ЈЕДАН ТАБЛО ДОКАЗИВАЧ ЗА ИНТУИЦИОНИСТИЧКИ ИСКАЗНИ РАЧУН

Недељко Стефановић, Момчило Боровчанин, Драган Додер, Александар Такачи
ГИС (Група за интелигентне системе), Математички факултет, Београдски универзитет

Сажетак – *У овом чланку приказаћемо један оптимизован доказивач теорема за интуиционистички исказни рачун и неке примене.*

1. ШТА ЈЕ ТО ИНУИЦИОНИСТИЧКА ИЛИ КОНСТРУКТИВНА ЛОГИКА?

Размотримо следећи класичан пример:

Задатак: Нађи позитивне ирационалне реалне бројеве a и b такве да је a^b рационалан број.

Предложено решење: Ако је $\sqrt{2}^{\sqrt{2}} \in \mathbf{Q}$, онда можемо ставити $a = \sqrt{2}$ и $b = \sqrt{2}$. Уколико пак $\sqrt{2}^{\sqrt{2}} \notin \mathbf{Q}$, онда можемо ставити $a = \sqrt{2}^{\sqrt{2}}$ и $b \in \sqrt{2}$ зато што је $\sqrt{2}^{\sqrt{2}}$ по претпоставци ирационалан и зато што важи

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^{\,2} = 2 \in \mathbf{Q}.$$

Да ли је овакво решење добро? Будући да смо у свим могућим случајевима доказали да тражени бројеви постоје, ово је заиста (ако се претпостави да је ирационалност броја $\sqrt{2}$ позната) корекан доказ постојања таквих бројева. Међутим, у задатку се није тражило да се докаже да они постоје, већ да се они нађу. Понуђено решење иако математички коректно извођено, не одговара задатку који је постављен јер ми у ствари на тај начин нисмо пронашли бројеве a и b са траженим особинама.

Штавише, формулацију овог задатка није ни могуће записати формално логички у оквиру класичне логике. Стога постоји потреба за њеним проширивањем. Размотримо следећу аксиоматизацију класичне логике:

1. $A \to (B \to A)$,
2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$,
3. $(A \wedge B) \to A$,
4. $(A \wedge B) \to B$,
5. $A \to (B \to (A \wedge B))$,
6. $A \to (A \vee B)$,
7. $B \to (A \vee B)$,
8. $(A \to C) \to ((B \to C) \to ((A \vee B) \to C))$,
9. $(\neg A) \to (A \to B)$,
10. $(A \to \neg B) \to (B \to \neg A)$,
11. $(\neg\neg A) \to A$,
12. (МП) $\dfrac{A,\ A \to B}{B}$,
13. $A(t) \to \exists x\, A(x)$,
14. $(\forall x\, A(x)) \to A(t)$,
15. (Ген_1) $\dfrac{A(x) \to B}{(\exists x\, A(x)) \to B}$,
16. (Ген_2) $\dfrac{A \to B(x)}{A \to \forall x\, B(x)}$,
17. $\forall x\, (x = x)$,
18. $\forall x \forall y\, ((x = y) \to (A(x) \to A(y)))$.

Овај запис захтева нека појашњења. Пре свега, објаснимо неке појмове. Променљива која је под дејством неког кватификатора (у овом случају $\forall$ или $\exists$) зове се *везана*, а у супротном *слободна*. рецимо, у формули

$$\forall x(f(x) = c \to R(c, y)) \to \exists z(R(f(z), c))$$

променљиве x и z су везане, а променљива y слободна. Међутим, пошто се у формули иста променљива може јавити и више пута, прецизније говорећи, појмови везаног и слободног се дефинишу за јављања променљиве. Рецимо, у формули

$$(\forall x \exists y\, R(x, y)) \to R(x, c)$$

је прво јављање променљиве x везано, а друго[1] слободно. Даље, нека је $A(x)$ формула и t неки[2] терм. Тада под формулом $A(t)$ подразумевамо формулу која се добија када сва слободна јављања променљиве x у формули $A(x)$ заменимо термом t. Ту замену сматрамо *регуларном* ако ниједан квантификатор није проширио своје дејство. Рецимо, нека је

$$\begin{aligned} A(x) &\equiv (\forall y\, R(x, y)) \to R(c, f(y)), \\ t &\equiv g(y, c), \end{aligned}$$

У овом примеру је

$$A(t) \equiv (\forall y\, R(g(y, c), y)) \to R(c, f(y)).$$

[1] Јављања променљивих уз сам квантор овде не бројимо.
[2] Израз

У добијеној формули је универзални квантификатор $\forall y$ проширио дејство на још једно јављање промењиве y, па замена није регуларна.

