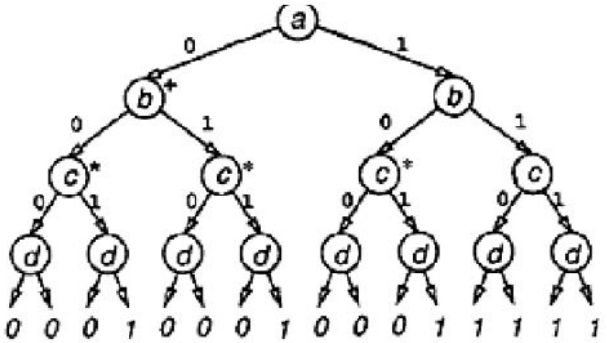
지향성 퍼징 모델체킹: 모델체킹에 내비게이션 얹기

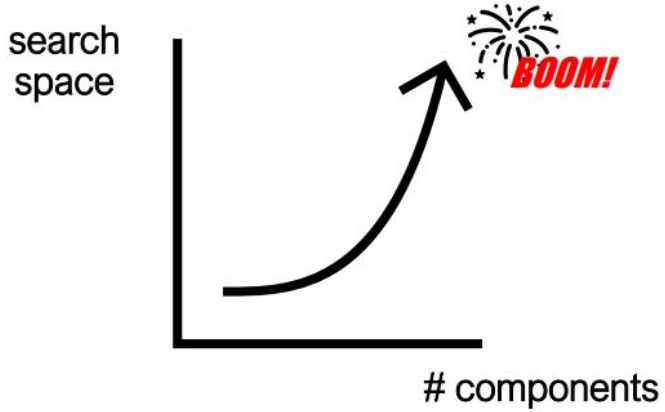
Directed ~~Fuzzing~~ Model Checking: Model Checking with GPS

