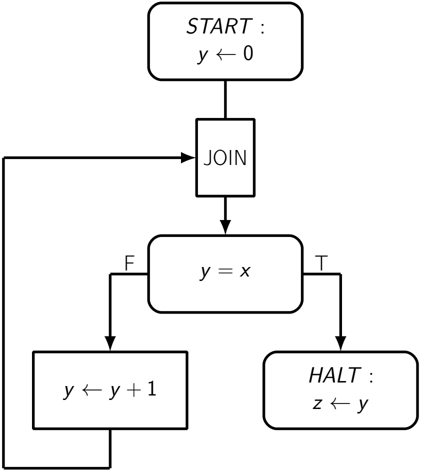
Лекция 3. Метод фундированных множеств Флойда

Цель лекции

Определить метод доказательства завершимости.

Содержание

Пример для доказательства



$D_x = \mathbb{Z}$
$D_y = \mathbb{Z}$
$D_z = \mathbb{Z}$
$\varphi(x) \geq 0$

Доказать, что блок-схема завершается при всех значениях входных переменных из указанного предусловия. Метод доказательства должен быть «автоматизируемым».

Поиск доказательства

Надо доказать, что все вычисления при входных переменных таких, что $\varphi(x)$, завершаются, т.е. достигают связки перед оператором HALT, т.е. что достигают конфигурации перед TEST, в которой истинен предикат в TEST.
Какие есть известные техники доказательства достижимости? Графы (из чего? из конфигураций). Из одной вершины есть дуга в другую вершину, если есть вычисление с этой парой конфигураций подряд. Предусловие дает некоторое подмножество вершин графа. Есть подмножество вершин - конфигураций перед TEST, в котороых истинен предикат в TEST. Надо доказать, что из каждой вершины одного множества существует путь в некоторую вершину второго множества. На графах применимы техники динамического программирования. Но здесь они не применимы из-за возможной бесконечности исходного множества и бесконечности графа.

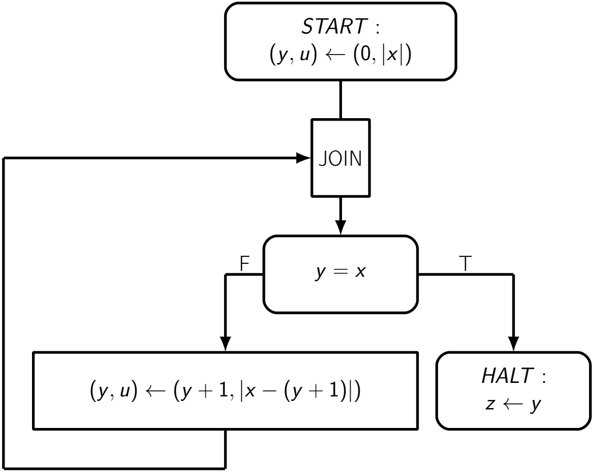
Поиск доказательства

Где еще встречалась достижимость в бесконечном случае? В принципе индукции. Там нужно сводить произвольные данные по переходам к базе. Если такая сводимость есть, то вместо доказательства бесконечного множества утверждений рассматривается доказательство конечного множества утверждений (про индуктивный переход и про базу).
Сводимость — то же, что и достижимость.
Итак, надо доказать возможность проведения индукции по путям из START в HALT. Мы пользовались этой индукцией при доказательстве частичной корректности - она предполагала завершаемость. Теперь надо обосновать, что индукцию можно было проводить.

Поиск доказательства

Весь вопрос в том, будет ли завершаться цепочка конфигураций с меткой оператора TEST в каждом вычислении, где выполнено $\varphi(x)$. Если при всех соответствующих значениях x можно сопоставить этой цепочке убывающую последовательность натуральных чисел, то возможность индукции по путям (т.е. завершаемость блок-схемы) будет доказана, т.е. не существует бесконечно убывающей последовательности натуральных чисел.
Попробуем добавить промежуточную переменную u, ее домен - $\{0, 1, 2, ...\}$, не влияющую на вычисление. По ходу вычисления эта переменная должна уменьшаться. Получится, что вычисление не может быть бесконечным, так как иначе переменная выйдет за границы домена.

Добавление убывающей переменной



Доказательство примера

Попробуем доказать, что переменная u уменьшается на каждой итерации цикла. То есть мы хотим доказать, что на всех вычислениях из x таких, что $x \geq 0$, в любых соседних конфигурациях связки между JOIN и TEST $u_{n+1} < u_n$. Для этого предварительно показываем по индукции, что каждый раз на этой связке выполнено индуктивное утверждение $x \geq y \wedge u = |x - y|$ (так же, как в предыдущей лекции).

База индукции. Путь из псевдосвязки перед START в связку перед TEST: $u_0 = |x|$ (из START). Получается: $\forall x \in \mathbb{Z} \cdot x \geq 0 \Rightarrow x \geq 0 \wedge |x| = |x - 0|$. Доказано.