Аксиоме 13 и 14 су ограничене на случај када је замена свих слободних јављања промењиве x у формули $A(x)$ термом t регуларна, а у аксиоми 18 на случај када је $A(y)$ формула која се добија заменом неких (не обавезно свих) слободних јављања промењиве x у формули $A(x)$ промењивом y, као и да су све те замене регуларне. Такође, правило Ген_1 је ограничено на случај када промењива x нема слободних јављања у формули B. Слично, правило Ген_2 је ограничено на случај када промењива x нема слободних јављања у формули A.

Према теоремама сагласмности и потпуности, теореме овог формалног система су тачно ваљане формуле класичне логике. Међутим, ако избацимо аксиому 11 добијамо систем у коме је формулу облика $\exists x\, A(x)$ могуће доказати само применом аксиоме 13, то јест само ако претходно пронађено израз који редставља "сведока" за $\exists x\, A(x)$. Заправо, то значи да је квантификатор $\exists$ променио значење и постао тачно оно што нама треба.

Анализом предложеног решења задатка датог на почетку види се да се у том случају не може задржати закон искључења трећег $A \vee \neg A$. Међутим, мала би корист била од логике у којој бисмо изгубили основне логичке законе.

Заправо, класични закони се не морају изгубити. Најпре се показује да су везници $\vee$, $\rightarrow$ и квантификатор $\exists$ променили значење – $\vee$ је прешао у нешто што се зове интуиционистичка (или конструктивна) дисјункција, $\rightarrow$ у нешто што се зове интуиционистичка (или конструктивна) импликација, а квантификатор $\exists$ у нешто што се зове квантификатор конструктивног постојања. Стога их је због избегавања забуна добро означити неким другим, до сада некоришћеним симболима. Ми ћемо овде конструктивну дисјункцију означавати са $|$, конструктивну импликацију са $\supset$, а квантор конструктивног постојања са $\complement$. Тако долазимо до следећег записа наше аксиоматике:

1. $A \supset (B \supset A)$,
2. $(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$,
3. $(A \wedge B) \supset A$,
4. $(A \wedge B) \supset B$,
5. $A \supset (B \supset (A \wedge B))$,
6. $A \supset (A|B)$,
7. $B \supset (A|B)$,
8. $(A \supset C) \supset ((B \supset C) \supset ((A|B) \supset C)$,
9. $(\neg A) \supset (A \supset B)$,
10. $(A \supset \neg B) \supset (B \supset \neg A)$,
11. $\neg\neg A \supset A$.
12. (МП) $\dfrac{A,\ A \supset B}{B}$,
13. $A(t) \supset \complement x\, A(x)$,
14. $(\forall x\, A(x)) \supset A(t)$,
15. (Ген_1) $\dfrac{A(x) \supset B}{(\complement x\, A(x)) \supset B}$,
16. (Ген_2) $\dfrac{A \supset B(x)}{A \supset \forall x\, B(x)}$,
17. $\forall x\, (x = x)$,
18. $\forall x \forall y\, ((x = y) \supset (A(x) \supset A(y)))$.

Притом важе сасвим сличне непомене као малопре. Међутим, поставља се питање шта ћемо са преосталим класичним логичким везницима и квантификатором класичног постојања. Срећом они су дефинабилни у интуиционистичој логици. Увешћемо их као изведене симболе следећим дефиницијама:

$$\begin{aligned}(A \vee B) &:= \neg(\neg A \wedge \neg B),\\ (A \rightarrow B) &:= \neg(A \wedge \neg B),\\ (\exists x A) &:= \neg \forall x \neg A.\end{aligned}$$

Доказује се да за њих важе сви закони класичне логике. Међутим, на овај начин ми добијамо једно проширење класичне логике у коме можемо да формулишемо неке проблеме које у класичној логици не можемо.

Ако се вратимо на задатак са почетка, када би се додале потребне аксиоме теорије скупова за потпуно формално излагање тог доказа, добили бисмо као резултат да тражени реални бројеви постоје, али не бисмо на тај начин извели конструктивно постојање. Њега бисмо могли да изведемо тек када бисмо расправили која од две алтернативе вежи. Конкретно, према Гељфондовој теореми је $\sqrt{2}^{\sqrt{2}}$ ирационалан број, па би уз претходно изведен доказ Гељфондове теореме добили и доказ конструктивног постојања бројева a и b са траженим особинама. На крају поменимо да је инуиционистичка логика уједно и најстарија некласична логика.

2. МОДЕЛИ ИНТУИЦИОНИСТИЧКЕ ИЛИ КОНСТРУКТИВНЕ ЛОГИКЕ

Модели интуционистичке логике су знатно сложенији од модела класичне логике. Овде ћемо се позабавити такозваним Крипкеовим моделима. Надаље ћемо разматрати само исказни фрагмент инуиционистичке логике уз напомену да се сви резултати могу уопштити и на предикатски случај.

