LTL i primeri svojstava koji se mogu izraziti u LTL-u

Seminarski rad u okviru kursa
Verifikacija softvera
Matematički fakultet

Ivona Jurošević, 1016/2018
ivonajurosevic@gmail.com

11. decembar 2018

Sažetak

Linearna temporalna logika (LTL) vrijeme modelira linearno, kao niz vremenskih trenutaka izomorfan skupu prirodnih brojeva. U ovom seminarskom radu prvo definišemo jezik LTL-a, tj. njegovu sintaksu i semantiku. Nakon toga ćemo pokazati neke primjere svojstava koji se mogu izraziti u LTL-u.

Sadržaj

1 Uvod

Linearna temporalna logika (LTL) je jedna vrsta temporalne logike. Temporalne logike su logike koje omogućavaju predstavljanje tvrđenja i rasuđivanje o tvrđenjima koja su kvalifikovana vremenskim odrednicama. Na primjer, u temporalnoj logici možemo da izrazimo tvrđenja kao što su "Ja sam uvijek gladan", "Ja ću u nekom trenutku biti gladan", "Ja ću biti gladan sve dok ne pojedem nešto". [3]

Začeci temporalne logike mogu se pronaći još u starogrčkoj filozofiji, ali oživljavanje temporalne logike kao formalne teorije počinje sredinom XX vijeka.

LTL omogućava formulisanje većine svojstava koja se tipično javljaju u verifikaciji zasnovanoj na proveravanju modela. Svojstva se formulišu kao LTL formule tako da sistem koji se verifikuje zadovoljava dato svojstvo akko je odgovarajuća formula valjana u tranzicionom sistemu T koji je model početnog sistema. [3]

2 Jezik linearne temporalne logike

Jezik linearne temporalne logike je sličan jeziku klasične logike, s dodatkom temporalnih operatora koji omogućavaju "gledanje"u budućnost.

U ovom poglavlju prvo opisujemo sintaksu, a zatim proučavamo semantiku LTL-a.

2.1 Sintaksa LTL-a

Osnova svakog jezika je njegov alfabet, odnosno skup simbola koje spajamo u riječi. Formalnije **alfabet** je proizvoljan neprazan skup čije elemente nazivamo **simboli** ili **znakovi**. **Riječ** alfabeta je svaki konačan niz njegovih simbola.

Definicija 2.1 *[2] **Alfabet LTL-a** je unija skupova A_1, A_2, A_3, A_4, A_5 pri čemu je:*

$A_1 = \{p_0, p_1, p_2, ...\}$, *prebrojiv skup čije elemente nazivamo logičke projenjive;*

$A_2 = \{\top, \bot\}$, *skup logičkih konstanti (istina i laž);*

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

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

$A_5 = \{(), \}$, *skup pomoćnih simbola (zagrade i zarez);*

Smatramo da su X, F, G unarni, a U, W binarni operatori. Oznake za operatore dolaze iz njihove interpretacije, ali to će kasnije biti detaljnije objašnjeno.

Sada ćemo definisati najvažnije riječi alfabeta, tj. formule LTL-a.

Definicija 2.2 *[2] Atomična formula je svaka logička promjenjiva ili logička konstanta. Pojam LTL formule definišemo na sledeći način:*

- *Svaka atomična formula je LTL formula.*
- *Ako su ϕ i ψ LTL formule onda su i $\neg\phi$, $\phi \wedge \psi$, $\phi \vee \psi$, $\phi \rightarrow \psi$ takođe LTL formule.*
- *Ako su ϕ i ψ LTL formule onda su i $X\phi$, $F\phi$, $G\phi$, $\phi U\psi$, $\phi W\psi$, takođe LTL formule.*
- *Ništa više nije LTL formula.*

Napomena 2.1 *Najveći prioritet imaju unarni veznici, zatim binarni temporalni (U, W), pa logički ($\wedge$, $\vee$), a najmanji ima implikacija ($\rightarrow$). Pregledniji zapis prioriteta dat je u tabeli 2.1:*

$\neg, X, G, F$
U, V
$\wedge, \vee$
$\rightarrow$

Tabela 1: Prioritet operatora

Napomena 2.2 *[2] U računarstvu se često za opisivanje sintakse jezika koristi Backus-Naurova forma (kratko BNF), gdje je sintaksa definisana rekurzivno uz pomoć produkcijskih pravila. BNF definicija LTL formule je data pravilom:*
$\Phi ::= \top|\bot|p|(\neg\phi)|(\phi \wedge \phi)|(\phi \vee \phi)|(\phi U \phi)|(\phi W \phi)|(X\phi)|(F\phi)|(G\phi)$.

