \equiv \phi_n$, vrijedi $Mod(G\psi_n) = All_n$.

[1] Ovdje iz tehničkih razloga pretpostavljamo da pozicije počinju od 1.

Definiramo $\psi_n^{'} := G\psi_n$. Kako je $(\psi_n^{'})_{n\in\mathbb{N}}$ niz LTL-formula i $Mod(\psi_n^{'}) = All_n$, iz leme 6 slijedi $|\psi_n^{'}| = 2^{\Omega(n)} \iff |\psi_n|+1 = 2^{\Omega(n)} \iff |\psi_n| = 2^{\Omega(n)}$. Iz prve tvrdnje znamo da $|\phi_n| \in \mathcal{O}(n)$ pa je $|\psi_n| = 2^{\Omega(n)}$ ekvivalentno s $|\psi_n| = 2^{\Omega(|\phi_n|)}$ čime smo dokazali tvrdnju.

4 Zaključak

U ovom radu predstavili smo linearnu temporalnu logiku i njezino proširenje operatorima prošlosti. Naveli smo činjenicu da su te dvije logike jednako ekspresivne, iako *a priori* to ne bismo očekivali. Ipak, dokazali smo sažetost LTL+PAST nad LTL koja je čak eksponencijalnog reda veličine čime vidimo da nije sasvim svejedno koju od te dvije logike koristimo za formaliziranje određenih procesa. Napomenimo da teoremom 1 nismo dokazali eskponencijalnu sažetost nad **konačnim** skupom propozicionalnih varijabli. To je zapravo pitanje koje i dalje stoji otvoreno.

Literatura

[1] Transition systems, https://cs.au.dk/ gerth/dADS1-12/daimi-fn64.pdf, 30.8.2023.

[2] Transition system basics, https://www.seas.upenn.edu/ utopcu/teach/old/VerInCtrlCaltech/VerInCtrl/lectureCSy.pdf, 30.8.2023.

[3] Dov M. Gabbay, Amir Pnueli, Saharon Shelah, and Jonathan Stavi. On the Temporal Analysis of Fairness. In Conference Record of the 7th ACM Symposium on Principles of Programming Languages (POPL'80), siječanj 1980, stranice 163–173. ACM Press, siječanj 1980.

[4] Nicolas Markey, Temporal Logic with Past is Exponentially More Succinct, https://hal.science/hal-01194627/document, 1.9.2023.

[5] Laura Horvat, Mateo Dujić: Algoritam za provjeru mješovito periodičkih modela linearne temporalne logike, 4.9.2023.

[6] Krešimir Burić, Linearna temporalna logika, https://repozitorij.pmf.unizg.hr/islandora/object/pmf%3A1509/datastream/PDF/view, 6.9.2023.

[7] Stephane Demri, Valentin Goranko, Martin Lange, Temporal Logics in Computer Science, 7.9.2023.

[8] Asymptotic Notation, https://www2.cs.arizona.edu/classes/cs345/summer14/files/bigO.pdf, 10.9.2023.

[9] Introduction to LTL - Basic intuition, https://www.youtube.com/watch?v=a9fo3dUly8A&ab_channel=Andrei Popescu, 12.9.2023.

[10] Sumit Nain, Moshe Y. Vardi: Branching vs. Linear Time: Semantical Perspective, 12.9.2023.