УДК 004.82

Лялецький О.В.[1], к.ф.-м.н., с.н.с.
Афонін А.О.[2], к.ф.-м.н.

Про формальний математичний текст і логічну та онтологічну коректності

Стаття присвячена поняттям логічної та онтологічної коректностей та їх використанню при виконанні верифікації різноманітних математичних текстів, поданих формальною природною мовою ForTheL.

Ключові слова: логічна коректність, онтологічна коректність, формальний математичний текст, мова ForTheL .

[1]Київський національний університет імені Тараса Шевченка,03680, м. Київ, пр-т Глушкова 4д, e-mail: *lav@unicyb.kiev.ua*
[2]Національний університет «Києво-Могилянська академія» , 04655, м. Київ, вул. Сковороди 2, e-mails: *andrew.afomin@gmail.com*

A.V.Lyaletski[1], PhD (Physics&Mathematics)
A.A.Afonin[2], PhD (Physics&Mathematics)

On formal mathematical text and logical and ontological correctness's

The paper is devoted to the notions of logical and ontological correctness's as well as to their usage in verifying various mathematical texts presented in the formal natural language ForTheL.

Key Words: logical correctness, ontological correctness, formal mathematical text, ForThel language.

[1]Taras Shevchenko National University of Kyiv, 03680, Kyiv, Glushkova av., 4d, e-mail: *lav@unicyb.kiev.ua*
[2] National University of Kyiv-Mohyla Academy, 04655, Kyiv, Skovorody vul., 2, e-mails: *andrew.afomin@gmail.com*

Статтю представив д.т.н., проф. Кудин В.І.

Сьогодні активно розвиваються застосування систем керування математичними знаннями, які орієнтовані на розв'язання як задач синтезу та верифікації програмного забезпечення та апаратних засобів, так і задач перевірки коректності протоколів (криптографічних, комунікаційних і т.д.). Сучасна індустрія високих технологій надзвичайно зацікавлена у методах ефективно вирішення цих задач. Тому на сучасному етапі стає необхідним застосування систем автоматизації міркувань [1], які орієнтовані на розв'язання завдань керування математичними знаннями, які потребують потужної комп'ютерної підтримки, здатної до накопичення, організації та застосовування (напів-)формалізованого математичного знання. Одним з можливих підходів, що ведуть до досягнення цієї мети, є розвиток комп'ютерних логік у напрямку можливості застосування онтологій у процесі дедуктивних побудов, а також проведення досліджень з логічної та онтологічної коректностей тексту та їх застосування в системах автоматизації обробки математичних знань. Саме направленість досліджень на використання конкретних властивостей предметної області за допомогою логічних і онтологічних зв'язків веде до вивчення засобів збільшення виразних (мовних) можливостей логік (включаючи логіки першого порядку), що дає новий поштовх до вивчення різних формалізмів для завдання логічних систем, наприклад, появи дескриптивної логіки. Поява ж нових формалізмів ініціює вивчення семантик логік, що з'являються, а також побудову нових моделей для вже добре відомих формальних систем, наприклад, для лямбда-числення.

1. *Математичний текст* - це непросто послідовність речень або лямбда-терм, який кодує деяке доведення. Він представляє собою складний об'єкт, який містить аксіоми, визначення, теореми, допоміжні твердження (леми) і доведення різних видів (суперечністю, індукцією, аналізом випадків і т.д). Що ж може буту його "коректністю"? Не аналізуючи всі можливі підходи до цього поняття, ми нижче розвиваємо свій підхід, який базується на можливостях системи САД (http://nevidal.org), що була створена у рамках робіт по Алгоритму Очевидності [2-4] та орієнтована на пошук доведень і верифікацію математичних текстів [5] .

Можна виділяти чотири головних підходу до формального представлення математичного тексту (вважаться, що читач знайом з ними хоче б в загальних рисах) [6]: (1) інтерактивний, (2) оснований на лямбда-нотації, (3) генеруючий

доведення на базі вибору той або іншій техніки виведення і (4) декларативний, який активно використовується в системі САД в вигляді сукупності речень, поданих формальною природною мовою ForTheL [7].