2.2 Semantika LTL-a

2.2.1 Tranzicioni sistem

Definicija 2.3 *[3] Tranzicioni sistem je uređena šestorka $(S, Act, \rightarrow, I, \nu, \lambda)$, gdje je:*

- *S skup stanja*
- *$\rightarrow \subseteq S \times Act \times S$ relacija prelaska $(s_i \rightarrow s_j)$*
- *$I \subseteq S$ skup početnih stanja*
- *ν skup iskaznih promjenjivih (skup predikata)*
- *$\lambda : S \rightarrow \P\nu$ funkcija mapiranja (svakom stanju pridružuje skup predikata koji važe u tom stanju)*

Napomena 2.3 *Skup stanja može biti konačan ili beskonačan (tipično je konačan ali veoma veliki).*

Definicija 2.4 *[3] Putanja u sistemu $T = (S, Act, \rightarrow, I, \nu, \lambda)$ je beskonačni niz koji alternira stanja i akcije $\sigma = s_0\alpha_1 s_1\alpha_2 s_2 ...$ takav da važi $s_i \rightarrow s_{i+j}$, akcija: α_i, za svako $i \geq 0$. Pri tome ćemo koristiti oznaku $\sigma_i := s_i$ za i-to stanje putanje i $\sigma_{|i} := s_i s_{i+1} s_{i+2} ...$ za rep putanje počev od i-tog stanja. Izvršavanje u sistemu T je bilo koja putanja σ takva da je $\sigma_0 \in I$. Za svako stanje $s \in S$ kažemo da je dostižno ako postoji izvršavanje σ takvo da je $s \in \sigma$.*

2.2.2 Tačnost LTL formule

Definicija 2.5 *[3] [4] Neka je data proizvoljna putanja σ nad T. Formula ϕ je tačna na σ (u oznaci $\sigma \models \phi$) ako:*

- *$\sigma \models p$ ako je $p \in \lambda(\sigma_0)$ (tačno u početnom stanju putanje)*
- *$\sigma \models \neg\phi$ ako ne važi $\sigma \models \phi$*
- *$\sigma \models \phi \wedge \psi$ ako $\sigma \models \phi$ i $\sigma \models \psi$*
- *$\sigma \models \phi \vee \psi$ ako $\sigma \models \phi$ ili$\sigma \models \psi$*
- *$\sigma \models \phi \rightarrow \psi$ ako $\sigma \models \psi$ ili $\sigma \models \neg\phi$*

- $\sigma \models X\phi$ *ako* $\sigma_{|1} \models \phi$
- $\sigma \models \phi U \psi$ *ako* $(\exists j)(\sigma_{|j} \models \psi \wedge (\forall i < j)(\sigma_{|i} \models \psi))$
- $F\phi$ *je ekvivalentno sa* $\top U \phi$
- $G\phi$ *je ekvivalentno sa* $\neg F \neg \phi$
- $\phi W \psi$ *je ekvivalentno sa* $(\phi U \psi) \vee G\phi$

Definicija 2.6 *[3] Formula ϕ je zadovoljiva u tranzicionom sistemu T ako postoji putanja σ takva da je $\sigma \models \phi$.*

Definicija 2.7 *[3] Formula ϕ je valjana u tranzicionom sistemu T ako za svaku putanju σ važi da je $\sigma \models \phi$.*

2.2.3 Semantika temporalnih operatora

Napomena 2.4 *Primjetimo da se semantika operatora U, F, W, G, X definiše rekurzivno u odnosu na odgovarajuće repove putanje σ (rep putanje je takođe putanja).*

Napomena 2.5 *Istinitost formula na putanji se određuje posmatranjem raznih sufiksa putanje.*

Definicija 2.8 *[1] [3]*

- ***operator X*** *(eng.* neXt*) - $X\phi$ je tačna na putanji σ ako i samo ako je ϕ tačna u σ_1, tj. ako ϕ važi u sledećem stanju putanje σ*
- ***operator F*** *(eng.* Future*) - $F\phi$ je tačna na putanji σ ako i samo ako postoji i takvo da je ϕ tačna u σ_i, tj. ako ϕ važi u nekom budućem stanju putanje σ*
- ***operator G*** *(eng.* Globally*) - $G\phi$ je tačna na putanji σ ako i samo ako je za svako i ϕ tačna u σ_i, tj. ako ϕ važi u svakom sledećem stanju putanje σ*
- ***operator U*** *(eng.* Until*) - $\phi U \psi$ znači da ϕ važi duž putanje σ dokle god ψ ne postane tačno*
- ***operator W*** *(eng.* Weak*) - $\phi W \psi$ ima slično značenje kao i $\phi U \psi$, s tim što ψ nikada ne mora postati tačno (u tom slučaju će ϕ važiti zauvijek)*

