XXXII Неделя науки СПбГПУ. Материалы межвузовской научно-технической конференции. Ч.V : С.9-10

УДК 681.3.06

П.Д.Дробинцев (асп., каф. ИУС), В.П.Котляров, к.т.н., проф.

ТЕХНОЛОГИИ АВТОМАТИЗИРОВАННОЙ ВЕРИФИКАЦИИ ФУНКЦИОНАЛЬНЫХ СПЕЦИФИКАЦИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Технологии автоматизированной верификации функциональных спецификаций в настоящее время применяются всё чаще в процессе производства программного обеспечения, что позволяет наряду с увеличением качества продукта уменьшить затраты на его производство.

Сегодня основным механизмом обеспечения требуемого качества программ является тестирование, которое в силу возросшей сложности и большого количества функциональных свойств программного обеспечения уже не может выступать единственным гарантом качества. Проблема современного тестирования заключается в необходимости исполнения огромного количества тестов на готовом продукте. Верификация в свою очередь позволяет доказать правильность программного обеспечения без непосредственного исполнения, а верификация функциональных спецификаций даёт возможность производить доказательство уже на этапе создания требований. При этом требования должны быть записаны на формальном языке. В работе рассмотрены возможности верификации требований представленных в нотации MSC (Message Sequence Chart).

Язык MSC даёт возможность описания взаимодействия системы с окружением в виде диаграмм (протоколов), посредством описания последовательности сообщений. Такая запись спецификаций позволяет проводить следующие виды верификации:

- временная верификация;
- верификация на основании базовых протоколов.

Временная верификация даёт возможность проверки соответствия формального графического описания системы и математического. При этом математическое описание также проводится в нотации языка MSC в виде указания абсолютных, относительных времён наступления событий, а также временных интервалов и таймеров.

Наиболее интересным видом верификации является верификация на основе базовых протоколов. При разработке требований на систему каждое требование записывается в виде отдельной MSC диаграммы, представляющей собой минимальный набор событий, переводящих систему из одного состояния в другое. На диаграмме также отмечаются состояния системы до и после перехода, эти состояния записываются в виде логических выражений. Таким образом, все функциональные требования заключаются в набор простых диаграмм (элементарных протоколов). В дальнейшем на этапе определения требований более высокого уровня создаются диаграммы, содержащие сценарии поведения с добавленными аннотациями, представляющими собой логические выражения над переменными, определяющими состояния системы. На этапе верификации производится проверка возможности выполнения сценария поведения системы на основе требований записанных в элементарных протоколах. Другими словами, происходит поиск подмножества протоколов, которое позволяет пройти весь сценарий. Также проверяется выполнимость аннотаций, что даёт возможность проверки переменных системы в любой точке исполнения сценария.

Вторым возможным вариантом использования элементарных протоколов является генерация трасс (линейных тестов) для системы. При данном подходе производится

генерация трасс, состоящих из последовательности элементарных протоколов, применённых в соответствии с информацией о состояниях системы. Также производится доказательство полноты покрытия функциональных требований на систему с полученными трассами. В реальной практике количество получаемых трасс очень велико, и это не позволяет использовать их для тестирования; в этом случае актуальным становится ограничение количества трасс с использованием различных критериев.

Таким образом, при записи функциональных спецификаций на формальных языках существует множество возможностей для верификации, и основной проблемой становится непосредственно сама запись спецификации и соблюдение выбранной стратегии верификации впоследствии. Применение описанных технологий в области телекоммуникаций позволило сократить затраты на качество программного продукта на 25–28%, уменьшить время тестового цикла в 1,5 раза и обеспечить 100% покрытие тестами функциональных спецификаций системы.