

Обеспечение надежности как важнейшего качества программ неизменно остается ключевым направлением развития современной методологии программирования. Широкое распространение микропроцессоров в системах управления, а также наметившаяся тенденция слияния программного и аппаратного обеспечения вычислительных систем (аппаратная реализация функций операционных систем, кремниевые компиляторы и др.) еще более повышают требования к надежности многих классов прикладных и системных программ.

В то же время прогресс в методах обеспечения надежности программ остается явно недостаточным. Традиционный способ обеспечения надежности программ путем тестирования не может полностью удовлетворить возрастающие требования практики. Качественно новый уровень в решении этой проблемы может быть достигнут сочетанием методов тестирования и верификации программ.

В общем случае верификация есть подтверждение (установление) корректности программы (отсутствия ошибок в программе) и может рассматриваться как дальнейшее развитие идей тестирования в новом аспекте. Если тестирование ограничено исследованием отдельных выполнений программы (для некоторых путей вычислений), то верификация — анализ свойств всех допустимых выполнений программы с помощью формальных доказательств присутствия требуемых свойств.

Эти новые мощные возможности не могут быть получены даром — они требуют развития соответствующего формального аппарата, которым необходимо овладеть разработчикам программ. Известно, что новые формализмы всегда страшат, и необходимы усилия и время для их восприятия. Уместно, однако, здесь вспомнить, что формализмы языков программирования также относительно недавно были новыми для многих. Тем не менее они были успешно освоены как инженерами, так и математиками, из которых сформировались специалисты новой профессии — программисты.

Аналогичная ситуация складывается сейчас в прикладной логике, являющейся фундаментом ряда прогрессивных идей в современной методологии программирования, к которым относится и верификация программ. Овладение формальным языком логики и методами формальных доказательств становится существенным элементом технологии качественной разработки программ.

Основная идея верификации программы состоит в том, чтобы формально доказать соответствие между текстом программы (на языке программирования) и спецификацией задачи (на языке спецификации). Программа и спецификация по сути описывают одну