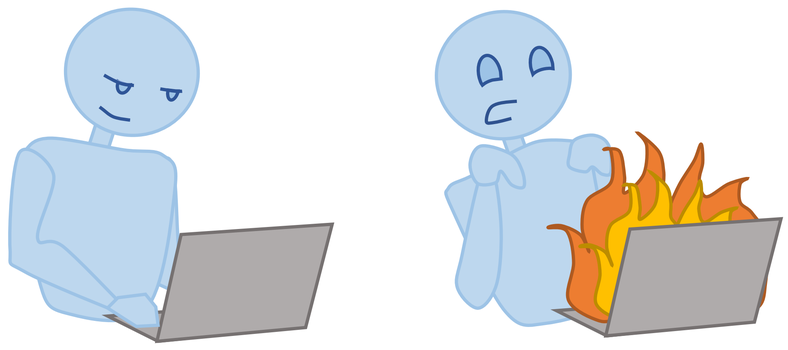
PerfFuzz: Automatically Generating Pathological Inputs

Caroline Lemieux, Rohan Padhye, Koushik Sen, Dawn Song
University of California, Berkeley

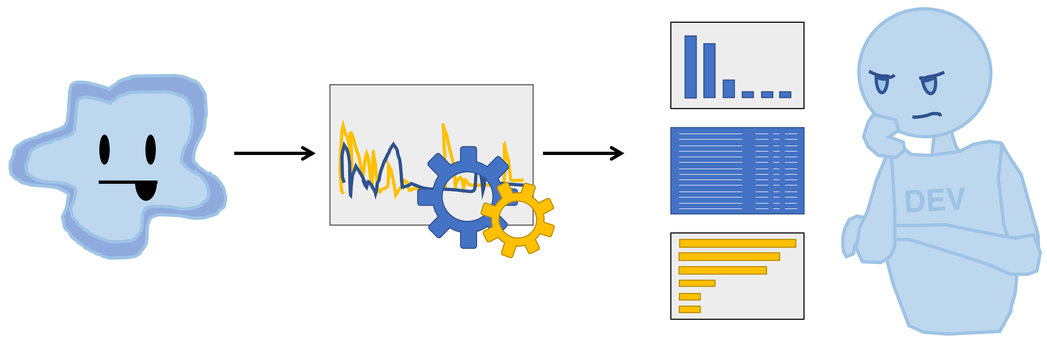
`https://github.com/carolemieux/perffuzz`

Performance problems arise unexpectedly



when programs are run on *pathological* inputs.

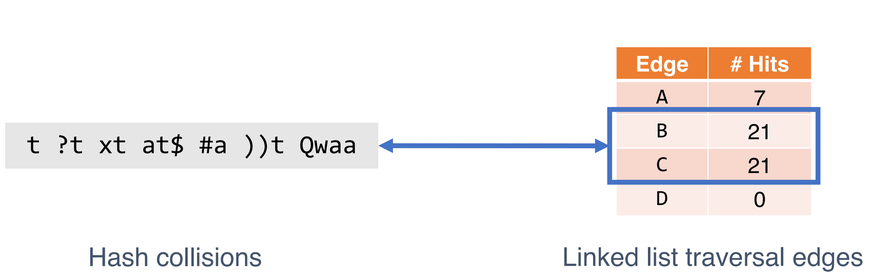
Profiling tools help devs diagnose the problem



...if they have a pathological input to start with!

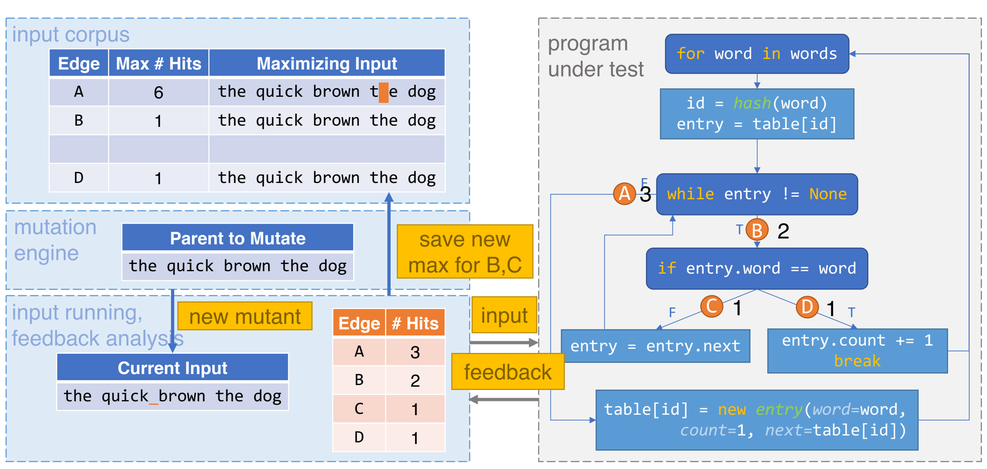
PerfFuzz generates pathological inputs using **feedback-directed mutational fuzzing**.

