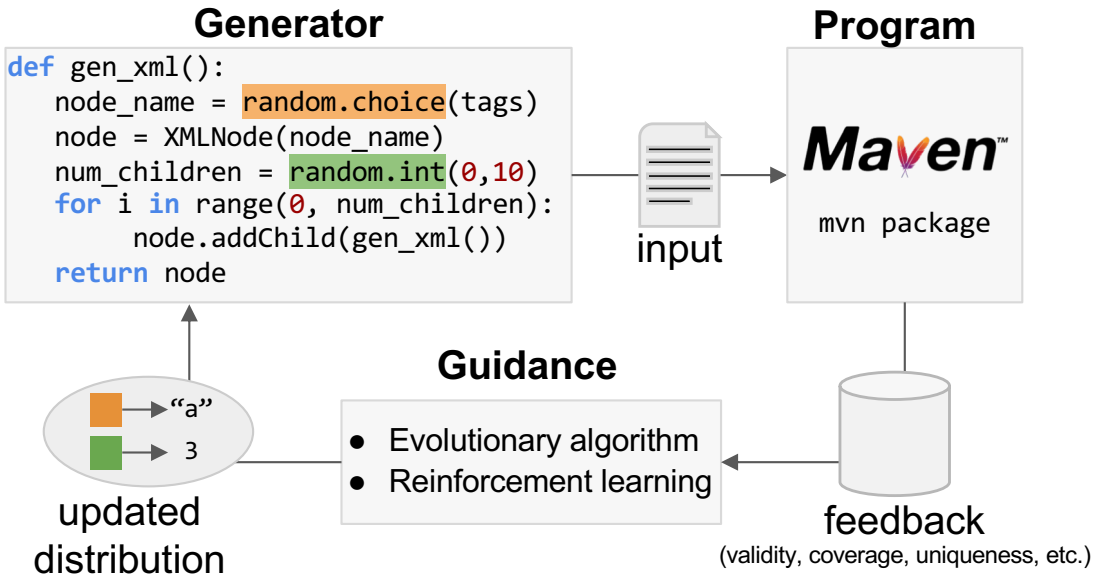
Machine Learning for Effective Fuzz Testing: PI: Koushik Sen, co-PI: Dawn Song, UC Berkeley

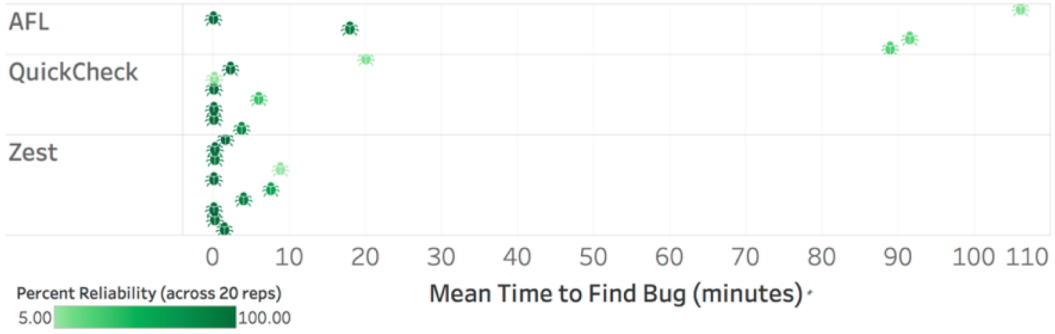
Feedback-directed mutational fuzzing:

- \+ Highly effective at finding bugs and security vulnerabilities
- \+ Uses feedback from program to tune input generation
- \- Fails to generate many structured inputs satisfying validity constraints

How can we leverage feedback to generate many diverse valid test inputs?



Zest (evolutionary algorithm) finds semantic bugs reliably and quickly



RLCheck (reinforcement learning)
quickly generates diverse valid test inputs