Лекция 4. Расширение моделей

Цель лекции

Расширить модель программы и модель требований, чтобы приблизить их к Си-программам и требованиям к ним.

Содержание

Процедурная абстракция

«Процедура – как черный ящик, в котором скрыт алгоритм за заголовком процедуры. При этом задача, которую должна решать процедура, должна быть известна. Вызывая процедуру, неизвестно, какой из алгоритмов будет в ней. Но в любом случае этот алгоритм должен решать задачу.»

Правила программного контракта

1. при каждом вызове процедуры ее фактические параметры должны удовлетворять предусловию процедуры.
2. при каждом возврате из процедуры ее возвращаемое значение удовлетворяет постусловию процедуры.

Первое должна обеспечить вызывающая процедура (вызываемая процедура пользуется этим), второе – вызываемая процедура (вызывающая процедура этим пользуется).

Новый оператор CALL

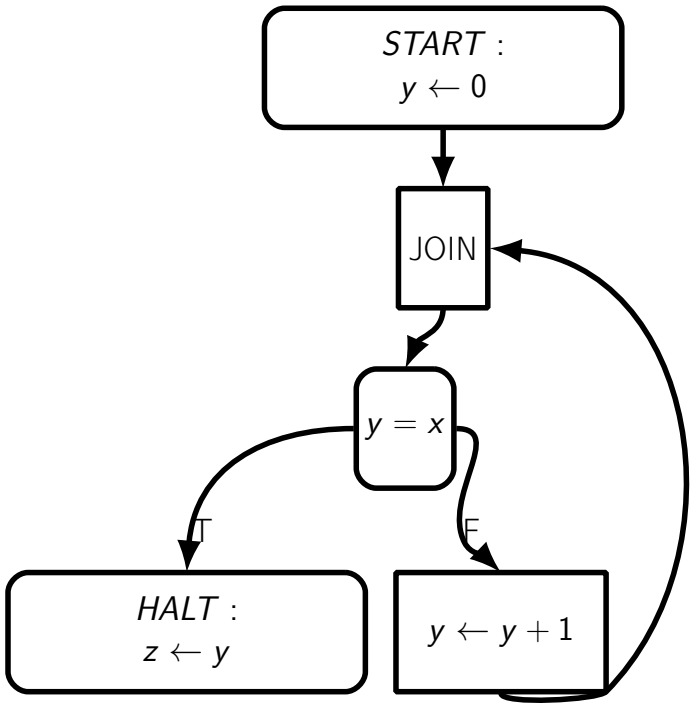
Оператор CALL означает вызов процедуры. Ему приписана имя вызываемой процедуры, функция получения вектора значений входных переменных вызываемой процедуры, функция обработки вектора значений выходных переменных в значения промежуточных переменных вызывающей процедуры.
Семантика: вычисление продолжается в вызванную процедуру с поддержкой стека вызовов.
Предикат пути и функция пути, если в пути встречаются операторы CALL, получают по 1 дополнительному аргументу для каждого возвращаемого значения операторов CALL в этом пути. Предикат пути дополняется постусловиями для каждого оператора CALL.

Пример доказательства

TBD

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.



Доказательство частичной корректности

Те же шаги метода индуктивных утверждений. Измененные предикат пути и формула пути.

Доказательство полной корректности

Надо добавить условия корректности вызова процедуры.

Шаг 6

Выписывание условия корректности вызова процедуры для каждого базового пути между точкой сечения и псевдоточкой в оператор CALL ($r_1,\ r_2,\ ...,\ r_N$ — дополнительные переменные для значений выходных переменных для операторов CALL внутри пути, $D_{r_1},\ D_{r_2},\ ...,\ D_{r_N}$ – выходные домены в операторах CALL, φ' — предусловие оператора CALL в конце пути, arg — функция построения входных переменных оператора CALL в конце пути): $\forall \bar{x} \in D_{\bar{x}}\ \forall \bar{y} \in D_{\bar{y}}\ r_1 \in D_{r_1}\ ...\cdot\ \varphi(\bar{x}) \wedge p_A(\bar{x},\ \bar{y})\ \wedge\ R_\alpha(\bar{x},\ \bar{y},\ r_1,\ r_2,\ ...,\ r_N) \Rightarrow \varphi'(arg(\bar{x},\ r_\alpha(\bar{x},\ \bar{y},\ r_1,\ r_2,\ ..., r_N)))$.

Рекурсия

TBD

Содержание

TBD