2024년 여름 소프트웨어재난센터 워크숍

손병호, 포항공대

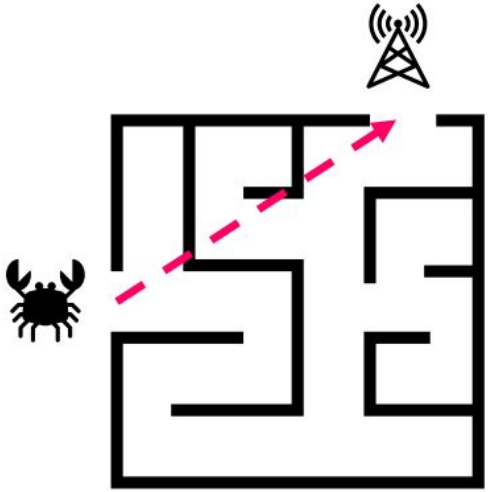
상태공간폭발





- 모델체킹 = fancy DFS
- 시스템 컴포넌트가 하나 늘어날 때마다 전체 시스템은 급격히 커짐

지향성 모델체킹: 모델체킹에 GPS 달기



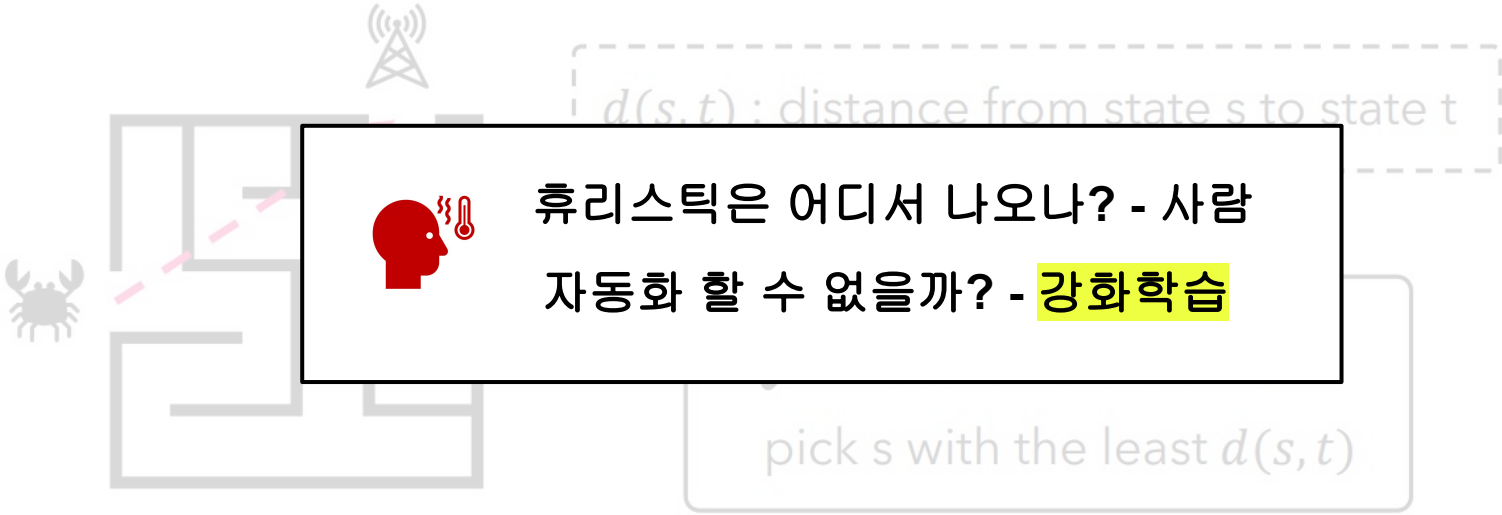
$d(s,t)$: distance from state s to state t

