УДК 510.6

Андрій Ю. Паскевич

Поняття локальної істиності та його застосування у автоматичному доведенні теорем.

Досліджено поняття істинності деякого твердження у заданій позиції всередині формули. Показано, що можливо коректно проводити міркування щодо окремих підформул, та яким чином запропонована техніка може полегшити обробку формалізованого математичного тексту.

Ключові слова: верифікація математичних текстів, автоматичне доведення теорем.

Andrey Yu. Paskevich

A notion of a local truth and its applications in automated theorem proving.

We investigate when a given statement can be considered true in a given position inside a formula. We show that we can consistently reason about interiors of a formula and argue that proposed methods can facilitate processing of a formalized mathematical text.

Key Words: verification of mathematical texts, automated theorem proving.

У задачах автоматичного пошуку доведення, що походять з реальної математики, як правило, не зустрічаються абсолютно універсальні твердження, визначення та правила. Звичайно, все, що використовується, має певні умови чинності (такі як обмеження типу або обмеження області визначеності), які мають бути задовільнені. Наприклад, ми не можемо скоротити дріб $\frac{xy}{x}$, поки не доведено, що x не дорівнює нулю.

Візьмемо велику формулу виду $(\cdots \forall x\, (x \in \mathbb{R}^+ \supset (\cdots \frac{xy}{x} \cdots)) \cdots)$. Зрозуміло, що ми можемо замінити $\frac{xy}{x}$ на y, але як це довести? Саме питання здається абсурдним: оскільки терм містить зв'язані змінні, ми не можемо проводити жодних міркувань щодо нього. З традиційної точки зору, необхідно перш розщепити велику формулу до квантора, що зв'язує x, зробити підстановку (або сколемізувати), відділити $x \in \mathbb{R}^+$ і лише тоді робити скорочення.

Можна заперечити, що немає сенсу робити будь-які спрощення, коли спрощувана формула знаходиться десь всередині іншої формули. Рано чи пізно, але все одно велика формула має бути розщеплена, аби цей дріб міг бути використаний у доведенні. Тим не менш, ми вважаємо за корисне і повчальне спростити задачу *у її початковій формі* наскільки можливо, для того, щоб обрати найбільш перспективний напрямок пошуку доведення.

Окрім спрощення, є також проблема всюду визначеності даної формули. Кожне входження символу, введеного за визначенням, має задовольняти умовам визначення, щоб вважатися коректним. Бажано пересвідчитись, що задача сформульована коректно, до того, як братися за її вирішення. Але така верифікація знов-таки пов'язана з міркуваннями щодо термів, які містять зв'язані змінні (що має місце у попередньому прикладі).

Та сама проблема існує і на пропозиційному рівні. Припустимо, що теорія, яка розглядається, містить аксіому $A \supset B$, де A та B — фіксовані пропозиційні літери, і розгляньте формулу вигляду $(\cdots(A \wedge (\cdots B \cdots))\cdots)$. Знов, було б корисно замінити B на $\top$ (істина) і спростити формулу в цілому. Знов, немає техніки, що дозволяла б робити це безпосередньо.

Повернемось до початкового прикладу. Справді, твердження "x не нуль" є безглуздим, але можна сказати "x не нуль у даному входженні дробу $\frac{xy}{x}$". Інтуїція підказує, що разом зі звичайним істиностним значенням існує так зване *локальне істиностне значення*, що визчається відносно до контексту, до деякої позиції у формулі. Твердження, що є, взагалі кажучі, хибним або навіть абсурдним, може стати локально істинним, якщо розглядати його у ції позиції.

У цій роботі запропоновано поняття локально істинного твердження та показано, що можливо проводити коректні міркування про "внутрішність" формули. Заради стислості викладення, ми випускаємо доведення отриманих результатів. Досить зазначити, що майже всі вони отримані індукцією за будовою формули.

