平成30年度 情報工学コース卒業研究報告要旨

高田 研究室	氏　　名	岡 野　兼 也
卒業研究題目	競技プログラミングコンテストの提出プログラムを利用した記号実行ツールKLEEの定量的評価	

情報システム開発において，時代とともに変化するユーザの要求に対応するため，ハードウェアと比較して変更が容易なソフトウェアにより，機能を実現することが増えている．これに伴い，開発されるソフトウェアの規模は年々大きなものとなり，複雑さも増している．一方，サイバー犯罪が増加しているという状況を鑑みると，情報システムの信頼性や機密性は重要である．

ソフトウェアの信頼性や機密性を確かめるためには，十分なソフトウェアテストの実施が必要不可欠である．しかし，ソフトウェアの大規模・複雑化により，人手による網羅的なテストケースの生成は困難なものとなっている．以上から，テストケース生成の自動化には大きな期待が寄せられている．

テストケースの自動生成手法の 1 つに，記号実行ツール KLEE を利用するというものがある．記号実行はプログラムを擬似的に実行し，実行可能な経路を網羅的に抽出する技術である．記号実行の実行中には変数はシンボルとして扱い，1 つの実行経路と対応した変数の値を探索することができる．KLEE は LLVM (Low Level Virtual Machine) ビットコードに変換された C 言語のプログラムに対して記号実行を行い，テストケースを生成するツールである．実際に Coreutils や BusyBox を始めとする，約 160 のソフトウェアに対して適用されている．生成されたテストケースは平均で 90%のコードカバレッジを実現し，脆弱性を発見することにも成功している．しかし，対象としたソフトウェアのほとんどは，システムソフトウェアと呼ばれるものであり，多様性に欠ける．

そこで，本研究では多様な特徴を持つプログラムに KLEE を適用し，KLEE の性能を評価した．KLEE を適用する対象として，多様なアルゴリズムを利用する，競技プログラミングコンテスト (AtCoder Grand Contest) の提出プログラムを選択した．本研究でのリサーチクエスチョン (RQ) は，**RQ1** KLEE が正常終了するかどうか，**RQ2** KLEE でのシンボル値の探索が 10 分間で 10 個以上完了するかどうか，**RQ3** 生成されたテストケースのコードカバレッジが 50%を超えるかどうかの 3 つである．

KLEE の実行後，プログラムや KLEE の実行結果から得られるメトリクスを利用して，コードカバレッジを目的変数とする線形回帰分析を行った．KLEE の実行や線形回帰分析の結果として，**RQ1** に対して，記号実行を行う際にシンボルとなる変数が利用するメモリ使用量の大きい場合に，KLEE が異常終了するということがわかった．**RQ2** に対して，グローバル変数がシンボルとなっている場合に KLEE は実行が低速になるということがわかった．**RQ3** に対して，プログラムの最大のネスト数が大きいほどコードカバレッジが高くなるということがわかった．一方で，プログラムの実行メモリや複雑さは，コードカバレッジに大きな影響を与えなかった．このことから，KLEE を利用する際には記号実行のシンボルとなる変数の大きさやグローバル変数の数に注意する必要があるということが確認できた．

今後の展望としては，他の競技プログラミングコンテスト運営サイトから抽出したプログラムに対して同様の実験を行い，本研究で得た結果と比較するということが挙げられる．