Search Heuristics

pick s with the least $d(s,t)$

- DFS, BFS 처럼 무식하게 탐색 x
- A* 알고리즘처럼 똑똑하게

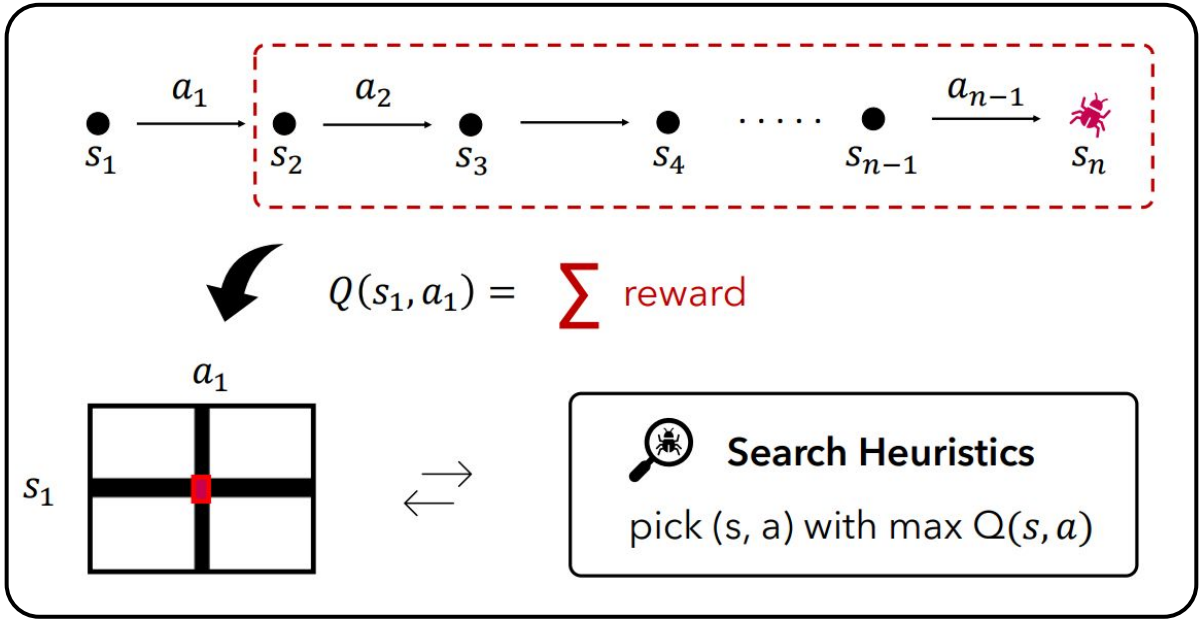
지향성 모델체킹: 모델체킹에 GPS 달기



휴리스틱은 어디서 나오나? - 사람

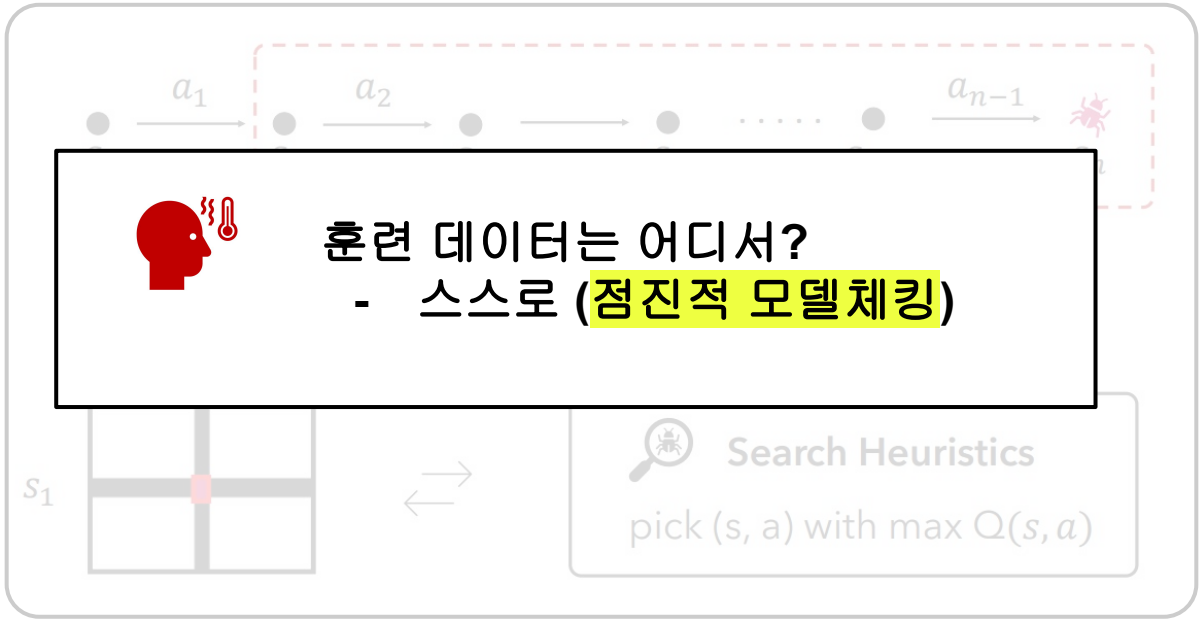
자동화 할 수 없을까? - 강화학습

강화학습으로 휴리스틱 자동생성하기



- 모델을 마구잡이로 돌려보며 경로 생성 (시뮬레이션)
- 오류 찾으면 “당근”, 못 찾으면 “채찍” (Q-러닝)