Загальні означення

Розглядаємо логіку першого порядку [1] з рівністю $\approx$, логічними зв'язками $\neg$, $\wedge$, $\vee$, $\supset$, $\equiv$ та кванторами $\forall$, $\exists$. Формули F та G вважаються *еквівалентними* (позначається через $F \simeq G$), якщо їхня логічна еквівалентність є теоремою логіки першого порядку, тобто $\models F \equiv G$. Універсальне замикання формули U позначається через $\forall U$.

Позиція — це слово в алфавіті $\{0, 1\}$. Множина позицій формули F, що позначається через $\Pi(F)$, визначається наступним чином (у наступному, $i.\Pi$ позначає $\{\, i.\pi \mid \pi \in \Pi \,\}$):

$$\begin{aligned} \Pi(A) &= \{\varepsilon\} && \text{де } A \text{ — пропозиційна змінна} \\ \Pi(*\,F) &= \{\varepsilon\} \cup 0.\Pi(F) && \text{де } * \in \{\forall x, \exists x, \neg\} \\ \Pi(F * G) &= \{\varepsilon\} \cup 0.\Pi(F) \cup 1.\Pi(G) && \text{де } * \in \{\wedge, \vee, \supset, \equiv\} \end{aligned}$$

Входження — це пара (F, π), де F є формулою та $\pi \in \Pi(F)$. Для кожної такої пари, $F|_\pi$ позначає підформулу F у позиції π: $F|_\varepsilon = F$, $(*\,F)|_{0.\pi} = F|_\pi$, $(F * G)|_{0.\pi} = F|_\pi$, $(F * G)|_{1.\pi} = G|_\pi$.

Для кожного входження (F, π) та формули U, формула $F[U]_\pi$ визначається наступним чином (вільні змінні з U можуть опинятися зв'язаними у $F[U]_\pi$):

$$\begin{aligned} F[U]_\varepsilon &= U & (*\,F)[U]_{0.\pi} &= (*\,F[U]_\pi) \\ (F * G)[U]_{0.\pi} &= (F[U]_\pi * G) & (F * G)[U]_{1.\pi} &= (F * G[U]_\pi) \end{aligned}$$

Локальні образи

Для кожного входження (F, π) та формули U, ми визначаємо (F, π)-*образ* U (позначається $\langle U\rangle_\pi^F$) за наступними тотожностями:

$$\begin{array}{lll}
\langle U\rangle_\varepsilon^F = U & \langle U\rangle_{0.\pi}^{F\wedge G} = G \supset \langle U\rangle_\pi^F & \langle U\rangle_{1.\pi}^{F\wedge G} = F \supset \langle U\rangle_\pi^G \\
\langle U\rangle_{0.\pi}^{\neg F} = \langle U\rangle_\pi^F & \langle U\rangle_{0.\pi}^{F\vee G} = G \vee \langle U\rangle_\pi^F & \langle U\rangle_{1.\pi}^{F\vee G} = F \vee \langle U\rangle_\pi^G \\
\langle U\rangle_{0.\pi}^{\forall x F} = \forall x\, \langle U\rangle_\pi^F & \langle U\rangle_{0.\pi}^{F\supset G} = G \vee \langle U\rangle_\pi^F & \langle U\rangle_{1.\pi}^{F\supset G} = F \supset \langle U\rangle_\pi^G \\
\langle U\rangle_{0.\pi}^{\exists x F} = \forall x\, \langle U\rangle_\pi^F & \langle U\rangle_{0.\pi}^{F\equiv G} = \langle U\rangle_\pi^F & \langle U\rangle_{1.\pi}^{F\equiv G} = \langle U\rangle_\pi^G
\end{array}$$

Формула $\langle U\rangle_\pi^F$ виражає твердження "*U є істинною у позиції π у F*". Відмітимо, що ця формула не залежить від підформули $F|_\pi$.

