Необозримые доказательства

Проблемы

Является ли объект в заявленном смысле корректным доказательством

Нет ли ошибки в проверяющей программе?

Правильно ли работает устройство, на котором запущена проверка?

Правда ли, что формальная модель, в которой проводится доказательство, непротиворечива.

Даже если она непротиворечива, нет ли в ней неявных аксиом, которые нам не нравятся?

Правда ли, что доказанное формальное утверждение означает то, что написано в заголовке?

Сложность создания

Что оно даёт взамен?

Всё равно надёжнее, чем проверка человеком для технических рассуждений с тонкими местами.

Некоторая надежда на поиск формально родственных фактов в большом объёме статей — нет шансов это сделать с теми текстами, которые у нас есть сейчас.

Какие инструменты сейчас есть.

С точки зрения процесса:
Человек указывает, что (примерно) делать дальше. Coq.
Автономный поиск доказательства с нуля. E Prover.
Попытки совмещения. Например, набор контрольных точек для автоматического поиска доказательств.

Область интересов:
Математические доказательства. Формализация математики.
Доказательства корректности программ или вычислительного аппаратного обеспечения. ACL2, Why3.
Работа с базами данных. Semantic Web etc. Jena inference engine.

Конкретные примеры.

Гипотеза Роббинса: Алгебраическая гипотеза про свойства операций. Доказать не удавалось с 1930-х годов. В 1996 году с помощью EQP, программы автоматического поиска доказательств, гипотеза была подтверждена. После изучения доказательства, в 1998 году Дан (Dahn B.I.) смог предъявить простое доказательство, доступное человеку. Главный алгебраический трюк можно уместить на пол-страницы текста.

Проблема 4 красок. Любую карту на плоскости можно окрасить в 4 краски так, что страны с общей границей (ненулевой длины) окрашены в разные цвета.

Первое доказательство использовало компьютерный перебор и какое-то неформальное доказательство корректности перебора.

В настоящий момент есть доказательство с помощью Coq (использующее особенности системы коиндуктивных типов, позволяющих упаковать перебор внутри стандартной процедуры проверки доказательства).

Для реализации полностью формального доказательства, понятие графа на плоскости было переопределено. Граф рассмотрели как набор флагов (троек вершина-ребро-грань, таких что грань слева от ребра). После этого имеется три отображения флагов: обход вершины против часовой стрелки, рассмотрение ребра с другой стороны и обход грани против часовой стрелки. Оказалось, что можно оставить только требование того, что композиция этих трёх взаимно-однозначных отображений тождественна. Планарность была выражена формулой Эйлера (которая в этой ситуации симметрична).

Mizar Mathematical Library

Самая большая библиотека формально доказанных математических фактов.

TPTP

Язык для записи формальных утверждений с наибольшим количеством независимых программ, могущих с ним работать. Большое количество собранных задач для автоматического поиска доказательства.

Утверждения пишутся похожим на обычные формализации способом. Пример (часть задания функции большинства): fof(majority,axiom,(! [X,Y] : f(X,X,Y)

= X)). ![X] — квантор всеобщности, ?[X] — квантор существования. При этом, что приятно, можно использовать обычное исчисление предикатов первого порядка.

MPTP - попытка выяснить, какие из фактов из MML можно доказать автоматически с помощью перевода их на язык TPTP.