Лекция 4. Методы Флойда для блок-схем с вызовами других блок-схем

Цель лекции

Добавить в блок-схемы возможность вызвать другую блок-схему как подпрограмму. Определить методы Флойда для таких блок-схем.

Содержание

1 Синтаксис и семантика

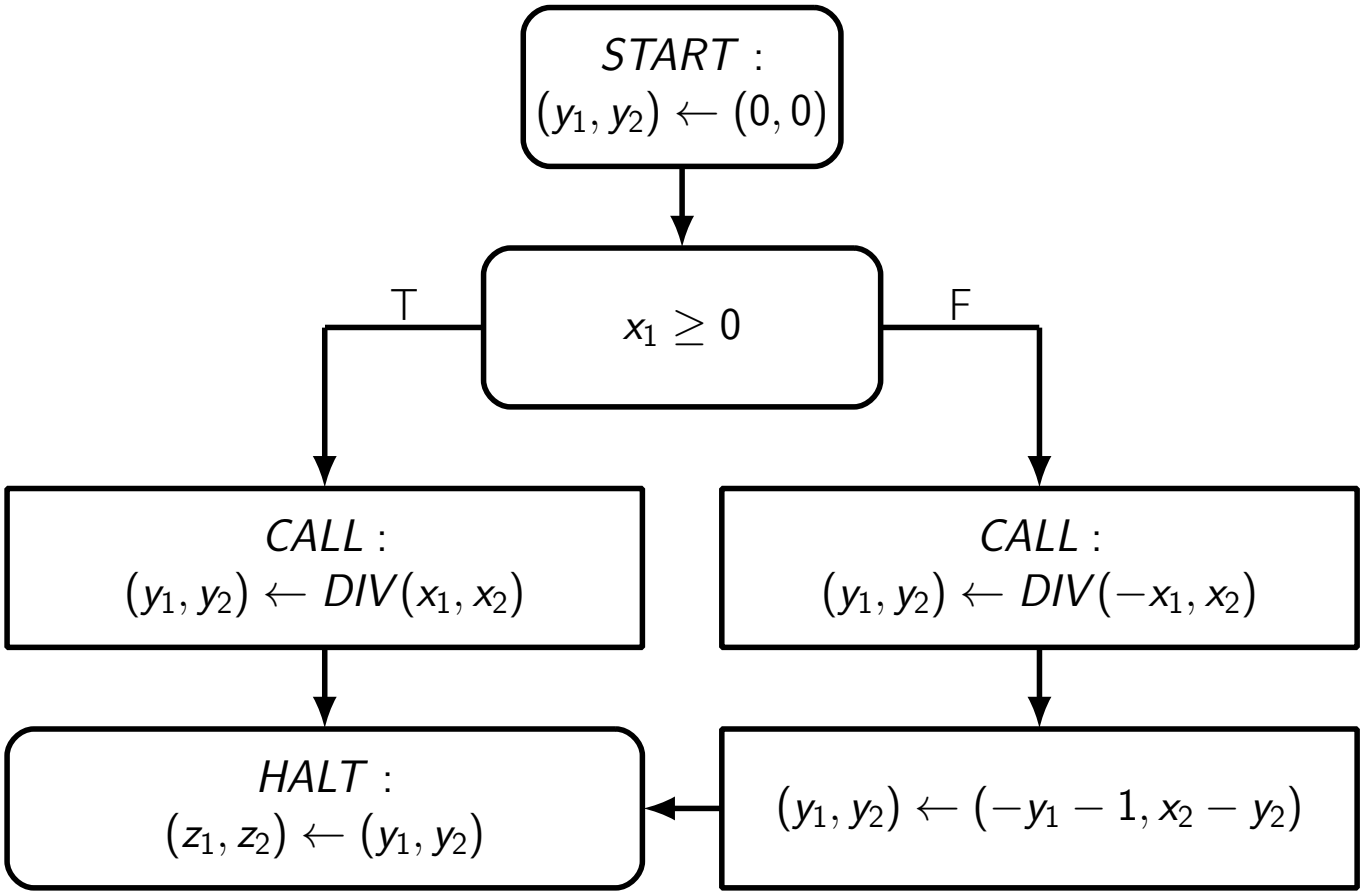
2 Полная корректность для нерекурсивного случая

