Лекция 3. Метод фундированных множеств Флойда

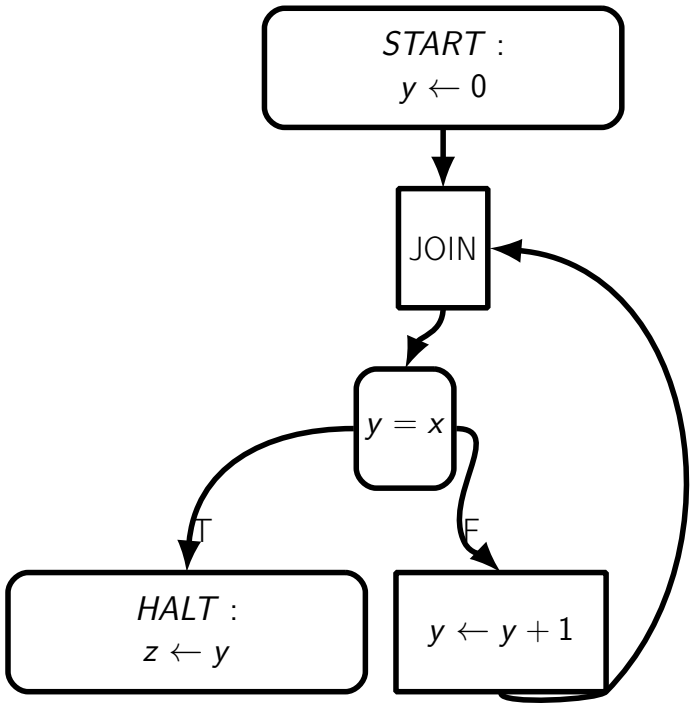
Цель лекции

Определить метод доказательства завершимости.

Содержание

Пример для доказательства

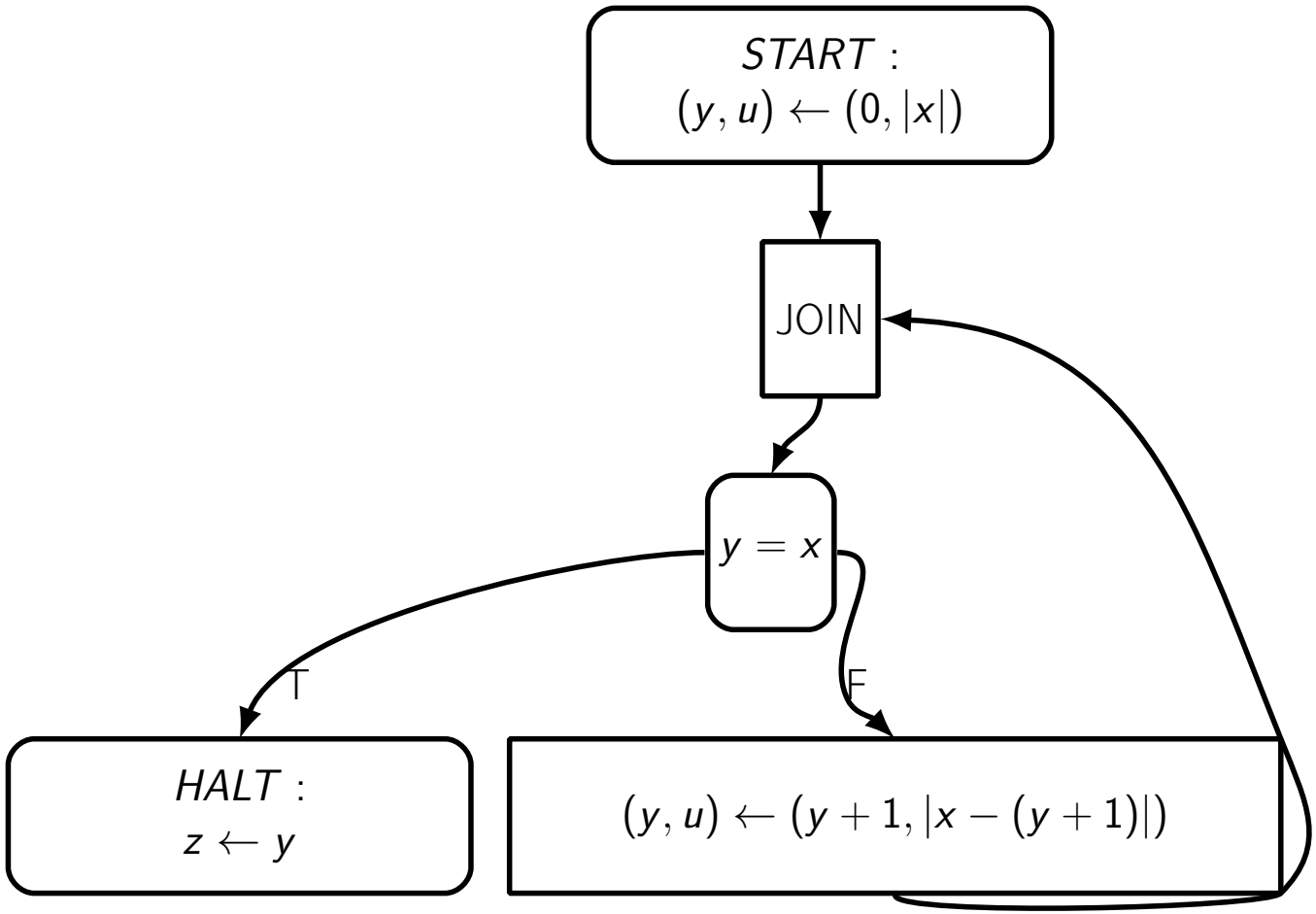
$D_x = D_y = D_z = \mathbb{Z}$. Доказать, что блок-схема завершается при всех значениях входных переменных таких, что выполнено $\varphi(x) \equiv x \geq 0$. Метод доказательства должен быть автоматизируемым.



Поиск доказательства

Надо доказать, что все вычисления из входных переменных таких, что $\varphi(x)$, завершаются, т.е. не являются бесконечными. Попробуем добавить еще одну промежуточную переменную u из ограниченного домена ($u \in \{0, 1, 2, ...\}$), чтобы на каждой итерации эта переменная уменьшалась (надо доказать, что эта переменная не выходит за границы домена). Получится, что вычисление не может быть бесконечным, так как иначе переменная выйдет за границы домена.

Поиск доказательства



Доказательство примера

Попробуем доказать по индукции, 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 $u_{n+1} < u_n$.

База индукции. Самые первые вхождения: $u_0 = |x|$ (из START), $u_1 = |x - 1|$ (после ASSIGN), причем $x \neq 0$. Получается: $\forall x \in \mathbb{Z} \cdot x \geq 0 \wedge x \neq 0 \Rightarrow |x - 1| < |x|$. Доказано.

Индуктивный переход. Пусть $u_n = |x - y_n|$, $u_{n+1} = |x - y_{n+1}|$, $y_{n+1} = y_n + 1$, $y_n \neq x$, тогда $u_{n+1} < u_n$. Тогда надо доказать, что если $y_{n+1} \neq x$, то $|x - (y_{n+1} + 1)| < |x - y_{n+1}|$. Когда истинно $|x - (y_n + 1)| < |x - y_n|$? Тогда и только тогда, когда $x \geq y_n + 1$. Но $x \neq y_n + 1$. Значит $x \geq y_n + 2$. Значит $|x - (y_n + 2)| < |x - (y_n + 1)|$. 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: $\forall x, y, z \in W \cdot x \prec y \wedge y \prec z \Rightarrow x \prec z$.

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.