

Памятка по использованию инструмента pvs

После очередного шага pvs показывает набор формул, которые надо воспринимать:

- сверху черты (антецедент) - как конъюнкция формул с кванторами существования на свободные переменные
- ниже черты (консеквент) - как дизъюнкция формул с кванторами всеобщности на свободные переменные

В рамках доказательства утверждения в pvs следует:

1. максимально упростить задействованные формулы (убрать кванторы, логические связи, вычислить всё, что можно, подставить тела вызываемых функций)
2. вручную попробовать доказать, что из конъюнкции формул над чертой следует формула под чертой. Потом всё то же провести с помощью команд pvs. Здесь достаточно либо применять алгебраические аксиомы (эквивалентности композиций функций), либо применить индукцию, если получается выражение над целыми числами.

Для этого вам понадобятся следующие команды pvs:

(skolem!) - преобразовать квантор всеобщности в консеквентах в новую переменную, преобразовать квантор существования в антецедентах в новую переменную

(inst) - для подстановки конкретного значения вместо переменной под квантором всеобщности

(prop) - убирает логические связи (конъюнкцию в антеценденте преобразовать в набор формул-конъюнктов)

Упрощение работает только с одной формулой! Чтобы ее собрать из разных формул, используйте merge-fnums.

(flatten) - перенести посылку импликации из консеквентов в антецеденты

(simplify) - делает простейшие упрощения (например, "(1::int)" заменить на просто "1")

(hide число) - если много консеквентов, убирает пока консеквент с данным номером - потом его надо будет доказать отдельно

(rewrite имяпредиката) - подставить вместо использования предиката его определение

В любой момент можно делать:

(undo) - возврат на шаг назад

(grind) - стратегия, которая часто приводит к верному доказательству (ее можно применять после каждого очередного шага, чтобы понять - вдруг pvs сам может доделать доказательство) - иногда может приводить к непонятным следствиям, поэтому надо пользоваться этой командой аккуратно