3 Полная корректность для рекурсии

Подпрограммы в языках программирования

- подпрограмма – это модуль (белый ящик, черный ящик), заголовок, прототип, сигнатура, интерфейс и реализация
- процедурная абстракция – годится любая реализация вызываемой подпрограммы из определенного множества реализаций
- формальные и фактические параметры
- способы передачи параметров в функцию (по значению, по ссылке, по имени)
- требуется этап сборки программы из подпрограмм

Пример блок-схемы



$D_{x_1} = D_{x_2} = D_{y_1} = D_{y_2} = D_{z_1} = D_{z_2} = \mathbb{Z}$. Как определить функцию, вычисляемую этой блок-схемой?

Синтаксис и семантика

- оператор CALL, ему сопоставлена блок-схема, функция вычисления значений для входных переменных этой блок-схемы, функция для обработки значений выходных переменных этой блок-схемы
- корректно-определенная блок-схема: добавить совпадение входного и выходного домена этой блок-схемы с функциями, сопоставленными оператору CALL
- в конфигурацию надо добавить аналог «стека вызовов», можно представить вычисление в виде дерева конфигураций
- т.е. функция, вычисляемая блок-схемой, *зависит* от функции, вычисляемой вызываемыми блок-схемами

Пример функции, вычисляемой блок-схемой

$M[DIV](a_1,\ a_2) =$	$M[P](x_1,\ x_2) =$
$(0,\ 0)$	$\begin{cases}(0,\ 0) & , x_1 \geq 0 \\ (-1,\ x_2) & , x_1 < 0\end{cases}$
$\begin{cases}(0,\ 0) & , a_1 \geq 0 \\ (-1,\ a_2) & , a_1 < 0\end{cases}$	$\begin{cases}(0,\ 0) & , x_1 \geq 0 \\ (-1,\ x_2) & , x_1 < 0\end{cases}$
$\begin{cases}\omega & , a_1 \geq 0 \\ (0,0) & , a_1 < 0\end{cases}$	ω
$\begin{cases}(a_1\ /\ a_2,\ a_1\ \%\ a_2) & , a_1 \geq 0 \wedge a_2 > 0 \\ \omega & , \text{иначе}\end{cases}$	?

Модель требований для блок-схем с вызовами

не требует изменений по сравнению с блок-схемами без вызовов

Содержание

1 Синтаксис и семантика

2 Полная корректность для нерекурсивного случая

3 Полная корректность для рекурсии

Соотношения корректности: рекурсии пока нет

- Хотим модульности – доказательство корректности не надо переделывать при смене вызываемой блок-схемы, если она из «нужного» множества.
- Множество блок-схем, полностью корректных относительно некоторой спецификации, вот пример «нужного» множества
- Можно задать это множество при помощи пары предикатов – предусловия и постусловия (спецификации для оператора CALL)
- Блок-схема с вызовами полностью корректна относительно своей спецификации и спецификаций для операторов CALL, если для всех блок-схем, полностью корректных относительно спецификаций для операторов CALL, ... (далее определение полной корректности для блок-схем без вызовов)

Формулы для полной корректности

- Смотрим на наш пример с DIV. Пусть $(\varphi_D,\ \psi_D)$ – спецификация, сопоставленная блок-схеме DIV.
- Полная корректность = частичная корректность + завершаемость
- Завершаемость: если блок-схема DIV зацикливается, то зацикливается и P. Пробуем выразить определение полной корректности (завершаемости) без квантора по функциям, вычисляемым блок-схемами, которые сопоставлены DIV.
- Какова «самая зацикливающаяся» блок-схема, полностью корректная относительно $(\varphi_D,\ \psi_D)$? Та, которая зацикливается на всех входах, где ложно φ_D, и завершается на всех входах, где истинно φ_D.
- Значит, P завершается тогда, когда завершается DIV, т.е. входы DIV удовлетворяют φ_D.

