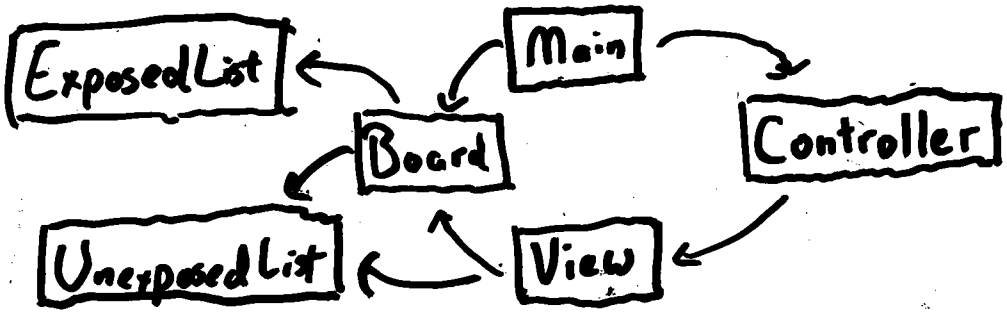
Modular Pluggable Analyses

Patrick Lam, MIT CSAIL

Goal: Apply Multiple Precise Analyses to a program to Verify Interesting Properties



Set Specification Language

List.add(n) requires not (n in Content)
modifies Content ensures Content' = Content ∪ n;

MinedCells ∩ ExposedCells ≠ ∅ => GameOver

- first-order formulas over sets

Set Definitions: E = {x | x.isExposed = true}; (typestate)
C = {n | root <next*> n}; (graph types)

Modular Analysis
- Establish rep invariants within each module
- Assume/guarantee reasoning to verify inter-mod props

Applications Analyze detailed properties by focussing analysis:
- internal data structure consistency properties
- correlations between obj. states & proc. invocations
- global consistency properties involving objs that participate in multiple data strs.