П р и к л а д 1. Нехай F є формулою

$$\forall x\,(x \in \mathbb{N} \supset \forall n\,(n \in \mathbb{N} \supset (x \approx \mathbf{fib}(n) \equiv \\ \equiv ((n \leqslant 1 \wedge x \approx 1) \vee x \approx (\mathbf{fib}(n-1) + \mathbf{fib}(n-2))))))$$

Ця формула представляє рекурсивне визначення — інакше кажучи, вона містить входження символу, що визначається, з правого боку від "головного" знаку еквівалентності. Справді, для $\pi = 0.1.0.1.1.1$, $F|_\pi = (x \approx (\mathbf{fib}(n-1) + \mathbf{fib}(n-2)))$. Треба переконатися, що аргументи $(n-1)$ та $(n-2)$ задовольняють умовам визначення та є строго меншими за n.

Зосередимось на другому аргументі $(n-2)$. Необхідно довести, що $\langle (n-2) \in \mathbb{N} \wedge (n-2) < n\rangle_\pi^F$. Ця формула, за визначенням, дорівнює

$$\forall x\,(x \in \mathbb{N} \supset \forall n\,(n \in \mathbb{N} \supset ((n \leqslant 1 \wedge x \approx 1) \vee ((n-2) \in \mathbb{N} \wedge (n-2) < n))))$$

Але ця формула є хибною за умови $n = x = 0$. Це вказує на помилку у запропонованому визначенні: $x = 0$ спростовує ліву частину диз'юнкції $F|_{0.1.0.1.1}$, отже ми маємо розглядати праву частину при $n = 0$ для того, щоб визначити істиностне значення усієї диз'юнкції. Тепер нескладно побудувати коректне визначення F':

$$\forall x\,(x \in \mathbb{N} \supset \forall n\,(n \in \mathbb{N} \supset (x \approx \mathbf{fib}(n) \equiv \\ \equiv ((n \leqslant 1 \wedge x \approx 1) \vee (n \geqslant 2 \wedge x \approx (\mathbf{fib}(n-1) + \mathbf{fib}(n-2)))))))$$

Властивості локальних образів

Лема 1. *Для будь-якого входження (F, π) та формули U, $\forall U \models \langle U\rangle_\pi^F$.*

Лема 2. *Для будь-якого входження (F, π) та формул U та V,*

$$\models \langle U \equiv V\rangle_\pi^F \supset (\langle U\rangle_\pi^F \equiv \langle V\rangle_\pi^F) \qquad \models \langle U \wedge V\rangle_\pi^F \equiv (\langle U\rangle_\pi^F \wedge \langle V\rangle_\pi^F)$$

Наслідок 3. $\models \langle U \supset V\rangle_\pi^F \supset (\langle U\rangle_\pi^F \supset \langle V\rangle_\pi^F)$

Наслідок 4. *Для будь-якого контексту C, що не містить кванторів,*

$$\models \big(\langle U_1 \equiv V_1\rangle^F_\pi \wedge \cdots \wedge \langle U_n \equiv V_n\rangle^F_\pi \wedge \langle t_1 \approx s_1\rangle^F_\pi \wedge \cdots \wedge \langle t_m \approx s_m\rangle^F_\pi\big) \supset$$
$$\supset \langle C[U_1, \ldots, U_n, t_1, \ldots, t_m] \equiv C[V_1, \ldots, V_n, s_1, \ldots, s_m]\rangle^F_\pi$$

Ці леми показують, що локальна істинність має цілком адекватні логічні властивості: істина є локальною істиною, кон'юнкція локальних істин є знов локальною істиною, нарешті, правило *modus ponens* також є локально застосовним. Але головна властивість локальних образів дається наступною теоремою.

Теорема 5. *Для будь-якого входження (F, π) та формул U та V,*

$$\models \langle U \equiv V\rangle^F_\pi \supset (F[U]_\pi \equiv F[V]_\pi)$$

Наслідок 6. *Для будь-якого входження (F, π) та формули U,*

$$\models \langle U\rangle^F_\pi \supset (F \equiv F[(U \wedge F|_\pi)]_\pi) \qquad \models \langle U\rangle^F_\pi \supset (F \equiv F[(U \supset F|_\pi)]_\pi)$$

Отже ми можемо безпечно замінювати підформули не лише на еквівалентні їм формули але також на *локально еквівалентні*. Зауважимо, що твердження, зворотнє до Теореми 5, має місце у пропозиційній логіці: $\models_0 \langle U \equiv V\rangle^F_\pi \equiv (F[U]_\pi \equiv F[V]_\pi)$. Тут локальна еквівалентність є *критерієм* підстановочної еквівалентності. У логіці першого порядку це не так, про що свідчить еквівалентність $(\exists x\, x \approx 0) \simeq (\exists x\, x \not\approx 0)$.

