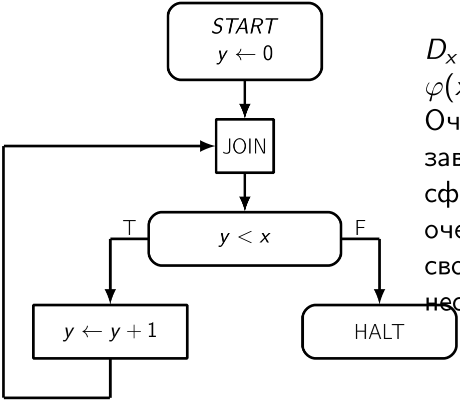
Лекция 3. Метод фундированных множеств Флойда

Цель лекции

Определить метод доказательства завершимости.

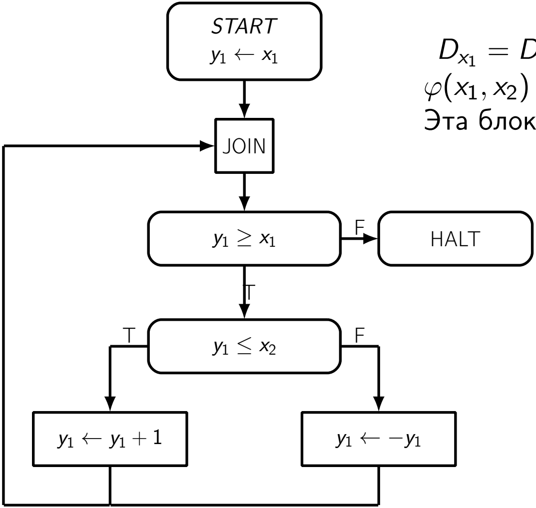
Содержание

Пример 1



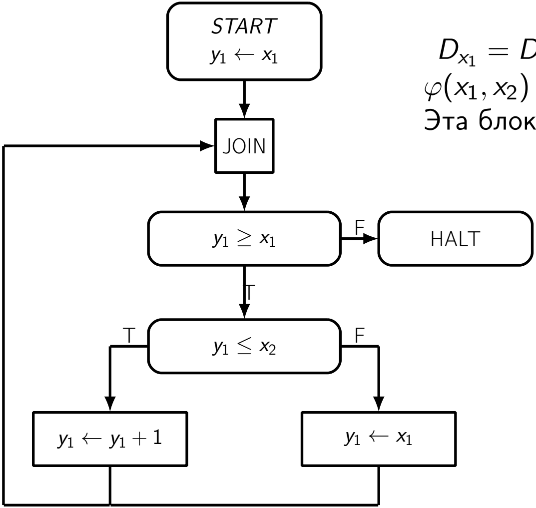
$D_x = D_y = \mathbb{Z}$
$\varphi(x) \equiv x > 0$
Очевидно, что эта блок-схема завершается? Постараемся сформулировать, почему это очевидно. Для этого сравним свой ответ на этот вопрос для нескольких блок-схем.

Пример 2



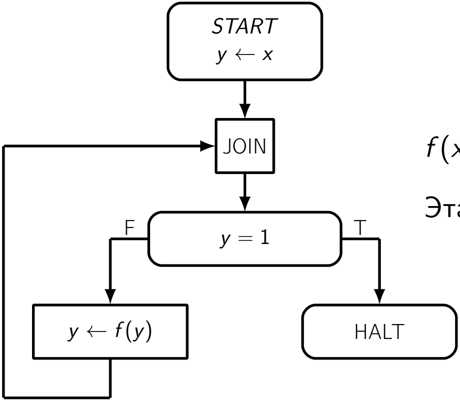
$D_{x_1} = D_{x_2} = D_{y_1} = \mathbb{Z}$
$\varphi(x_1, x_2) \equiv 0 \leq x_1 \leq x_2$
Эта блок-схема завершается?

Пример 3



$D_{x_1} = D_{x_2} = D_{y_1} = \mathbb{Z}$
$\varphi(x_1, x_2) \equiv 0 \leq x_1 \leq x_2$
Эта блок-схема завершается?

