На пути к парадигмам задания спецификаций программ и мероприятие SpecifyThis 2024

Кондратьев Дмитрий Александрович

Институт систем информатики им. А. П. Ершова СО РАН
Новосибирский Государственный Университет

Мероприятия серии SpecifyThis

На текущий момент было проведено два мероприятия серии SpecifyThis:

- SpecifyThis 2022.
- SpecifyThis 2024.

По названию данные мероприятия похожи на соревнования по дедуктивной верификации VerifyThis.

Есть потенциал превращения данных мероприятий в соревнования по заданию спецификаций программ.

Однако, на текущий момент мероприятия серии SpecifyThis представляют собой не соревнования, а треки конференции ISoLA.

Отметим, что тематика задания спецификаций программ особенно представлена на Российских соревнованиях по формальной верификации серии VeHa.

Парадигмы задания спецификаций программ

В статье о SpecifyThis был впервые введен такой термин, как парадигмы задания спецификаций программ:

Ahrendt W., Herber P., Huisman M., Ulbrich M. SpecifyThis – Bridging Gaps Between Program Specification Paradigms // Lecture Notes in Computer Science. 2022. Volume 13701. pp. 3–6.
DOI: `https://doi.org/10.1007/978-3-031-19849-6_1`

Однако тематика парадигм задания спецификаций программ тогда осталась не раскрыта.

Обсуждение на Дне Проблем семинара STEP в 2022 году

На Дне Проблем семинара STEP в 2022 году было высказано, что спецификации бывают:

- Функциональные
- Темпоральные

Также было высказано, что спецификации бывают:

- Исполнимые
- Неисполнимые

Была надежда, что терминология парадигм задания спецификаций программ прояснится на следующем мероприятии серии SpecifyThis.

Парадигмы задания спецификаций программ на мероприятии SpecifyThis 2024

В статье по итогам SpecifyThis 2024 вновь упоминаются парадигмы задания спецификаций программ:

Ernst G., Herber P., Huisman M., Ulbrich M. SpecifyThis Bridging Gaps Between Program Specification Paradigms: Track Introduction // Lecture Notes in Computer Science. 2025. Volume 15221. pp. 3–7.
DOI: `https://doi.org/10.1007/978-3-031-75380-0_1`

Но снова терминология парадигм задания спецификаций программ осталась не прояснена.

Но при этом на треке SpecifyThis 2024 были интересные статьи о задании спецификаций программ.

Интересные статьи с трека SpecifyThis 2024

Статья о едином языке для задания спецификаций программ:

Ernst G., Pfeifer W., Ulbrich M. Contract-LIB: A Proposal for a Common Interchange Format for Software System Specification // Lecture Notes in Computer Science. 2025. Volume 15221. pp. 79–105.
DOI: `https://doi.org/10.1007/978-3-031-75380-0_6`

Отметим известные языки для задания спецификаций программ:

- ACSL – языка для заданий спецификаций программ, заданных на языке C.
- JML – язык для задания спецификаций программ, заданных на языке Java

В данной статье предлагается единый язык Contract-LIB для задания спецификаций программ на основе входного языка SMT-решателей SMT-LIB.

Contract-LIB: A Proposal for a Common Interchange Format for Software System Specification

Статья о едином языке для задания спецификаций программ:

Ernst G., Pfeifer W., Ulbrich M. Contract-LIB: A Proposal for a Common Interchange Format for Software System Specification // Lecture Notes in Computer Science. 2025. Volume 15221. pp. 79–105.
DOI: `https://doi.org/10.1007/978-3-031-75380-0_6`

Общедоступна реализация языка Contract-LIB, позволяющая перевести конструкции языка Contract-LIB в AST-представление:

`https://github.com/Contract-LIB/contract-lib-java`

Contract-LIB: A Proposal for a Common Interchange Format for Software System Specification

Ernst G., Pfeifer W., Ulbrich M. Contract-LIB: A Proposal for a Common Interchange Format for Software System Specification // Lecture Notes in Computer Science. 2025. Volume 15221. pp. 79–105.
DOI: `https://doi.org/10.1007/978-3-031-75380-0_6`
Рассмотрим возможные проблемы:

- Лежащий в основе язык SMT-LIB основан на префиксной записи, S-выражениях, что может быть непривычно для пользователей, не знакомых ни с языком SMT-LIB, ни с языками семейства Lisp. Отметим, что в разработанной в ИСИ СО РАН системе дедуктивной верификации C-lightVer для задания спецификаций используется язык Applicative Common Lisp.
- Для языков задания спецификаций важен расширяемый набор библиотек, описывающий теории предметной области. Для языка Contract-LIB такие библиотеки еще предстоит наработать.

Важное преимущество состоит в простоте лексического и синтаксического анализа языка.

Еще одна интересная статья с трека SpecifyThis 2024

Статья о важной проблеме дедуктивной верификации программ, где есть вставки кода на других языках программирования:

Furia C.A., Tiwari A. Challenges of Multilingual Program Specification and Analysis // Lecture Notes in Computer Science. 2025. Volume 15221. pp. 124–143.
DOI: https://doi.org/10.1007/978-3-031-75380-0_8

В данной статье описаны примеры таких случаев, представляющие сложность для дедуктивной верификации. Это полезный материал для проверки возможностей систем дедуктивной верификации и для будущих соревнований.

Вместо заключения

Вместо заключения дискуссионные вопросы:

- Почему мероприятие SpecifyThis пока что не переросло в соревнование по заданию спецификаций программ?
- Почему пока что нет попыток в явном виде перечислить парадигмы задания спецификаций программ?

Спасибо за внимание!

На пути к парадигмам задания спецификаций программ и мероприятие SpecifyThis 2024

Кондратьев Дмитрий Александрович

Институт систем информатики им. А. П. Ершова СО РАН
Новосибирский Государственный Университет