З'ясуємо, чи варті довіри міркування з Прикладу 1. Визначимо *визначення* як замкнену формулу вигляду $\forall \vec{x}\,(C(\vec{x}) \supset (P(\vec{x}) \equiv D(\vec{x})))$, де P є предикатним символом, $\vec{x}$ — послідовністю різних змінних, C — *формулою-умовою*, яка не містить P, а D — *формулою-розкриттям.* Розглянемо деяке входження (F, π), де $F|_\pi = P(\vec{s})$. Якщо можна довести $\langle C(\vec{s})\rangle^F_\pi$, то за Лемою 1 та Наслідком 3, маємо $\langle P(\vec{s}) \equiv D(\vec{s})\rangle^F_\pi$ (звісно, за умови, що визначення є частиною теорії). Тоді, за Теоремою 5, ми можемо розкрити визначення, замінивши $P(\vec{s})$ у (F, π) на $D(\vec{s})$.

Повертаючись до Прикладу 1, можна гарантувати, що таке розкриття завжди можливе (завдяки істиності $\langle n - 1 \in \mathbb{N} \ \wedge \ n - 2 \in \mathbb{N}\rangle^F_\pi$) та завжди скінчене (завдяки істиності $\langle n - 1 < n \ \wedge \ n - 2 < n\rangle^F_\pi$).

Висновок

Запропоноване поняття локально істинного твердження дозволяє формалізувати і перевіряти певні властивості коректності формул по відношенню до заданної теорії, може служити для розкриття визначень та для спрощуючих процедур. Зокрема, ця техніка може бути застосована для обробки не всюду визначених функцій та предикатів у математичних проблемах. Замість введення в логіку спеціальних індивідних та істинисних значень для позначення невизначеності [2], ми вимагаємо, щоб для кожного входження функціонального (предикатного) символу, відповідна функція (предиктат) була визначена a priori, тобто умови визначеності були локально істинними у тій позиції. Це відповідає традиційній математичній практиці, де входження частково визначених символів звичайно супроводжуються обмеженнями, що забезпечують визначеність.

Зауважимо, що отримані результати є чинними у інтуіціоністський логіці. Більш того, визначення (F, π)-образу легко поширити на мову (уні)-модальної логіки [3]: $\langle U \rangle_{0.\pi}^{\Box F} = \Box \langle U \rangle_{\pi}^{F}$ та $\langle U \rangle_{0.\pi}^{\Diamond F} = \Box \langle U \rangle_{\pi}^{F}$. Тоді всі наші твердження можуть бути доведені у модальній логіці **K**, отже у будь-якій нормальній модальній логіці.

В наступному, ми плануємо інтегрувати цю техніку в процедуру обробки математичних текстів в Системі Автоматизованої Дедукції (САД) [4] та дослідити на практиці її можливості. Зокрема, цікавим питанням є наступне: яким чином перетворення формули під час пошуку виводу впливають на її "локальні властивості", тобто на множину тверджень, що є локально істинними в цій формулі.

Література

[1] Мендельсон Э. Введение в математическую логику. – М.: Наука, 1984. – 319 с.

[2] Feferman S. Definedness. // Erkenntnis (Intern. J. of Analytic Philosophy). – 1995. – 43. – pp. 295–320.

[3] Фейс Р. Модальная логика. – М.: Наука, 1974. – 520 с.

[4] Aselderov Z., Verchinine K., Degtyarev A., Lyaletski A., Paskevich A., Pavlov A. Linguistic Tools and Deductive Technique of the System for Automated Deduction. – Proc. of the Third Intern. Workshop on Implementation of Logics. – Tbilisi, Georgia, Oct 2002 – pp. 21–24.

Надійшла до редакції 18.11.2002