2.2.4 Neke ekvivalencije formula

Definicija 2.9 *Kažemo da su dvije LTL formule ϕ i ψ logički ekvivalentne $\phi \equiv \psi$ ako za sve sisteme T i sve putanje σ iz T važi:*

$$\sigma \models \phi \text{ ako i samo ako } \sigma \models \psi.$$

Primer 2.1 *[1]*

$$\neg F\phi \equiv G\neg\phi$$
$$\neg G\phi \equiv F\neg\phi$$
$$\neg X\phi \equiv X\neg\phi$$
$$F(\phi \vee \psi) \equiv F\phi \vee F\psi$$
$$G(\phi \wedge \psi) \equiv G\phi \wedge G\psi$$
$$F\phi \equiv \top U \phi$$
$$\phi U \psi \equiv \phi W \psi \wedge F\psi$$
$$\phi W \psi \equiv \phi U \psi \vee G\phi$$
$$\phi U \psi \Rightarrow \phi W \psi$$
$$G\psi \vee G\phi \Rightarrow \phi W \psi$$

3 Svojstva na LTL jeziku

LTL omogućava formulisanje većine svojstava koja se tipično javljaju u verifikaciji zasnovanoj na provjeravanju modela.

Svojstva se formulišu kao LTL formule tako da sistem koji se verifikuje zadovoljava dato svojstvo akko je odgovarajuća formula valjana u tranzicionom sistemu T koji je model početnog sistema.

Primer svojstva koje se ne može izraziti na LTL jeziku je svako svojstvo koje uključuje vremensko rezonovanje o svim putanjama. Na primer „Iz svakog dostižnog stanja se može stići u neko početno stanje". Ili„Počevši od nekog trenutka, sve putanje će imati svojstvo p." [3]

3.1 Invarijante

Definicija 3.1 *[3] Invarijanta je svojstvo koje treba da važi u svim dostižnim stanjima tranzicionog sistema. Označavaju se formulama $G\phi$, gdje je ϕ neka iskazna formula.*

Primer 3.1 $G(x \neq 0)$ - *U svim dostižnim stanjima je* $x \neq 0$.

Primer 3.2 $G(x = 0 \vee y = 0)$ - *U svim dostižnim stanjima je ili* $x = 0$ *ili* $y = 0$.

3.2 Sigurnosna svojstva

Definicija 3.2 *[3] Sigurnosno svojstvo je svojstvo koje izražava da se neka negativna pojava nikada neće desiti. U oznaci imaju G kao vodeći veznik, ali potformula može sadržati i druge ne-iskazne veznike. (npr. Nikada se neće desiti* $x = 0$*).*

Primer 3.3 $G(x = 1 \Rightarrow ((x = 1)W(y \neq 0)))$ - *Kada x postane 1, ostaće 1 sve dok je y jednako 0.*

3.3 Svojstva živosti

Definicija 3.3 *[3] Svojstvo živosti je svojstvo koje izražava da će se neka pozitivna pojava sigurno desiti u budućnosti.*

Primer 3.4 $G(x = 1 \Rightarrow F(y = 1))$ - *Kada x postane 1, sigurno će u nekom trenutku i y postati 1.*

3.4 Svojstva pravednosti

Definicija 3.4 *[3] Svojstvo pravednosti je svojstvo koje izražava da će se neka pojava dešavati beskonačno puta tokom izvršavanja.*

Primer 3.5 $G(F(x = 1)) \Rightarrow G(F(y = 1))$ - *Ako x postaje 1 beskonačno puta tokom izvršavanja tada će i y postajati 1 beskonačno puta tokom izvršavanja.*

4 Zaključak

Linearna temporalna logika je od velikog značaja u verifikaciji softvera. Tehnika verifikacije je zasnovana na sistematskom ispitivanju svih mogućih putanja u izvršavanju nekog sistema. Ispituje se da li sistem ispunjava neko zadato svojstvo (invarijantu, sigurnosno svojstvo, i sl.)

Oslanja se na matematičku logiku, teoriju formalnih jezika, teoriju grafova. Primjenjujući Linearnu temporalnu logiku možemo da lakše opišemo svojstva koja je potrebno provjeriti.

Literatura

[1] Alessandro Artale. Linear temporal logic, 2011.

[2] Krešimir Burić. Linearna temporalna logika, 2014. on-line at: https://urn.nsk.hr/urn:nbn:hr:217:529525.

[3] Milena Vujošević Janičić. Slajdovi sa predavanja - Proveravanje Modela, 2018. on-line at: http://www.programskijezici.matf.bg.ac.rs/vs/predavanja/07_proveravanje_modela/proveravanje_modela_slajdovi.pdf.

[4] Julien Schmaltz. Linear temporal logic, 2014.

A Dodatak