## Міністерство освіти і науки України

## Запорізький національний технічний університет

кафедра програмних засобів

# реферат

з дисципліни «Якість програмного забезпечення» на тему:

# «статистичні методи верифікації. Обмежена перевірка моделей bmc»

Виконав:

студент групи КНТ-115 Л.І. Кулик

Прийняла:

проф., д.т.н Г.В.Табунщик

2018

**ВСТУП**

В останні роки такий метод забезпечення якості програмного забезпечення (ПЗ), як обмежена перевірка моделей (Bounded Model Checking, BMC), досліджується все більш і більш активно, оскільки він дозволяє успішно виявляти як функціональні, так і нефункціональні дефекти в реальному ПО.

Для пошуку помилок в методі перевірки моделей використовується розгляд повного простору станів заданої програми з метою пошуку станів, які порушують ті чи інші властивості коректності (наприклад, витоку пам'яті або порушення формальної специфікації).

**Метод обмежуваної перевірки моделей**

Метод обмежуваної перевірки моделей (від англ. BMC, Bounded Model Checking) - це одна з найбільш часто вживаних формальних технік при розробці напівпровідникових пристроїв. Метод зобов'язаний своїм успіхом великим можливостям SAT вирішувачів. Він був запропонований в 1999 як допоміжний для необмеженого методу перевірки моделей на основі BDD.

Цей метод заснований на розгортанні графа станів програми на кінцеве число кроків. На кожному етапі перевіряється, чи може специфікація бути порушена не більше, ніж за поточне обране число кроків. Якщо порушення не виявлено, виконується перевірка умов розгортання (від англ. «Unwinding assertions»), таких як умови в заголовках циклів, для того, щоб виключити подальше розгортання графа по нездійсненним шляхах. Така перевірка може показати, що подальше збільшення числа кроків безглуздо, тому що жодна з умов розгортання не виконана. Це доводить коректність вихідної програми. В іншому випадку, число кроків збільшують і перевірку повторюють до тих пір, поки не виявлять порушення специфікації, або не вийдуть за межі вказаного максимального числа кроків. Перевірка коректності розгорнутого фрагмента графа станів зазвичай має на увазі кодування умови порушення специфікації у вигляді завдання для вирішувача.

В якості оптимізацій застосовуються окреме розкриття циклів і обчислення порога повноти (від англ. «completeness threshold»).

У BMC, як правило, використовуються вирішувачі, що підтримують бітову арифметику.

BMC - це найкращий метод для знаходження поверхневих помилок, надає повну трасу контрприклада в разі їх виявлення. Інструментам, які реалізують цей метод, як правило, властива висока точність аналізу. Вони підтримують найширший набір конструкцій в програмі, включаючи динамічно виділяємі структури в пам'яті, операції з масивами, використання арифметики покажчиків, бітові операції над числами, обмеженість розмірів цілочисельних типів даних (наприклад, перелічуваних) та інші, не вимагаючи при цьому вбудованого знання про структурах даних в програмі. З іншого боку, доказ відсутності помилок гарантується тільки для простих програм, тобто програм без глибоких циклів.

# ПЕРЕЛІК ПОСИЛАНЬ

1. Обнаружение дефектов в программном обеспечении путем объединения ограниченной проверки моделей и аппроксимации функций­: [Електронний ресурс] ­­­– режим доступу: http://docplayer.ru/370182-Obnaruzhenie-defektov-v-programmnom-obespechenii-putem-obedineniya-ogranichennoy-proverki-modeley-i-approksimacii-funkciy-1.html
2. Bounded Model Checking­: [Електронний ресурс] ­­­– режим доступу: https://satassociation.org/articles/FAIA185-0457.pdf