Формулы для полной корректности

- Частичная корректность: если DIV завершилась, то ее выходные переменные удовлетворяют постусловию ψ_D. Надо доказать, что при всех таких значениях переменных вычисления будут приводить к HALT в блок-схеме P с теми переменными, которые удовлетворяют постусловию ψ.
- Квантор по функциям, вычисляемым блок-схемами, которые сопоставлены DIV, превращается в квантор по разным значениям выходных переменных DIV, удовлетворяющих постусловию ψ_D.

Формулы в примере

Получаются следующие формулы для доказательства полной корректности примера:

- завершаемость вызова DIV (путь START-T):
  $\forall x_1, x_2 \in \mathbb{Z} \cdot \varphi(x_1,\ x_2) \wedge x_1 \geq 0 \Rightarrow \varphi_D(x_1,\ x_2)$
- завершаемость вызова DIV (путь START-F):
  $\forall x_1, x_2 \in \mathbb{Z} \cdot \varphi(x_1,\ x_2) \wedge x_1 < 0 \Rightarrow \varphi_D(-x_1,\ x_2)$
- частичная корректность на пути (START-T-HALT):
  $\forall x_1, x_2 \in \mathbb{Z}\ \forall r_1, r_2 \in \mathbb{Z} \cdot \varphi(x_1,\ x_2) \wedge x_1 \geq$
  $0 \wedge \psi_D(x_1,\ x_2,\ r_1,\ r_2) \Rightarrow \psi(x_1,\ x_2,\ r_1,\ r_2)$
- частичная корректность на пути (START-F-HALT):
  $\forall x_1, x_2 \in \mathbb{Z}\ \forall r_1, r_2 \in \mathbb{Z} \cdot \varphi(x_1,\ x_2) \wedge x_1 <$
  $0 \wedge \psi_D(-x_1,\ x_2,\ r_1,\ r_2) \Rightarrow \psi(x_1,\ x_2,\ -r_1 - 1,\ x_2 - r_2)$

Формулы для блок-схем с циклами и вызовами

Составляем формулы по тому же принципу, но отсчитываем базовые пути не только от START, но и от каждой точки сечения.

Содержание

1 Синтаксис и семантика

2 Полная корректность для нерекурсивного случая

3 Полная корректность для рекурсии

Рекурсия

- Определение полной корректности такое же, как и для блок-схем без вызовов (не требуется выбирать «нужное» множество).
- Доказываем полную корректность по индукции по глубине рекурсии.
- Базовый случай: глубина рекурсии равна 0 (выход из рекурсии).
- Индуктивный переход: считаем, что доказали полную корректность на тех значениях входных переменных, которые приводят к глубине рекурсии не больше n. Тогда если все вызовы блок-схем такие, то можно сделать индуктивный переход – доказать полную корректность для множества значений входных переменных, приводящих к глубине рекурсии $n + 1$.

Завершаемость индукции

- Надо доказать, что все рекурсивные вызовы приводят к меньшей глубине рекурсии.
- Можно формализовать это правило при помощи фундированного множества и оценочной функции.
- Оценочная функция сопоставляется блок-схеме. Ее область определения – входной домен блок-схемы. Ее область значений – фундированное множество.