Индуктивный переход. Путь из связки перед TEST в связку перед TEST. Надо доказать, что $\forall x, y, u \in \mathbb{Z} u \geq 0 \Rightarrow x \geq 0 \wedge y \neq x \wedge x \geq y \Rightarrow x \geq (y+1) \wedge |x - (y+1)| = |x - (y+1)|$. Это очевидно истинно. Доказано.

Значит, на всех вычислениях на связке перед оператором TEST выполнено утверждение $x \geq y \wedge u = |x - y|$.

Доказательство примера

Попробуем теперь доказать, что на каждом базовом пути из связки перед TEST в эту же связку переменная u уменьшается. Пусть $u = |x - y|$ выполнено вначале пути, $u' = |x - (y + 1)|$ выполнено в конце пути, причем имеется предикат пути $y \neq x$. Тогда надо доказать, что $\forall x \in \mathbb{Z}, y \in \mathbb{Z}, u \in \mathbb{Z} u \geq 0 \Rightarrow x \geq 0 \wedge y \neq x \wedge x \geq y \wedge u = |x - y| \Rightarrow |x - (y + 1)| < |x - y|$. Оно истинно. Доказано.

Значит, не может быть бесконечного вычисления, т.к. иначе переменная u выйдет за свой домен.

Упрощение доказательства

- Можно не добавлять u во все операторы START и ASSIGN, а ввести функцию от конфигурации, дающую те же значения переменной u.
- Можно ввести индуктивное утверждение и доказывать убывание u из этого индуктивного утверждения.
- Можно использовать другое множество значений переменной u. Главное - чтобы в нем не было бесконечно убывающей последовательности значений.
- Можно вместо этого домена переменной u рассматривать надмножество этого домена. Это упростит выкладки.

Содержание

Предварительные определения

Отношение строгого частичного порядка – это бинарное отношение $\prec$ на некотором множестве W, обладающее следующими свойствами:

1. антирефлексивность: $\forall x \in W \cdot \neg(x \prec x)$.
2. транзитивность: $\forall x, y, z \in W \cdot x \prec y \land y \prec z \Rightarrow x \prec z$.

Фундированное множество – множество, снабженное отношением строгого частичного порядка, в котором не существует бесконечно убывающей последовательности элементов.

Метод фундированных множеств

Шаг 1

Выбор множества т.с. (все циклические пути имеют т.с.) и фундированного множества $(W, \prec)$.

Шаг 2

Выбор индуктивного утверждения для каждой т.с., выписывание условий верификации для каждого базового пути между точками сечения и псевдосвязкой у START.

Шаг 3

Выбор оценочной функции для каждой точки сечения $(u_A : D_{\bar{x}} \times D_{\bar{y}} \to W', W \subseteq W')$.

Метод фундированных множеств (продолжение)

Шаг 4

Выписывание условия корректности оценочной функции для каждой точки сечения:
$\forall \bar{x} \in D_{\bar{x}}\ \forall \bar{y} \in D_{\bar{y}}\ \cdot\ \varphi(\bar{x}) \wedge p_A(\bar{x},\ \bar{y}) \Rightarrow u_A(\bar{x},\ \bar{y}) \in W.$

Шаг 5

Выписывание условия завершимости для каждого базового пути между точками сечения (из A в B):
$\forall \bar{x} \in D_{\bar{x}}\ \forall \bar{y} \in D_{\bar{y}}\ \cdot\ \varphi(\bar{x}) \wedge p_A(\bar{x},\ \bar{y})\ \wedge\ R_\alpha(\bar{x},\ \bar{y}) \Rightarrow$
$u_B(\bar{x},\ r_\alpha(\bar{x},\ \bar{y}))\ \prec\ u_A(\bar{x},\ \bar{y}).$

Корректность метода фундированных множеств

Теорема

Дана блок-схема P, спецификация $(\varphi,\ \psi)$. Если все составленные условия верификации, корректности и завершимости истинны, то $\langle\varphi\rangle\ P\ \langle T\rangle$, т.е. блок-схема завершима.

Схема доказательства: по индукции доказать выполнение индуктивных утверждений в точках сечения, из фундированности W сделать вывод об отсутствии бесконечных вычислений.

Примеры фундированных множеств

Натуральные числа

$W \equiv \{0, 1, 2, \ldots\}$ – множество целых неотрицательных чисел
$x \prec y \equiv x < y$ – с естественным порядком на нем

Кортежи

$W \equiv W_1 \times W_2$ – пара двух фундированных множеств $(W_1, \prec_1)$ и $(W_2, \prec_2)$.
$(x_1, x_2) \prec (y_1, y_2) \equiv x_1 \prec_1 y_1 \vee x_1 = y_1 \wedge x_2 \prec_2 y_2$ – лексикографический порядок.