PerfFuzz maximizes **control-flow-graph edge** hits: a less noisy signal for pathological behavior.

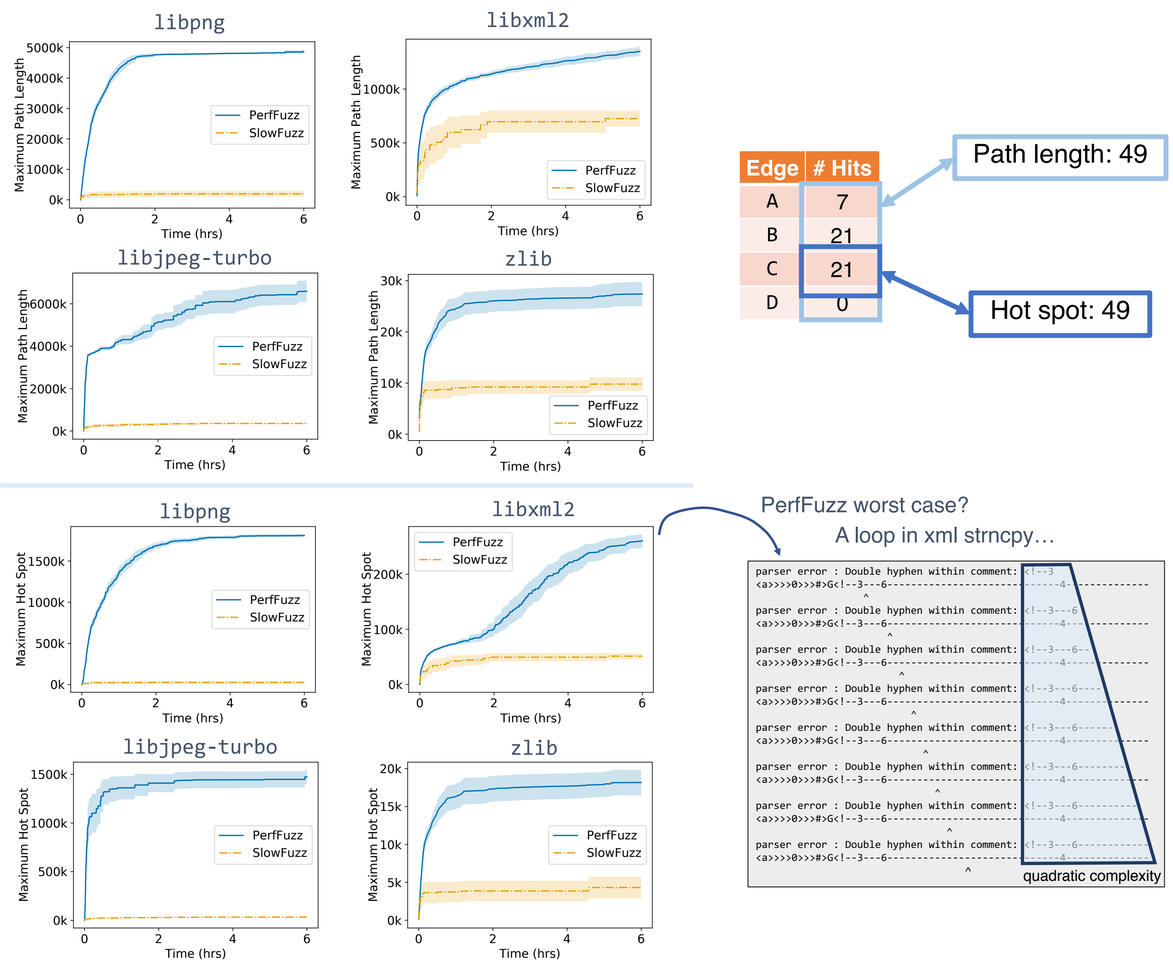


Edge	# Hits
A	7
B	21
C	21
D	0

Detailed architecture.



Macro-Benchmarks



Micro-Benchmarks