강화학습으로 휴리스틱 자동생성하기



점진적 모델체킹: 쉬운 문제로 준비운동하기

- 3대의 노드가 있는 분산 시스템
- 5대의 노드가 있는 분산 시스템

점진적 모델체킹: 쉬운 문제로 준비운동하기

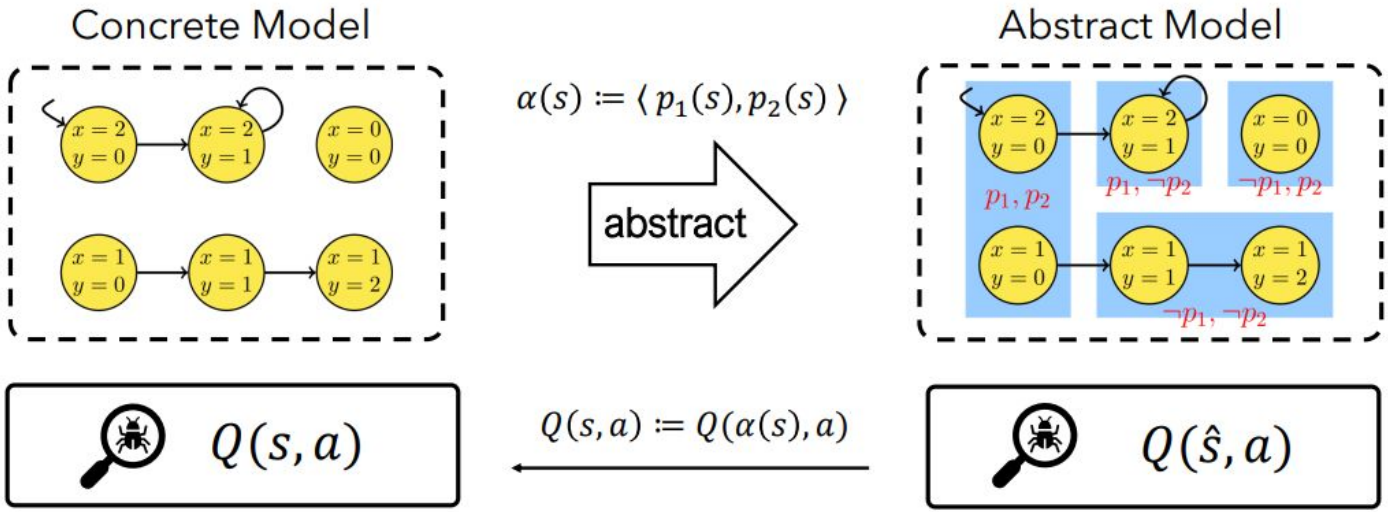
사실상 똑같은 문제 아닌가?