Подібно звичайному математичному тексту, ForTheL-текст складається з визначень, тверджень, припущень, теорем, доведень и т.п. Він є послідовністю розділів верхнього рівня. Ці розділи - аксіоми, визначення, теореми та леми - відіграють в ForTheL ту ж саму роль, що й в звичайних математичних текстах. Будь-який розділ верхнього рівня складається з послідовності припущень, можливо порожньої, за якою йде твердження. Спеціальним розділом верхнього рівня є розділ "сигнатура", де вказується область визначеності нового синтаксичного примітива - перелічуються поняття до об'єму яких мають належати його аргументи. В онтологічні коректному тексті (дивись нижче), кожен синтаксичний примітив має вперше з'явитися або в розділі "визначення", або в розділі "сигнатура".

Твердження в розділі "теорема" може супроводжуватись доведенням. Доведення в ForTheL - це послідовність припущень, селекцій та тверджень (які можуть мати власні доведення), а також розділів нижнього рівня: випадків та простих блоків. Послідовність розділів типу "випадок" має завершувати доведення за розглядом випадків. Прості блоки використовуються лише для структуризації доведення: для обмеження області дії припущень та декларацій змінних. Мова ForTheL підтримує декілька схем доведень: від суперечного, за розглядом випадків, за загальною індукцією. Речення ForTheL також вважаються розділами нижнього рівня, зокрема, твердження, що супроводжується доведенням, є одним складним розділом.

Щодо семантики ForTheL-тексту, то вона залежить від завдання, що поставлено системі: наприклад, перевірка коректності або пошук релевантних фактів стосовно заданого твердження.

2. Перейдемо тепер к поняттям, що розглядаються у статті.

Для означення логічної коректності нам потребуються деякі поняття.

У тому, що слідує нижче, ForTheL-розділ A розглядується як трійка $(T,|A|[\Lambda])$, де T означає тип розділу, $|A|$ - формульне зображення розділу A, і Λ - послідовність підрозділів розділу A, якщо ці підрозділи існують [8].

Типи A можуть бути наступними: toplevel для будь-якого розділу (аксіома, визначення, розширення сигнатури, теорема, лема) верхнього рівня, case для розділу "випадок", assume для розділу "припущення", select для розділу "селекція", affirm для розділу "твердження", posit для розділу "постулат".

Вважається, що речення з забезпечуваним доведенням має той же тип, як така ж пропозиція без доведення. (Вони відрізняються тільки в третьому компоненті трійки, - списку підрозділів, - які порожні для речення без доведення.) Згадайте, що, так само, зображення формули речення не залежить від присутності доведення. У розділі "випадок", гіпотеза випадку належить до розділу зображення формули і не з'являється серед його підрозділів. Постулат - твердження в кінці аксіоми, визначення або розширення сигнатури; тобто, іншими словами, твердження, яке потрібні довести.

Формула F є *логічно коректною* відносно послідовності розділів Γ (логічний контекст формули F), тоді, тільки тоді, коли F може бути виведеною в класичному численні предикатів 1-го порядку з зображень формул розділив з Γ.

3. Підхід до означення онтологічної коректності ґрунтується на понятті "локального образа".

Ми використовуємо скінчені послідовності натуральних чисел для позначення позицій підформул та термів всередині формули.

Локальний образ формули U в позиції π в формулі F (позначається ${}^{F}\langle U\rangle_{\pi}$) - це формула першого порядку, що є формальним еквівалентом твердження U є локально істинною в позиції π в F. Формула ${}^{F}\langle U\rangle_{\pi}$ визначається рекурсією по структурі формули F.

Адекватність цього поняття підтверджується його наступними властивостями (знак $\models$ використовується для означення істинності, $\equiv$ - логічної еквівалентності, $\supset$ - імплікації):

- $\forall U \models {}^{F}\langle U\rangle_{\pi}$, тобто істинна формула є локально істинною в будь-якому оточенні ($\forall U$ тут означає універсальне замикання формули U);

- Якщо $\models {}^{F}\langle U\rangle_{\pi}$ і $\models {}^{F}\langle U\supset V\rangle_{\pi}$, то $\models {}^{F}\langle V\rangle_{\pi}$ ("локальний" modus ponens);

- Якщо $\models {}^{F}\langle U\equiv V\rangle_{\pi}$, то $\models (F[U]_{\pi} \equiv F[V]_{\pi})$, тобто: якщо два твердження є локально еквівалентними в деякій позиції формули, вони є взаємно замінюваними в цій позиції ($F[U]_{\pi}$ означає формулу, де U підставлено в позицію π формули F);

- Якщо $\vDash {}^{F}\langle s = t\rangle_{\pi}$, то $\vDash (F[s]_{\pi} \equiv F[t]_{\pi})$, тобто, аналогічно до попереднього, але тут π є позицією терму.

