Лекция 6. Леммы, ghost-блок-схемы, auto-active verification

Цель лекции

Научиться еще эффективнее использовать SMT-солверы для дедуктивной верификации.

Содержание

1 Леммы

2 Ghost-блок-схемы

Добавление термов

- Продолжаем доказывать полную корректность блок-схемы, вычисляющей квадратный корень. Часть условий верификации пока не доказаны. Продолжаем их доказательство.
- Анализ триггеров показывает, что солвер *может* не доказывать условия верификации, т.к. нечем инстанцировать квантор.
- Какой нужен терм (чтобы получить нужное противоречие)? Куда можно добавить этот терм?

Место добавления

- Получается, нам нужно новое утверждение, которое даст и триггер, и противоречие. Куда добавляем?
- в предусловие или постусловие нельзя, это часть требований
- в индуктивное утверждение? К чему это приведет?
- в оценочную функцию? К чему это приведет?
- добавить новые точки сечения с нужными индуктивными утверждениями и оценочными функциями? К чему это приведет?

Лемма

- Лемма – это истинное утверждение, которое включается в посылку условий верификации.
- Лемму нужно тоже доказать.
- В *Why3* лемму надо оформить нужным образом и написать до целей – условий верификации.
- Посмотрите в *Why3IDE*, как лемма добавляется в посылку условия верификации.

Лемма в примере

- Составьте лемму, которая даст нужный терм для недоказанного условия верификации для пути START-A.
- Могут ли солверы доказать эту лемму?
- Могут ли солверы теперь доказать условие верификации?

Порядок лемм

- Одной этой леммы недостаточно. Нужны дополнительные леммы.
- Важен ли порядок лемм? Важен! Проведите соответствующий эксперимент с *Why3IDE*.
- Итак, для доказательства леммы используются леммы, которые расположены до нее. Это нужно использовать для доказательства лемм.
- Добавьте нужные леммы для доказательств в нашем примере.

Индукция и солверы

- Одна из лемм не доказывается («для любого неотрицательного числа существует целочисленный квадратный корень»). Почему?
- Для доказательства этой леммы нужен метод математической индукции. Солвер не может автоматически применять этот метод (он не сводится к инстанцированию кванторов). Как доказать лемму по индукции?

Леммы и пруверы

- Леммы бывают такими сложными (в них можно перенести всю сложность из условий верификации), что доказывать их из других лемм или сложно (сложно выписать нужные шаги доказательства леммы, если вообще возможно), или непредсказуемо (добавление лемм может привести к тому, что ранее доказывавшиеся леммы перестанут доказываться из-за возникновения новых лишних инстансов кванторов).
- Поэтому один из выходов – доказательство лемм при помощи пруверов (мы вручную указываем путь доказательства в прувере).
- Мы посмотрим, как все же можно как можно больше доказать при помощи солверов.

Содержание

1 Леммы

2 Ghost-блок-схемы

Вставка блок-схем

- Почему бы не вставить вызов дополнительной блок-схемы в нашу блок-схему? Эта блок-схема будет иметь спецификацию, ее постусловие будет вставлено в условие верификации базовых путей, на которых стоит этот вызов.
- Нам важно постусловие – оно будет вставлено в условие верификации. Это постусловие должно быть тем утверждением, которое необходимо для доказательства условия верификации.

Методы Флойда как метод доказательства утверждения

- Само постусловие тоже надо доказать (как и лемму). Дополнительная блок-схема будет что-то делать. Главное – что доказательство полной корректности этой блок-схемы относительно нужной спецификации методами Флойда будет доказательством утверждения-постусловия.
- Можно использовать всё, что может быть в блок-схемах: циклы, рекурсию. Получим... доказательство методом математической индукции!
- Эта идея называется auto-active verification.

Много ручной работы

- Предложите нужные блок-схемы и спецификации для завершения доказательства полной корректности примера с квадратным корнем.
- Докажите полную корректность всех блок-схем «на бумажке».
- Теперь надо доказать полную корректность в Why3. Надо выписать много условий верификации. Нам нужен инструмент автоматизации их построения.