- 매우 달라서 일반화 필요

Small Model

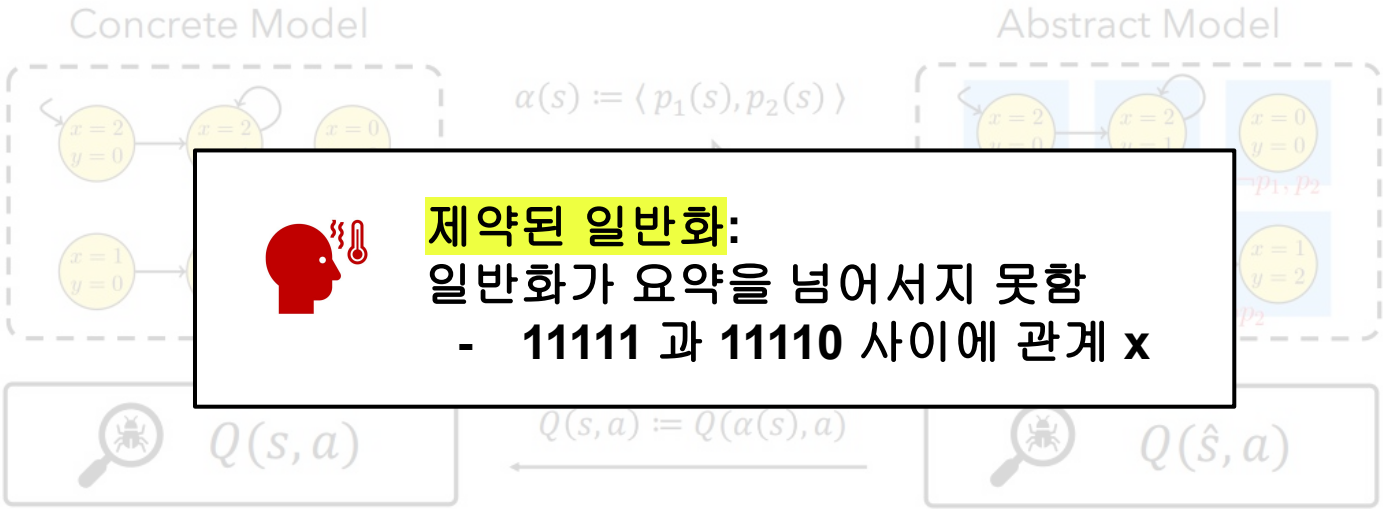
Big Model

휴리스틱 요약하기: 요약상태마다 점수 부여



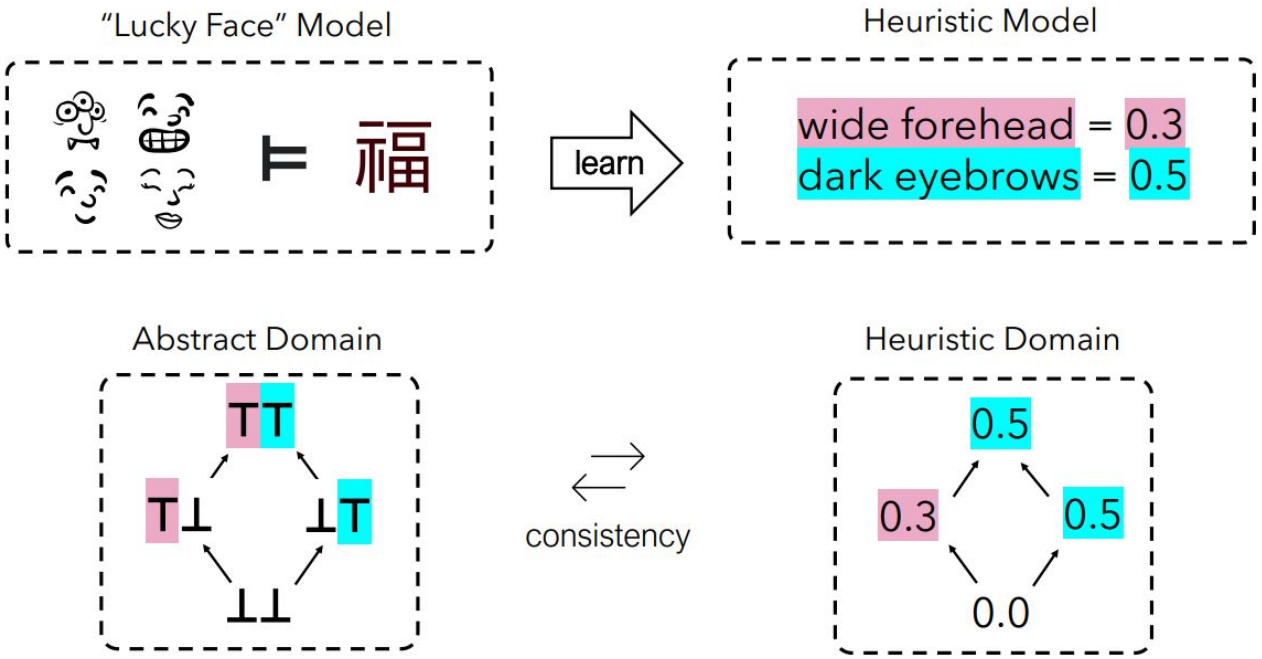
- 명제 요약: 상태를 k개 명제로 구성된 특성벡터로 요약 (α(s) = ŝ)
- **요약된 휴리스틱**: Q(s, a)가 아니라 Q(ŝ, a)

휴리스틱 요약하기: 요약상태마다 점수 부여



제약된 일반화:
일반화가 요약을 넘어서지 못함
- **11111 과 11110 사이에 관계 x**

휴리스틱 조립하기: 특성마다 점수 부여



끝.