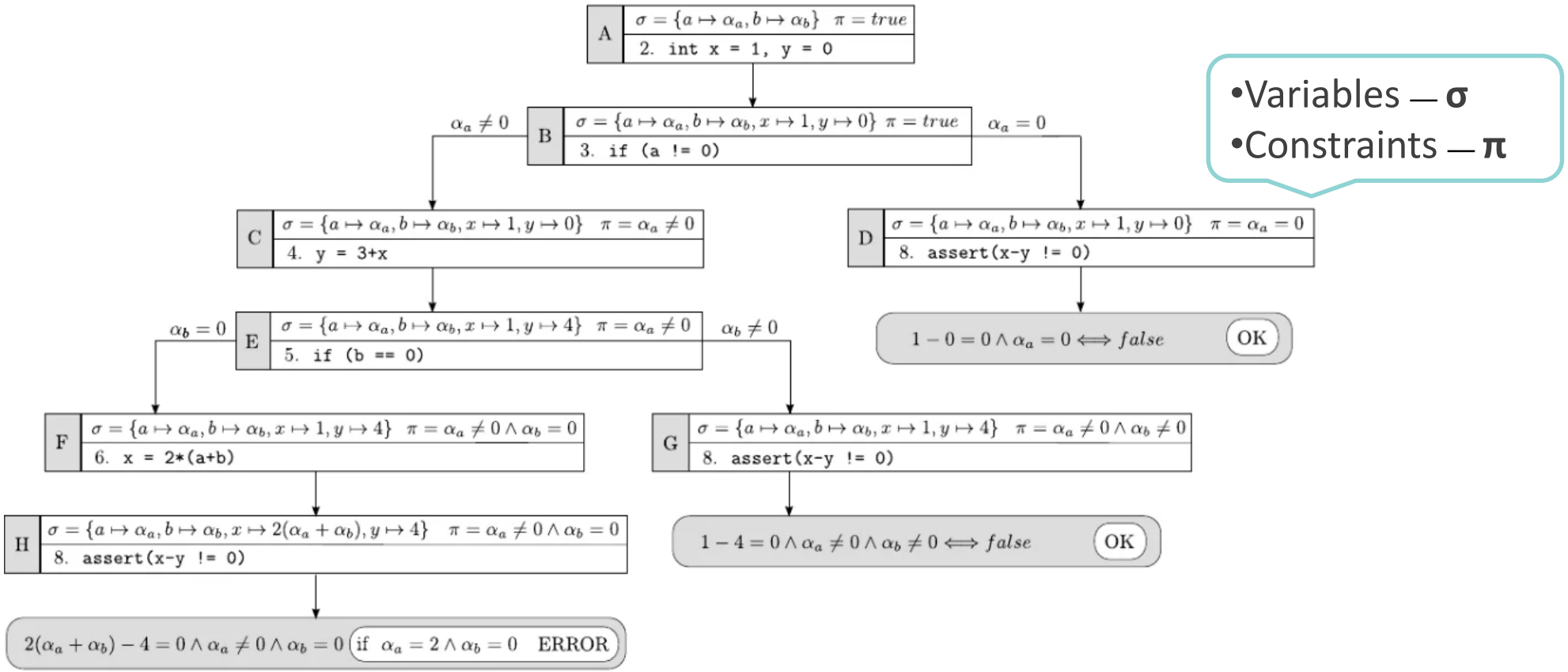
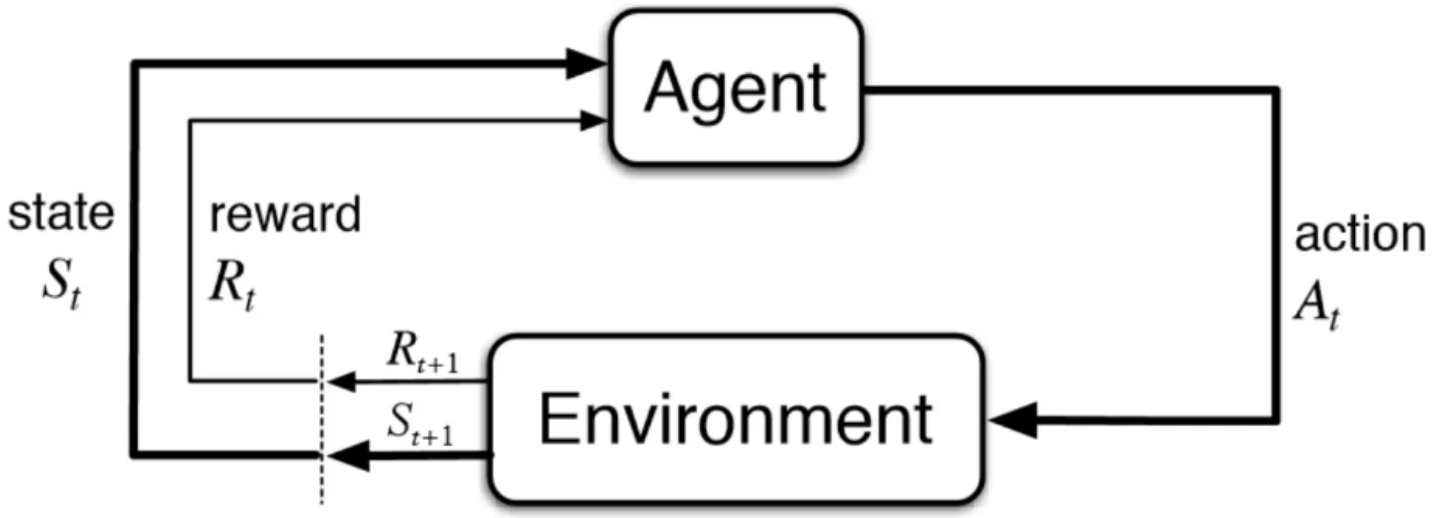
Symbolic execution + RL