Формулы завершаемости

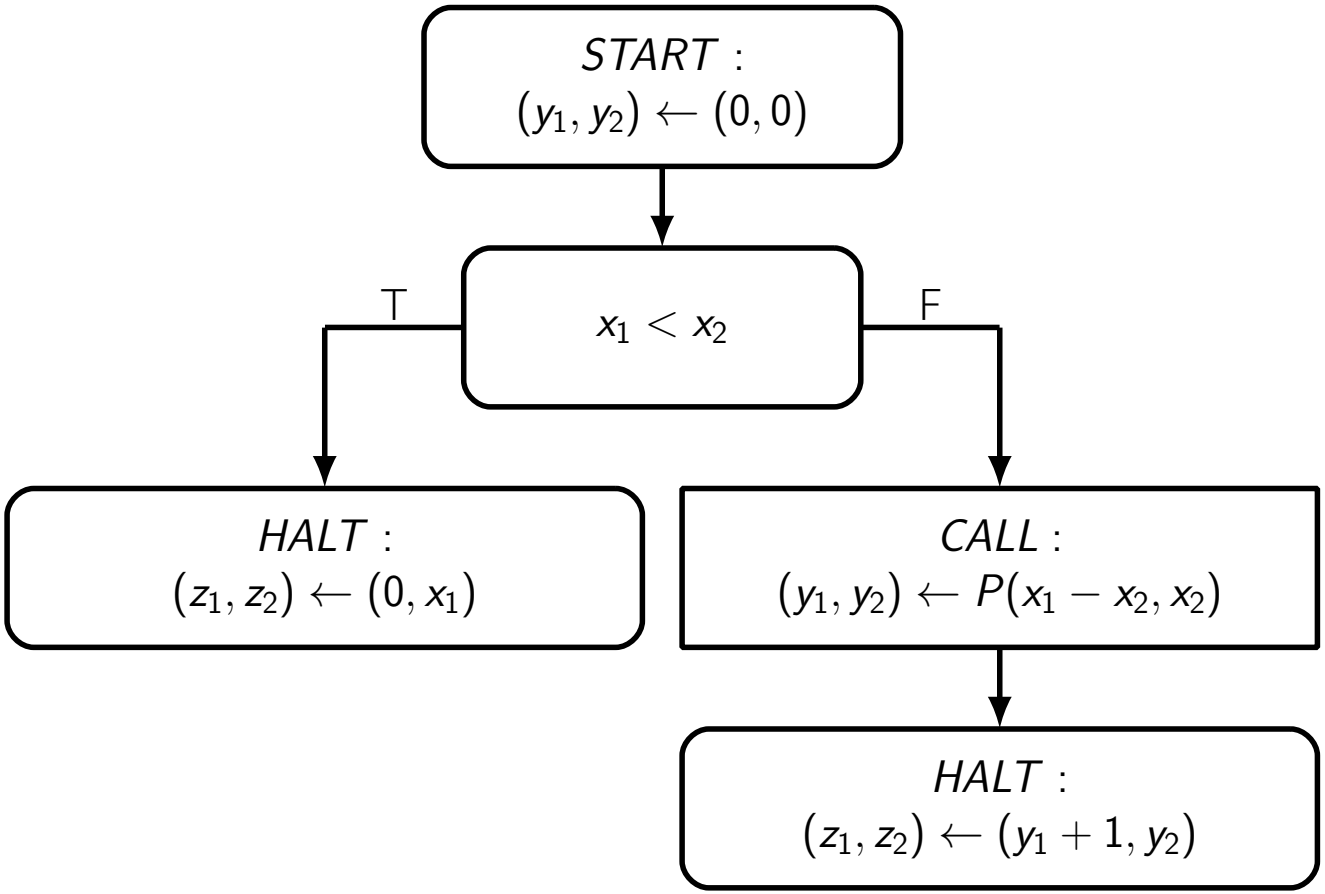
- Надо доказать фундированность множества.
- Надо доказать, что при всяком вызове блок-схемы с входными переменными, удовлетворяющими предусловию, значение оценочной функции принадлежит фундированному множеству.
- Надо доказать, что при всяком базовом пути, приводящем к рекурсивному вызову, оценочная функция на входных переменных вызываемой блок-схемы меньше оценочной функции на входных переменных вызывающей блок-схемы.

Формулы полной корректности

- Как только доказана завершаемость индукции, ее можно применять для доказательства частичной корректности и завершаемости блок-схемы.
- Каждому вектору значений входных переменных соответствует своя глубина рекурсии. Доказываем частичную корректность и завершаемость индукцией по глубине рекурсии, т.е. постепенно увеличивая множество значений входных переменных.
- Для этого применяем формулы из доказательства полной корректности для нерекурсивного случая, сопоставив вызываемым блок-схемам спецификацию вызывающей блок-схемы.

