Дедуктивная верификация предикатных программ

Чушкин Михаил Сергеевич
Новосибирский государственный университет (Новосибирск), Россия
e-mail: chushkinm@rambler.ru

В данной работе рассматривается класс программ, решающих задачи вычислительной и дискретной математики. Для реализации подобных программ лабораторией системного программирования ИСИ был разработан язык предикатного программирования P.

Программа на языке P представляет собой набор определений предикатов. Определение предиката имеет вид:

A(x: y) **pre** P(x) { S(x: y) } **post** Q(x, y),

где A – имя определяемого предиката, x – аргументы, y – результаты, S(x: y) – оператор, P(x) – предусловие, истинное перед исполнением и Q(x, y) – постусловие, истинное после исполнения.

Большинство работ по дедуктивной верификации базируется на логике Хоара. Описываемый метод дедуктивной верификации предикатных программ отличается от метода Хоара и других подходов. Ключевым является понятие *логики оператора*. Логика оператора - предикат (логическое утверждение), зависящий от значений переменных оператора. Он определяет логику действий оператора и является его точным эквивалентом.

Тотальная корректность программы определяется следующим утверждением [1]:

$ P(x) \Rightarrow [L(S(x:)) \Rightarrow Q(x,)] \land \exists y L(S(x:)) $

Используя это условие можно автоматически построить условие корректности для программы, однако оно будет длинным и сложным, даже для коротких программ. Специализация условия тотальной корректности для разных видов операторов определяет систему правил вывода. [2]

Используемые в данной работе правила точнее, чем соответствующие правила Хоара. Последовательный оператор разделен на оператор суперпозиции и параллельный оператор. Нет циклов, вместо них используются рекурсивные процедуры. Для доказательства завершаемости рекурсивных программ используется функция меры, которая строится на порядок проще, чем инвариант цикла. Указателей нет, вместо них используются алгебраические типы. Формируемый набор условий корректности в целом проще и лучше структурирован, чем аналогичный набор, получаемый методом Хоара. Однако автоматическое доказательство условий корректности остается чрезвычайно трудоемким и сложным.

В рамках работы реализован генератор условий корректности в системе предикатного программирования. Генератор позволяет автоматически формировать условия корректности для программ с исходным кодом на языке P. Реализован транслятор, позволяющий автоматически переносить полученные условия корректности на язык спецификаций системы PVS.

Список литературы:

[1] *Карнаухов Н.С., Першин Д.Ю., Шелехов В.И.* Язык предикатного программирования P. Новосибирск, 2010. 42с. (Препр. / ИСИ СО РАН; N 153).

Шелехов В.И. Методы доказательства корректности программ с хорошей логикой // Современные проблемы математики, информатики и биоинформатики. ? 2011. ? 17с. http://conf.nsc.ru/files/conferences/Lyap-100/fulltext/74974/75473/Shelekhov_prlogic.pdf

Работа выполнялась в рамках гранта РФФИ № 12-01-00686.