Автоматизация дедуктивной верификации С-программ без использования инвариантов циклов

Кондратьев Дмитрий
(ИСИ СО РАН)

В Институте систем информатики им. А.П. Ершова СО РАН разработан комплексный подход к автоматизации дедуктивной верификации программ на языке С. Ошибкой в программе является несоответствие программы и ее спецификации. Традиционным методом проверки программ на наличие ошибок является тестирование. Но тестирование не может гарантировать отсутствие ошибок в программе. Эту проблему можно решить, используя дедуктивную верификацию. Дедуктивная верификация принимает на вход программу и ее формальные спецификации, такие как предусловие, постусловие и инварианты циклов. Инвариантом цикла является утверждение, которое истинно перед исполнением цикла, истинно для каждой итерации цикла и обеспечивает корректность на выходе из цикла. В ходе дедуктивной верификации из программы и ее формальных спецификаций выводятся логические формулы, называемые условиям корректности программы. Условия корректности представляют собой утверждения о том, что программа соответствует спецификациям. Истинность условий корректности проверяют программные системы для доказательства теорем. Автоматизация дедуктивной верификации программ на языке С является актуальной задачей современного программирования. Для ее решения необходимо автоматизировать решение проблемы задания инвариантов циклов, доказательство условий корректности и локализацию ошибок в случае их наличия. Для решения этих проблем был разработан комплексный подход, реализованный в системе *C-lightVer*. Данный подход включает символический метод верификации финитных итераций для элиминации инвариантов циклов, стратегии доказательства условий корректности и метод локализации ошибок. Символический метод верификации финитных итераций основан на замене действий циклов определенного вида применением специальной рекурсивной функции *rep*. Стратегии доказательства основаны на структуре условий корректности, структуре программы и свойствах функции *rep*. Метод локализации ошибок основан на генерации отчета о соответствии условий корректности и фрагментов программы, и на проверке выполнения свойств циклов, которые могут означать наличие ошибок.