令和元年度 情報工学コース卒業研究報告要旨

高田・松原 研究室	氏　　名	宮 木　龍
卒業研究題目	ファジングツールAFLの利用を支援するツールの開発	

ソフトウェア開発において，ソフトウェアが要求を満たしていることを確認するため，ソフトウェアテストが行われる．近年，ソフトウェアの開発規模が飛躍的に増大し，ソフトウェアテストの重要性が一層高まっている．しかし，ソフトウェアテストの大部分は手作業で行われ，漏れやミスが発生したり，大きなコストがかかるといった問題がある．

このような問題を軽減するため，ソフトウェアテストの自動化に対する需要が高まっている．自動化が可能なソフトウェアテストの1つとして，ファジングが注目されている．ファジングは，ファズと呼ばれるデータを生成して対象のソフトウェアに入力し，挙動を監視するという流れを繰り返すことで，不具合を自動で検出するテスト手法である．ファジングを自動で行うツールをファジングツールと呼ぶ．ファジングによって不具合の低減やテストにかかる労力の削減といった効果が得られるが，ファジングはファジングツールの利用経験がないと導入の敷居が高いという問題がある．

本研究では，ファジングの導入の敷居が高いという問題を軽減することを目的とする．目的を達成するため，ファジングツールの利用経験がない開発者でもファジングを利用できるよう，ファジングツールの利用を支援するツールを提案する．提案ツールで対象とするファジングツールは，数多くの脆弱性を検出した運用実績を持つ American Fuzzy Lop（以下，AFLとする）とした．提案ツールに求められる要件を決定するため，AFLを用いてソフトウェアの不具合を検出し，それを修正するまでの流れにおいて，AFLの利用経験がないユーザにとってどのようなことが問題となるかを考えた．そして，それを基に提案ツールに求められる要件を決定した．要件は，要件1. ツールの指示どおりに入力を与えるだけでファジングを開始できること，要件2. ファジングで検出した不具合をユーザが簡単に再現できること，要件3. ファジングによって得られた結果を活かしたデバッグを支援することの3点とした．決定した要件に基づいて，提案ツールの開発を行った．

提案ツールは，AFLの起動に必要な入力を指定するようユーザに指示し，AFLを起動する機能を提供する．これによって要件1に対応した．AFLは不具合を起こさないファズを変化させて新たなファズを生成し，不具合を起こすファズとその元となったファズを出力する．提案ツールは，AFLが出力するファズから任意のファズをテスト対象プログラムに入力した状態でGDBを起動する機能を提供する．この機能で，不具合を起こすファズを選び，起動したGDBを操作することで，不具合を再現することができる．これによって要件2に対応した．また，この機能で，不具合を起こすファズの元となったファズを選べば，不具合が起こる場合と起こらない場合とで実行結果を比較することができる．AFLが出力する不具合を起こすファズのサイズが大きいと，ファズ中で不具合の原因となった箇所が分からないという問題がある．そこで，提案ツールはデルタデバッギングによって不具合を起こすファズのサイズを最小化する機能を提供する．この機能によって，不具合を起こすファズの不具合の原因となる箇所を特定する作業を支援する．以上，不具合が起こる場合と起こらない場合とで実行結果を比較する作業，不具合を起こすファズ中で不具合の原因となる箇所を特定する作業の2点を支援することで，要件3に対応した．

本研究では，AFLの利用経験のないユーザに対して，AFLの利用を支援するツールの提案，開発を行った．今後の課題としては，ファジング終了タイミングの判断の支援や，AFLが実行経路情報を収集するためにテスト対象プログラムに挿入した命令をGDB起動時に除去することが挙げられる．