Крипкеов модел чине непразан скуп W снабдевен релацијом парцијалног уређења[3] $\geqslant$, као и релацијом задовољења $\models$ између елемената скупа W и формула тако да буду испуњени следећи услови:

1. За ма које $w, w' \in W$ и исказно слово p из $w \models p$ и $w' \geqslant w$ следи $w' \models p$.

2. За ма које $w \in W$ и ма које формуле A, B је $w \models A \wedge B$ еквивалентно са $w \models A$ и $w \models B$.

3. За ма које $w \in W$ и ма које формуле A, B је $w \models A|B$ еквивалентно са $w \models A$ или $w \models B$.

4. За ма које $w \in W$ и ма коју формулу A је $w \models \neg A$ еквивалентно са непостојањем $w' \in W$ таквог да је $w' \geqslant w$ и $w' \models A$.

5. За ма које $w \in W$ и ма које формуле A, B је $w \models A \supset B$ еквивалентно са тим да за свако $w' \in W$ из $w' \geqslant w$ и $w' \models A$ следи $w' \models B$.

Притом, елементе скупа W зовемо *световима*, релацију $\geqslant$ релацијом *временског поретка* ($w' \geqslant w$ се чита као "w' је после w" или "w' је касније од w"), а релацију $\models$ релацијом *задовољења* ($w \models A$ се чита као "формула A важи у свету w"). Најједноставнији примери Крипкеових модела су они који се састоје од само једног света, при чему у том свету важе тачно оне формуле које су тачне при једној фиксираној двовалентној валуацији (изабраним истиносним вредностима исказних слова) у складу са класичним исказним таблицама.

За формулу се каже да важи у неком Крипкеовом моделу ако важи у свим његовим световима. Доказује се да је формула интуиционистичка теорема ако и само ако важи у свим Крипкеовим моделима. Такође, доказује се да особина 1 важи за све формуле, а не само за исказна слова, и то у свим Крипкеовим моделима.

Штавише, Крипкеов модел је једнозначно одређен скупом светова, релацијом временског поретка на њима и важењем исказних слова на њима. Прецизније, ако је W било који непразан скуп, $\geqslant$ релација парцијалног уређења на њему, L скуп исказних слова, $f : W \longrightarrow P(L)$ произвољна функција која световима додељује подскупове скупа L са особином да за све $w, w' \in W$ из $w' \geqslant w$ следи $f(w') \supseteq f(w)$, онда постоји тачно једна релација $\models$ између светова и формула тако да се на тај начин добија Крипкеов модел и да за ма који свет w и исказно слово p услов $w \models p$ еквивалентан са $p \in f(w)$. Такође, на тај начин су описани сви Крипкеови модели. Овим је описан поступак конструкције Крипкеових модела.

Када се на претходни начин зада Крипкеов модел, важење сложенијих формула у световима тог модела се утврђује индуктивно по сложености формуле коришћењем осталих аксиома Крипкеових миодела.

[3]Рефлексивом, антисиметричном и транзитивном релацијом

3. МЕТОД СЕМАНТИЧКИХ ТАБЛОА ЗА ИНТУИЦИОНИСТИЧКУ ЛОГИКУ

Овај метод ће управо бити заснован на Крипкеовим моделима интуиционистичке логике. Најпре уведимо појмове означених и неозначених формула. Неозначена формула је обична формула у класичном смислу. Означена формула је неозначена формула којој претходи тачно једно од слова F или T. Интуиционистички табло је дрво чији су чворови означене формуле и који има два типа гранања – α-гранање и β-гранање, при чему су испуњени следећи услови:

1. Ако се за неке формуле A и B на некој грани појављује формула $T(A \wedge B)$, онда се на тој истој грани негде пре првог (евентуалног) гранања (могуће и било где пре тог појављивања формуле $T(A \wedge B)$) појављују формуле TA и TB.

2. Ако се за неке формуле A и B на некој грани појављује формула $F(A \wedge B)$, онда се на тој истој грани негде пре првог (евентуалног) гранања (могуће и било где пре тог појављивања формуле $F(A \wedge B)$) појављује бар једна од формула FA, FB, или након тог јављања формуле $F(A \wedge B)$ има β-гранања пре првог следећег (евентуалног) α-гранања, при чему се приликом првог таквог β-гранања дрво цепа на бар две гране од којих се на једној јавља формула FA, а на другој FB пре првог следећег (евентуалног) гранања на тим гранама.

3. Ако се за неке формуле A и B на некој грани појављује формула $T(A|B)$, онда се на тој истој грани негде пре првог (евентуалног) гранања (могуће и било где пре тог појављивања формуле $T(A|B)$) појављује бар једна од формула TA, TB, или након тог јављања формуле $T(A|B)$ има β-гранања пре првог следећег (евентуалног) α-гранања, при чему се приликом првог таквог β-гранања дрво цепа на бар две гране од којих се на једној јавља формула TA, а на другој TB пре првог следећег (евентуалног) гранања на тим гранама.