Пример

Вычисление частного и остатка при делении



$$D_{x_1} = D_{x_2} = D_{y_1} = D_{y_2} = D_{z_1} = D_{z_2} = \mathbb{Z}.$$

Пример::схема доказательства

1. Надо доказать полную корректность блок-схемы P относительно спецификации: $\varphi(x_1,\ x_2) = x_1 \geq 0 \wedge x_2 > 0$, $\psi(x_1,\ x_2,\ z_1,\ z_2) = (x_1 = z_1 * x_2 + z_2 \wedge 0 \leq z_2 < x_2)$.
2. Доказываем возможность индукции по глубине рекурсии: берем фундированное множество $(\{0, 1, 2, ...\}, <)$. Его фундированность была доказана ранее. Берем оценочную функцию $u(x_1,\ x_2) = x_1$, индуктивное утверждение совпадает с φ.
3. Составляем условия верификации.

Пример::условия верификации

Доказываем возможность рассуждать по индукции:

- корректность индуктивного утверждения:
  $\forall x_1,\ x_2 \in \mathbb{Z} \cdot \varphi(x_1,\ x_2) \wedge x_1 \geq x_2 \Rightarrow \varphi(x_1 - x_2,\ x_2)$
- корректность оценочной функции:
  $\forall x_1,\ x_2 \in \mathbb{Z} \cdot \varphi(x_1,\ x_2) \Rightarrow u(x_1,\ x_2) \geq 0$
- завершаемость индукции:
  $\forall x_1,\ x_2 \in \mathbb{Z} \cdot \varphi(x_1,\ x_2) \wedge x_1 \geq x_2 \Rightarrow u(x_1 - x_2,\ x_2) < u(x_1,\ x_2)$

Теперь доказываем индукцией по глубине рекурсии, в ней будут применяться следующие условия верификации:

- частичная корректность (путь START-T-HALT):
  $\forall x_1,\ x_2 \in \mathbb{Z} \cdot \varphi(x_1,\ x_2) \wedge x_1 < x_2 \Rightarrow \psi(x_1,\ x_2,\ 0,\ x_1)$
- частичная корректность (путь START-F-HALT):
  $\forall x_1,\ x_2,\ y_1,\ y_2 \in \mathbb{Z} \cdot \varphi(x_1,\ x_2) \wedge x_1 \geq$
  $x_2 \wedge \psi(x_1 - x_2,\ x_2,\ y_1,\ y_2) \Rightarrow \psi(x_1,\ x_2,\ y_1 + 1,\ y_2)$
- завершаемость не требует доказательства, т.к. нет циклов

Подставляем формулы

- корректность индуктивного утверждения:
  $\forall x_1,\ x_2 \in \mathbb{Z} \cdot x_1 \geq 0 \wedge x_2 > 0 \wedge x_1 \geq x_2 \Rightarrow x_1 - x_2 \geq 0 \wedge x_2 > 0$
- корректность оценочной функции:
  $\forall x_1,\ x_2 \in \mathbb{Z} \cdot x_1 \geq 0 \wedge x_2 > 0 \Rightarrow x_1 \geq 0$
- завершаемость индукции:
  $\forall x_1,\ x_2 \in \mathbb{Z} \cdot x_1 \geq 0 \wedge x_2 > 0 \wedge x_1 \geq x_2 \Rightarrow x_1 - x_2 < x_1$
- частичная корректность (путь START-T-HALT): $\forall x_1,\ x_2 \in \mathbb{Z} \cdot x_1 \geq 0 \wedge x_2 > 0 \wedge x_1 < x_2 \Rightarrow x_1 = x_1 + 0 * x_2 \wedge 0 \leq x_1 < x_2$
- частичная корректность (путь START-F-HALT):
  $\forall x_1,\ x_2,\ y_1,\ y_2 \in \mathbb{Z} \cdot x_1 \geq 0 \wedge x_2 > 0 \wedge x_1 \geq x_2 \wedge x_1 - x_2 = x_2 * y_1 + y_2 \wedge 0 \leq y_2 < x_2 \Rightarrow x_1 = x_2 * (y_1 + 1) + y_2 \wedge 0 \leq y_2 < x_2$