Индекс УДК: 004.432.42
“Унифицированный формат для доказательств на языках с зависимыми типами”
Халанский Д. В., Университет ИТМО, Санкт-Петербург.
Научный руководитель: Исаев Валерий Иванович, национальный исследовательский университет “Высшая Школа Экономики”, Санкт-Петербург.

Введение.

Существует широкая потребность в формальных методах доказательств строгих суждений. Помимо очевидного применения таких подходов в математических дисциплинах, можно выделить использование аксиоматического вывода в программировании в контекстах, когда корректность алгоритма не сразу видна, или в условиях повышенной важности отсутствия проблем в работе программы при любых условиях, например, в космической, авиационной, медицинской индустриях. Иначе, при разработке программного обеспечения для, к примеру, микроконтроллера, который предполагается использовать в медицинском оборудовании, необходимо провести формальную верификацию того, что никакие входные воздействия не приведут к тому, что система окажется в некорректном состоянии.

Формальные доказательства вручную -- это процесс, в котором можно допустить трудноуловимые ошибки, поэтому существуют системы, которые осуществляют проверку доказательств. К сожалению, системами доказательств зачастую сложно пользоваться в силу сложности оперирования высокоуровневыми суждениями, свойственными доказательствам в математике. Дополнительно проблема в удобстве использования усугубляется тем, что существует несколько различных систем доказательств, и результаты, доказанные в одной из них, нельзя простым образом перенести в другую.

Наиболее популярны в современности системы доказательств, основанные на механизме зависимых типов, и можно, ограничившись рассмотрением таких систем, создать механизм перевода доказательств из одной системы в другую.

Цель работы.

Создать унифицированный формат для представления доказательств, проведённых в системах, основанных на механизме зависимых типов.

Базовые положения работы.

Системы доказательств, построенные на механизме зависимых типов, являются функциональными языками программирования. В таких системах запрещены функции, которые могут не завершиться, и доказательство теорем осуществляется через соответствие Карри-Говарда -- соотношение между типом в функциональном языке программирования и высказыванием в математической логике.

Промежуточные результаты.

В рамках данной работы:

- Проанализированы наиболее популярные языки с зависимыми типами: Coq, Agda и Idris.
- Изучена возможность единообразного представления доказательств на этих языках и в гомотопической теории типов.
- Выделен набор конструкций, обобщающих механизмы, используемые в этих системах.
- Составлены правила трансляции из этих механизмов в новые конструкции и обратно.

Основной результат.

В результате работы предложен новый язык с зависимыми типами, задающий промежуточное представление при трансляции между разными системами доказательств.