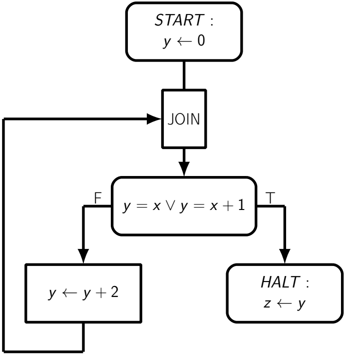
Лекция 3. Метод фундированных множеств Флойда

Цель лекции

Определить метод доказательства завершимости.

Содержание

Пример для доказательства



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

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

Поиск доказательства

Осознаем, что надо доказать: что все вычисления при значениях входных переменных таких, что $\varphi(x)$ (все нижеперечисленное эквивалентно друг другу):

- завершаются
- достигают связки перед оператором HALT
- содержат конфигурацию перед оператором TEST, в которой его предикат истинен. Если же такой конфигурации нет, то вычисление будет бесконечным.

Достижение чего-либо – это словно приближение. Если есть некоторое определение расстояния до чего-то, которое на каждом шаге уменьшается, то рано или поздно мы остановимся.

Поиск доказательства

Есть ли такое «расстояние» в нашем случае? Надо откуда-то догадаться, как можно определить расстояние. Например, так: $|x+1-y|$. Оно неотрицательно. Каждая конфигурация на связке перед оператором TEST с ложным предикатом на ней вынуждает выполнить итерацию цикла. Будет ли при этом уменьшаться расстояние – проверим при помощи формул. $\forall x, y \in \mathbb{Z}\ x \geq 0 \wedge y \neq x \wedge y \neq x+1 \Rightarrow |x+1-(y+2)| < |x+1-y|$. Это условие ложно. Строим контрпример: оно ложно при $y = 3, x = 1$. Но этот контрпример невозможен, т.к. он не соответствует оператору START. Как его учесть? Дополнительно доказать, что на каждой конфигурации перед TEST выполнено индуктивное утверждение $y \leq x+1$.

Индуктивное утверждение

Базовый путь из псевдосвязки перед START в точку сечения:
$\forall x \in \mathbb{Z}\ x \geq 0 \Rightarrow 0 \leq x + 1$
Базовый путь из точки сечения в точку сечения:
$\forall x, y \in \mathbb{Z}\ x \geq 0 \wedge y \neq x \wedge y \neq x + 1 \wedge y \leq x + 1 \Rightarrow y + 2 \leq x + 1$
Наконец, доказываем уменьшение расстояния: $\forall x, y \in \mathbb{Z}\ x \geq 0 \wedge y \neq x \wedge y \neq x + 1 \wedge y \leq x + 1 \Rightarrow |x + 1 - (y + 2)| < |x + 1 - y|$.

Доказательство

Итак, мы рассматривали конфигурации на связке перед оператором TEST (т.к. это точка сечения). Мы ввели «расстояние» от произвольной конфигурации этого множества до конфигурации, в которой истинен предикат в операторе TEST. Мы показали, что на всех путях между точками сечения (а такой путь один) расстояние уменьшается. То есть мы показали, что всякая конфигурация с ложными предикатом в TEST приводит к базовому пути, на котором расстояние уменьшается. Но т.к. расстояние неотрицательно, то оно не может уменьшаться бесконечно, значит в вычислении не могут бесконечно встречаться конфигурации, в которых предикат в операторе TEST ложен. Завершимость доказана.

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: $\forall x, y, z \in W \cdot x \prec y \wedge y \prec z \Rightarrow x \prec z$.

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.