Применение логики программы для спецификации и верификации реактивных систем

Тумуров Эрдэм Гармаевич
Институт систем информатики имени А.П. Ершова СО РАН (Новосибирск), Россия
e-mail: erdemus@gmail.com

Цель настоящей работы – расширить понятие логики программы для представительного подкласса программ – реактивных систем.

В работе [1] определено понятие логики для программ, невзаимодействующих с внешним окружением программы. Логика такой программы – предикат (логическое утверждение), определяющий логику решения задачи и являющийся точным эквивалентом программы. Эффективно и просто строится логика императивных и функциональных программ для различных выражений, операторов и типов, за исключением указателей. На базе логики программы определена формула тотальной корректности программы относительно спецификации в виде предусловия и постусловия. Разработана система правил доказательства корректности программ для различных операторов, а также разработан метод дедуктивной верификации предикатных [2] программ, имеющий преимущества по сравнению с классическим методом Хоара [3].

Для реактивной системы логика программы – набор предикатов на переменных состояния системы. Предикат из этого набора истинен после исполнения некоторой очередной акции трассы, составленной перемешиванием акций параллельных взаимодействующих процессов. Акция – максимальный фрагмент кода программы процесса (без циклов внутри), для которого логика легко строится. Содержательное описание алгоритма функционирования реактивной системы формализуется в виде спецификации, представленной машиной мета-состояний, как аппроксимации логики программы на множестве трасс.

Разрабатываемый аппарат ориентирован на разработку, тестирование, моделирование и верификацию программной и аппаратной части встроенных систем аэрокосмической отрасли, энергетики, медицины и др. приложений, где необходима предельная надежность систем.

Литература

[1] Шелехов В.И. Логика невзаимодействующих программ // 4-я Российская школа-семинар "Синтаксис и семантика логических систем". – 2012.

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

[3] Hoare C. A. R. An axiomatic basis for computer programming // Comm. of the ACM. 1969. Vol. 12 (10). P. 576-585.

Работа выполнена при поддержке РФФИ, проект 12-01-00686.