Пример 4



$$D_x = D_y = \mathbb{Z}$$
$$\varphi(x) \equiv x > 0$$
$$f(x) \equiv \begin{cases} x/2 & ,\, 2|x \\ 3x+1 & ,\, \neg(2|x) \end{cases}$$

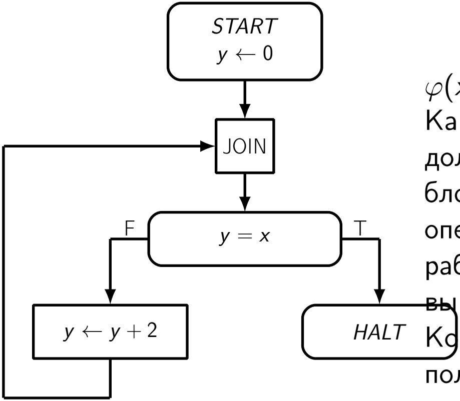
Эта блок-схема завершается?

Выводы из примеров

- Чтобы доказывать завершаемость, нужно иметь ответ на вопрос, почему блок-схема завершается.
- Направление мысли: завершение блок-схемы – значит «выполнение своей задачи полностью». «Завершимый процесс работы блок-схемы» – это постепенное выполнение задачи, приближение к ее полному выполнению.
- Что-то похожее для метода индуктивных утверждений: нужно иметь ответ на вопрос, почему блок-схема частично корректна, чтобы получить доказательство. Доказательство – это лишь подтверждение мысли, ее выражение в определенном виде.

Содержание

Пример для доказательства



$$D_x = D_y = \mathbb{Z}$$

$\varphi(x) \equiv x \geq 0 \wedge 2|x$

Какова «работа, которую должна выполнить блок-схема»? Каждый оператор «выполняет часть работы» и «приближает к выполнению полностью». Когда эта «работа выполнена полностью»? Формально доказать завершаемость блок-схемы на φ.

Поиск доказательства

- Чем больше значение переменной y, тем мы ближе к завершению, к выполнению «работы полностью».
- Математически: рассмотрим произвольное вычисление, отметим конфигурации перед оператором TEST, получили последовательность конфигураций.
- Обозначим y_i – последовательность значений переменной y в этой последовательности.
- Докажем, что последовательность y_i возрастает и ограничена сверху. Значит, она конечна.

Формулы

- Возрастание: $\forall i \cdot \; y_i + 2 > y_i$ – истинно
- Ограниченность (предполагаем, что верхняя граница равна $x + 1$): $\forall x \forall i \cdot x \geq 0 \wedge (2|x) \Rightarrow y_i \leq x$ – ложно! Контрпример: $x = 0$, $y_i = 2$. Но он невозможен. Не хватает дополнительного условия в посылке импликации: о том, что $y_i \leq x$.
- Можно ли доказать, что на каждой конфигурации перед TEST выполнено утверждение $y \leq x$?

Индуктивное утверждение

- Обозначим A – нашу точку сечения. Обозначим q – индуктивное утверждение. Составим условия верификации.
- Путь S-A (1): $\forall x \in \mathbb{Z}\ x \geq 0 \wedge (2|x) \Rightarrow q(x, 0)$
- Путь A-F-A (2):
$\forall x, y \in \mathbb{Z}\ x \geq 0 \wedge (2|x) \wedge q(x, y) \wedge y \neq x \Rightarrow q(x, y + 2)$
- (3) $\forall x, y \in \mathbb{Z}\ x \geq 0 \wedge (2|x) \wedge q(x, y) \Rightarrow y \leq x$
- Первая прикидка: $q(x, y) = (y \leq x)$. Но (2) не выполнено. Контрпример: $x = 2, y = 1$. Исправляем:
$q(x, y) = (y \leq x \wedge (2|y))$. Теперь все истинно!

Доказательство

Итак, мы рассматривали конфигурации на связке перед оператором TEST (т.к. это точка сечения). Мы доказали, что в каждой конфигурации в точке сечения истинно индуктивное утверждение $q(x, y) = (y \leq x \wedge (2|y))$. Оно позволяет доказать, что в этих конфигурациях значение переменной y не больше значения переменной x и строго возрастает в каждой следующей конфигурации вычисления. Значит, последовательность конфигураций не может быть бесконечной. 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. антисимметричность: $\forall x,\ y \in W \cdot x \prec y \Rightarrow \neg(y \prec x)$.
3. 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.