By: Andrey Podivilov, Sergey Savin
Mentor: Vadim Lomshakov

Path selection for symbolic execution

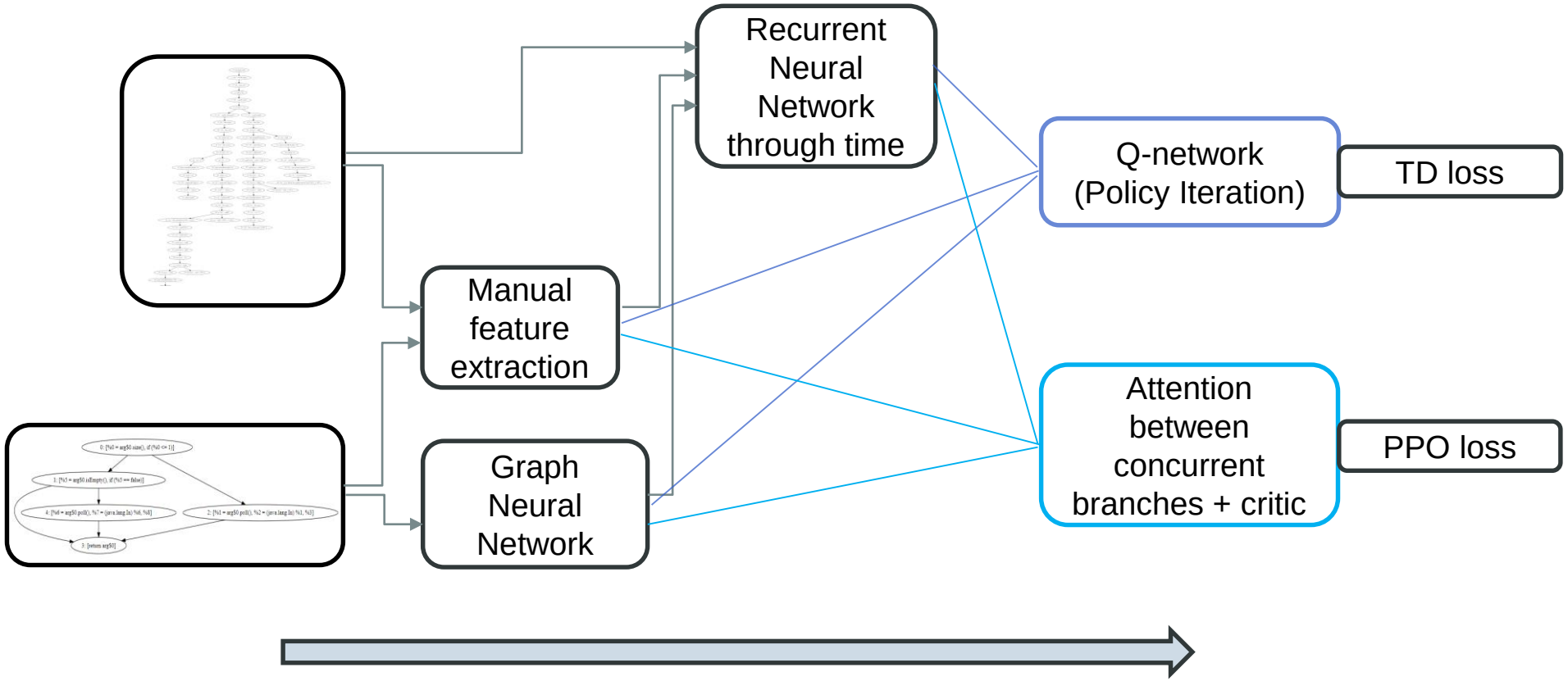


Why RL?



- Environment – Symbolic Engine run
- Reward – code coverage over time, detected vulnerabilities, etc.
- Agent – Path Selector
- State – covered region of an Execution Tree
- Action – branch selection

Architecture



Results

	guava	antlr	pdfbox
PPO	$\mathbf{3.55}_{\pm 0.25}$	$\mathbf{3.03}_{\pm 1.25}$	$2.27_{\pm 0.13}$
PI	$3.45_{\pm 0.15}$	$2.98_{\pm 0.73}$	$\mathbf{2.45}_{\pm 0.3}$
USVM heuristic-1	$2.87_{\pm 0.34}$	$2.6_{\pm 0.66}$	$2.31_{\pm 0.34}$
USVM heuristic-2	$2.7_{\pm 0.39}$	$1.96_{\pm 0.23}$	$2.2_{\pm 0.47}$

Average Coverage

Thank you for your Attention!

Q&A

Andrey Podivilov
Sergey Savin

Interns, Cloud BU
andrey.podivilov@gmail.com
sergeyrid@yandex.ru