Отзыв научного руководителя на отчёт по выполнению учебной практики бакалавра группы 21Б15-мм
Дудникова Ильи Алексеевича
на тему

"Formalization of definability theory in Lean"

К известной максиме Святослава Сергеевича Лаврова о том, что *хорошо написанная программа равноценна хорошей статье* существует и в некотором смысле обратное утверждение. Идеал научной программы Владимира Воеводского состоит в том, чтобы математические журналы принимали к публикации только статьи, сопровождаемые их машинно-проверяемыми эквивалентами. Но далее естественно спросить, почему мы уверенны в корректности работы программы, проверяющей доказательство? Мотивацией учебной практики Ильи Алексеевича Дудникова послужила прошлогодняя статья Гильермо Переса и Ратима Рахи (см. [6] на с. 14 отчёта), в которой исправляется допущенная ранее другими авторами ошибка, связанная с фрагментом арифметики целых чисел со сложением и делимостью. Получается парадоксальная ситуация: на основе разрешимости (что на самом деле не имеет места) некоторой арифметической теории были разработаны инструменты для проверки корректности программ со счётчиками. Как оказалось, класс формул можно сузить (без потери ценности в приложениях) и получить-таки разрешимость. Остаётся лишь надеяться, что теперь все ошибки исправлены.

Либо предоставить формальное доказательство в системе интерактивного построения доказательств, ведь здесь мы имеем дело с самыми основами всякого математического рассуждения: логикой первого порядка и элементарной теорией чисел. Для этих целей был выбран язык Lean с активно развиваемой библиотекой mathlib [1] . В приложениях обычно используются самые простые арифметические инструменты: простые числа, делимости, НОК, НОД, возведение в степень, побитовые операции, и поэтому особенную важность играют вопросы выразимости с помощью формул языка первого порядка L_σ сигнатуры σ в так называемых арифметических структурах. Носителем интерпретации символов σ являются неотрицательные целые числа $\mathbb{N}$, а интерпретация всякого функционального и предикатного символа осуществляется посредством некоторой формулы языка элементарной арифметики $L_{\langle 0,1,+,*,<\rangle}$. Далее определяется множество всех выразимых в $\langle \mathbb{N}; \sigma\rangle$ предикатов $\mathrm{Def}(\langle \mathbb{N}; \sigma\rangle)$ и понятие Def-полноты [2] . Основной целью проекта было заложить основы для быстрого введения в Lean арифметических структур и разработать инструменты для построения формальных доказательств теорем о выразительных возможностях этих структур. В mathlib продолжают появляться основные результаты теории моделей, которые в этом проекте не пригодятся. Поэтому было принято решение работать с проектом 2020 года igl2020, в котором также формализованы все базовые понятия логики первого порядка.

Пусть для удобства в сигнатуре отсутствуют функциональные символы, и арифметический язык `arith_lang` определяется лишь числом предикатных символов и функцией, задающей их арность. Обратной стороной удобства задания арифметических структур является техническая трудность доказательства возможности приведения (*coercion*) всякой арифметической структуры к структуре, как она определялась в igl2020. Для написания следующей части файла `arith_structure.lean` [3] потребовалось много аккуратности.

```
def arith_struc.to_struc {L : arith_lang} (S : arith_struc L) : struc L :=
  {
      ⋮
  }

instance arith_struc_to_struc_coe {L : arith_lang} : has_coe (arith_struc L) (struc L)
    := ⟨arith_struc.to_struc⟩
```

[1] The mathlib Community. „The Lean Mathematical Library“. In: *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs.* New York, NY, USA: Association for Computing Machinery, 2020, 367–381. DOI: 10.1145/3372885.3373824. URL: https://doi.org/10.1145/3372885.3373824.

[2] Ivan Korec. „A list of arithmetical structures complete with respect to the first-order definability“. In: *Theoretical Computer Science* 257.1 (2001), pp. 115–151. DOI: https://doi.org/10.1016/S0304-3975(00)00113-4.

[3] URL: https://github.com/airh4ck/igl2020/blob/definability_of_sets/src/arith_structure.lean.

Несмотря на внушительное число строк и нетривиальную структуру фрагмента кода, который заменён здесь многоточием, написан он вполне ясно. Это является несомненным успехом.

Логика построения определений и доказательств в Lean подсказывает новые определения и обобщения тех понятий, которые изначально предполагалось формализовать. Об одной из таких потенциальных возможностей идёт речь на страницах 7–8. Интерпретацию предикатных символов новой арифметической структуры можно задавать с помощью формул языка другой арифметической структуры. На этом пути появилось одновременно как много весьма любопытных вопросов, так и технических трудностей. В совместном обсуждении этой проблемы было принято решение зафиксировать *стандартную* структуру $\langle \mathbb{N}; 0, 1, +, *, < \rangle$, с помощью которой и будут задаваться интерпретации предикатных символов всякой `arith_struc`. В сущности, моё руководство заключалось всего лишь в отслеживании появления и развития новых определений и лемм в работе Ильи Алексеевича так, чтобы можно было успеть *в рамках учебной практики* доказать некоторое достаточно содержательное утверждение.

Указанное выше ограничение позволило построить формальное доказательство теоремы о том, что в случае выразимости в некоторой структуре S_1 всякого предиката из определения структуры S_2, множество $\mathrm{Def}(S_2)$ содержится в $\mathrm{Def}(S_1)$. Подготовка необходимых лемм и само доказательство является вторым важным техническим результатом работы (см. с. 9–12 отчёта). Теперь видим, что для сопоставления выразительных возможностей арифметических структур (в частности, для доказательства Def-полноты) можно сосредоточиться на доказательствах выразимости конкретных предикатов.

Работа выполнена абсолютно самостоятельно, а текст отчёта по учебной практике написан на английском довольно аккуратно. О результатах работы были сделаны доклады на секциях "Системное программирование" и "Фундаментальная информатика" научной конференции по проблемам информатики СПИСОК-2023. Как мне видится, перенести полученные результаты в mathlib не должно быть сложно, и работу интересно было бы продолжить так, чтобы суметь формализовать теорему о выразимости из указанной выше статьи Переса и Рахи. А на данный момент *работа Дудникова Ильи Алексеевича безусловно заслуживает* ***зачёта*** *с оценкой* ***"A"***.

Ассистент кафедры информатики,
кандидат физико-математических наук

Старчак Михаил Романович

31.05.2023