

МЕТОД ПЕРЕИСПОЛЬЗОВАНИЯ АБСТРАКЦИЙ В СТАТИЧЕСКОМ АНАЛИЗЕ ДЛЯ ПОИСКА СОСТОЯНИЙ ГОНКИ

Карпов Максим Евгеньвич

Студент

Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия

E-mail: me@m-k.mx

Научный руководитель — К.ф.-м.н.

Хорошилов Алексей Владимирович

Контроль качества — важный этап жизненного цикла разработки ПО. Для его обеспечения создано множество подходов: инспекция кода, тестирование, статический анализ и др. Из них формальная верификация, как разновидность статического анализа, дает самые сильные гарантии, но и требует больше всего ресурсов: как человеческих, так и вычислительных.

В основе подходов проверки моделей лежит исследование множества достижимых состояний программы и проверка на нём заданных свойств. Так как в реальных программах количество состояний может быть огромным, применяются абстракции, делящие пространства состояний на классы эквивалентности, в которых опущены несущественные для анализа детали.

В ИСП РАН разрабатывается инструмент SPALockator[1] на основе фреймворка для статической верификации SPAChecker. Новшество SPALockator — существенно улучшенная абстракция чередования потоков, которая избегает комбинаторного взрыва состояний. Однако, оно сделало неприменимым имеющийся механизм переиспользования абстракций, который ускорял анализ повторяющихся фрагментов кода.

В работе представлен альтернативный метод переиспользования абстракций, совместимый с изменениями в SPALockator. Разработанная реализация сохраняет многопоточную семантику программы и позволяет эффективно переиспользовать результаты анализа повторяющихся частей. Реализация была протестирована на параллельных программах из набора SV-COMP.

Литература

1. Andrianov P.S. Analysis of correct synchronization of operating system components. Proceedings of the Institute for System Programming, vol. 31, issue 5, 2019, pp. 203-232