# AFLGo 최적화 하기

Tae Eun Kim

2021.11.19

**Abstract**

지향성 퍼징은 원하는 지점에 도달하는 입력을 생성하는 것을 목표로 한다. AFLGo는 이 목표를 탐색문제로 접근하여 풀었는데, 탐색이 Local optima에 빠지는 것을 방지하기 위해 Exploration 과 Exploitation 단계를 나눈다. 하지만 그 전환 시점은 사용자의 입력에 의존하기에 매번 다양한 대상 프로그램에 대한 적절한 값을 찾기가 어렵다. 여기에 대한 대안으로 다른 탐색 기법을 적용한다면 별도의 입력없이도 대상 프로그램을 효과적으로 탐색할 수 있을 것이다.

지향성 퍼징 도구들의 목적은 사용자가 원하는 지점까지 도달하는 입력을 빠르게 생성하는 것이다. 이 중 AFLGo는 각 프로그램 지점 사이의 거리를 고려하여 목표 지점에 더 가까이 도달하는 입력을 탐색해나간다. 만약 특정한 입력이 지난 경로가 평균적으로 목표 지점과 가깝다면 해당 입력을 기반으로 더 많은 입력을 생성하는 방식이다.

하지만 계속해서 제일 가까운 입력만을 사용한다면, 더 이상 목표지점과 가까워 질 수 없는 막다른 길로 빠질 위험이 있다. 따라서 AFLGo는 전반적인 탐색을 충분히 한 후에 거리 정보를 적극적으로 활용하는 탐색으로 넘어간다. 이 때, 그 전환 시점은 사용자의 입력에 의해 결정되는데, 대상 프로그램마다 적절한 전환 시점은 다를 수 있어 어려움이 발생한다.

이에 대한 대안으로 참고할 수 있는 것은 Ant Colony Optimization(ACO) 라는 경로 탐색 기법이다. ACO는 개미가 길을 표시하듯이 매력적인 길에 페로몬으로 표시를 하고, 페로몬이 가장 강한 길을 최적의 경로로 선택한다. 이때, local optima에 빠지지 않는 핵심은 이 페로몬이 시간이 지날수록 감소한다는 것이다. 따라서 한때 매력적이었던 길도 새로운 업데이트가 없으면 그 매력을 잃음으로써 최적 경로의 후보에서 제외된다.

AFLGo가 local optima에 빠질 위험은 거리 정보가 고정된 값이기 때문에 발생한다. 이 때, ACO의 페로몬 개념을 AFLGo에 적용한다면 막다른 지점에 다다른 입력은 그 매력을 잃게 되고, 계속해서 뻗어나갈 수 있는 입력은 살아남을 것이다. 먼저, 특정 입력의 거리 정보를 초기 페로몬 값으로 설정해주되 이는 시간에 따라 감소하도록 한다. 그리고 해당 입력으로부터 더 좋은 입력이 발생하였다면 기존 입력에 페로몬을 추가해주면 된다.