# 탐색 문제로 본 지향성 퍼징

Tae Eun Kim

2021.12.03

**Abstract**

지향성 퍼징은 프로그램 내부의 길을 찾는 탐색문제로 볼 수 있다. 그렇기에 대부분의 탐색문제와 마차가지로 국소 최적해(local optima)에 빠질 위험을 가지고 있다. 기존 기술인 AFLGo는 탐색 과정을 탐험과 집중 단계로 나누어 이러한 문제를 해결하려고 하였다. 하지만 정적분석을 활용한 지향성 퍼징에서는 정적분석 단계가 탐험을 대체하기에 더 효율적인 탐색이 가능하다.

지향성 퍼징의 목적은 특정한 지점에 도달하는 입력을 찾는 것이다. 이는 프로그램이라는 미로 속에서 길을 찾는 것으로도 볼 수 있고, 이러한 시각은 지향성 퍼징을 탐색문제로서 접근할 수 있게 한다. 다른 현실적인 탐색 문제들이 그렇듯이 지향성 퍼징도 국소 최적해(local optima)의 위험이 존재한다.

기존 기술인 AFLGo는 이 문제를 해결하기 위해 탐색 과정을 두 단계로 나누어 진행하였다. 먼저 탐험 단계를 통해 프로그램을 전체적으로 둘러보고, 이후 집중 단계에서 더 매력적인 길을 집중적으로 탐색하게 된다. 어디서 시작해야 원하는 지점에 도달 할 수 있을지 모르기 때문에 탐험 단계에서 가능한 시작 지점들을 최대한 많이 수집하는 것이다. 이 때, 탐험 단계에서는 주어진 정보(AFLGo의 경우에는 거리정보)를 온전히 활용하지 못하는 대신 막다른 길에 도달하지 않기 위한 공학적 등가교환(trade-off)이 이루어진다.

하지만 정적분석을 활용한 지향성 퍼징에서는 별도의 탐험단계가 필요하지 않다. 정적분석 과정에서 탐험의 목적이 성취되기 때문이다. 정적분석을 통해 얻은 정의-사용(Def-Use) 정보는 특정 지점에 어떻게 데이터 흐름이 도달하는지 알려준다. 이는 달리 말해, 어디서부터 시작해야 원하는 지점에 도달할 수 있을 지 알려주는 단서로써, AFLGo의 탐험 단계보다 더 구체적이고 직접적인 정보가 된다. 따라서 정적분석을 활용한 지향성 퍼징은 주어진 정보를 처음부터 적극적으로 활용하여 더 효과적인 탐색, 즉 퍼징을 할 수 있을 것으로 기대된다.

이렇게 문제의 특성이 무엇이고, 접근의 특성이 무엇인지 이해하는 것이 중요하다. 그렇지 않다면 정적분석을 활용함에도 불구하고 별도로 탐험 단계를 두는 등, 접근 방식의 장점을 제대로 살리지 못할 수 있기 때문이다.