4. Ако се за неке формуле A и B на некој грани појављује формула $F(A|B)$, онда се на тој истој грани негде пре првог следећег (евентуалног) гранања (могуће и било где пре тог појављивања формуле $F(A|B)$) појављују формуле FA и FB.

5. Ако се за неке формуле A и B на некој грани појављују формуле TA и $T(A \supset B)$, онда се на тој грани појављује и формула TB.

Притом то јављање формуле TB може бити и пре неког од поменутих јављања формула TA, односно $T(A \supset B)$, или чак пре оба, али никако након неког гранања које је након оба та јављања.

6. Ако се за неке формуле A и B на некој грани појављују формуле $T(A \supset B)$ и FB, онда се на тој грани појављује и формула FA. Притом то јављање формуле FA може бити и пре неког од тих јављања формула $T(A \supset B)$ и FB, или чак пре оба, али никако након неког гранања које је након оба та јављања.

7. Ако се за неке формуле A и B на некој грани појављује формула $F(A \supset B)$, онда након тог јављања формуле $F(A \supset B)$ на тој грани постоји најмање једно α-гранање, при чему се на бар једном од наставака првог таквог гранања појављују формуле TA и FB пре првог следећег (евентуалног) гранања.

8. Ако се за неку формулу A на некој грани појављује $T\neg A$, онда се на тој грани пре првог следећег (евентуалног) гранања појављује FA.

9. Ако се за неку формулу A на некој грани појављује $F\neg A$, онда на тој грани након тог чвора има барем једног α-гранања, при чему се на барем једном од наставака првог таквог гранања појављује формула TA пре првог следећег (евентуалног) гранања.

Уколико се на некој грани за неку формулу A појављују формуле TA и FA, при чему се формула FA јавља након формуле TA или између њих нема нити једног α-гранања, онда се та грана зове *затвореном*. Притом, ако се на неком месту дрво грана α-гранањем на неки број наставака међу којима постоји такав наставак да су све гране које пролазе кроз њега затворене, онда се та затвореност по дефиницији преноси на све гране које пролазе кроз то гранање. Дрво је затворено ако су му све гране затворене. Доказује се да за ма коју формулу A важи да је A теорема ако и само ако постоји затворен табло са формулом FA у корену.

Таблои за ову логику се могу дефинисати и слободније, правилима са мање ограничења од наведених. Овде је изабран овај приступ јер он прилком стављања коначног броја формула у део од корена па до пре првог следећег гранања форсира један тип конструкције таквог дрвета код кога ако конструишемо незатворен табло, можемо бити сигурни да и нисмо могли никако конструисати одговарајући затворен табло спровођењем конструкције на неки други начин. Прецизније, ако конструишемо по овим правилима незатворен табло са на почетку постављеном означеном формулом облика FA у корену, онда можемо бити сигурни да формула A није теорема интуиционистичке логике под условом да нисмо убацивали у табло формуле које нам наведена правила нису сугерисала. Један доказивач базиран на овој методи је имплементиран.

У исказном случају се на овај начин у коначном броју корака проверава да ли је формула теорема интуиционистичке логике или не. У предикатском случају би поступак такође био заустављив да смо којим случајем на улазу задали теорему интуиционистичке логике. У супротном, ако смо на улазу дали формулу која није теорема, процес њеног испитивања у општем случају не би трајао коначан број корака. Међутим, према класичним логичким резултатима, алгоритам који би у општем случају у коначном броју корака утврдио да нека формула (која није теорема ове логике) заиста није теорема и није могуће направити.

ЛИТЕРАТУРА

[1] Melvin Fitting, "First-Order Logic and Automated Theorem Proving," 1996, 2nd ed., *Springer-Verlag*

[2] Raymond M. Smullyan, "First-Order Logic," 1968, *Springer-Verlag*

[3] S. C. Kleene, "Introduction to Metamathematics," 1952, *North-Holland*

[4] Жарко Мијајловић, Зоран Марковић, Коста Дошен, "Хилбертови проблеми и логика", 1986., *Завод за уџбенике и наставна средства – Београд*

[5] Уредници A. Robinson и A. Voronkov, "Handbook of Automated Reasoning," томови 1,2, 2001, *Elsevier Science*

Abstract – In this paper we present one optimised theorem prover for the intuitionistic propositional calculus and some application.

A VARIANT OF TABLEAU PROVER FOR THE INTUITIONISTIC PROPOSITIONAL CALCULUS

Nedeljko Stefanović, Momčilo Borovčanin, Dragan Doder, Aleksandar Takači