Ці властивості легко перетворюються у відповідні перетворення. Як результат, ми отримуємо так званий апарат локальних трансформацій, за допомогою якого ми можемо перевірити будь-якого логічного попередника розділу *A* на предмет його участі в локальних трансформаціях формального представлення |*A*| [9]. Це веде до наступного означення онтологічної коректності розділу.

Розділ *A* є *онтологічно коректнім відносно Г* тоді, і тільки тоді, коли кожне входження нелогічного символу в |*A*| або має відповідне означення, або має відповідне розширення сигнатури, або являється головним входженням в деяке означення чи в розширення сигнатури *A*.

ForTheL-текст *T* є *онтологічне коректнім* тоді, і тільки тоді, коли кожен розділ з *T* є онтологічне коректнім відносно його логічних попередників.

4. Введені поняття логічної і онтологічної коректностей були застосовані в системі САД. Так, були проведені експерименти по верифікації різноманітних реальних математичних текстів.

До найбільш цікавих експериментів належать:

- верифікація доведення скінченого і нескінченного варіантів теореми Рамсея, а також принципу компактності в формулюванні;
- верифікація доведення стабільності відношення потоншення (refinement) над класом специфікацій програм щодо деяких операцій над специфікаціями;
- верифікація доведення деяких властивостей кінцевих груп;
- верифікація доведення теореми Тарського про нерухому точку;
- верифікація доведення збіжності ряду із знакозмінними членами, який монотонно убуває по абсолютному значенню;
- верифікація доведення ірраціональності квадратного кореня з простого числа;
- верифікація доведення нерівності Коши-Буняковського для векторів над R.

Додатково відмітимо, що розроблений підхід до створення ефективних методів логіко-онтологічної верифікації формальних текстів може бути застосованим для перевірки властивостей протоколів, ефективного витягання та управління математичними знаннями, впорядкованого накопичення математичної інформації.

Список використаних джерел

1. Handbook of Automated Reasoning / *Eds.: Robinson A. and Voronkov A.* – Elsevier Science Publishers B.V., 2001. – Vol. 1, 2. – 2184 pp.
2. Glushkov *V.M.* Some problems of automata theory and artificial intelligence // Kibernetika. – 1970. – No. 2. – P. 3-13. (In Russian)
3. *Verchinine K., Lyaletski A., Paskevich A.* System for Automated Deduction (SAD): a tool for proof verification. // Lecture Notes in Computer Science. – 2007. – Vol. 4603. – P. 398-403.
4. *Lyaletski A., Paskevich A., Verchinine K.* SAD as a mathematical assistant — how should we go from here to there? // Journal of Applied Logic. – 2006. – 4(4) . – P. 560-591.
5. *Lyaletski A., Paskevich A., Verchinine K.* Theorem proving and proof verification in the system SAD // Lecture Notes in Computer Science. – 2004. – Vol. 3119. – P. 236-250.
6. *Anisimov A.V., Vershinin K P., Paskevich A. Yu., Lyaletski A.* On automated deduction in the environment of an natural formal language // Proceedings of the 3rd International conference "New information technologies in Education for All: E-Education". – Kyiv. – 2008. – P. 383-391. (In Russian)
7. *Vershinin K., Paskevich A.* ForTheL - the language of formal theories // Journal of Information Theories and Applications. – 2000. – 7, № 3. – P. 120-126.
8. *Anisimov A., Verchinine K., Lyaletski A., Paskevich A.* On Correctness of Mathematical Texts from a Logical and Practical Point of View // Lecture Notes in Computer Science (Intelligent Computer Mathematics: AISC/MKM/Calculemus 2008). – 2008. – Vol. 5144. – P. 583-598.
9. *Paskevich A., Verchinine K., Lyaletski A., Anisimov A.* Reasoning inside a formula and ontological correctness of a formal mathematical text // Calculemus/MKM 2007 — Work in Progress. – RISC-Linz Report Series. Number 07-06. – 2007. – P. 77-91.

Надійшла до редколегії 13.12.2013