CodeContracts

Motivation

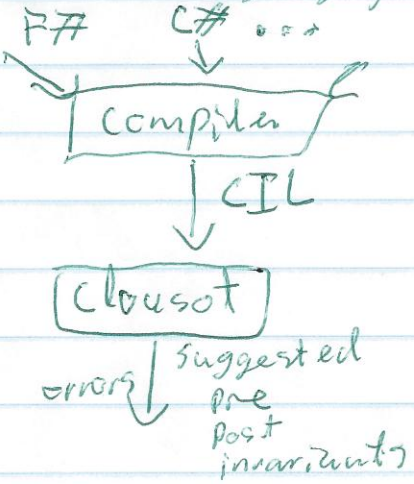
Compile time checks for .Net

specification

Spec# & JML ⇒ Comments

Contract.requires(...)

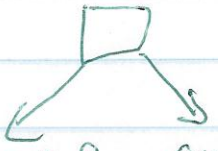
- IDE support
- Easier to parse bytecode (var...)
- Bytecode changes are rare
- Supports all .Net languages



How it works

Inference

- CFG construction — pre/post/inv inserted — if e
- Sorted call graph
- Facts (abstract interpretation) ⟨PC, S⟩



Uses ordering to push/pull information

Checking

{implicit, explicit}

~~Direct checking~~ Assertion crawling ⟨PC, C⟩

Direct checking S ⇒ C? true, false, T, ⊥

Domain Retirement ← might need to recompute

Goal Directed backwards analysis

Push back proof obligation using weakest precondition

Classification

Unsound and uncomplete
- Aliasing

Modularity
Intraprocedural

Feels lightweight but uses medium weight tools

Expressiveness
Safety properties (assert)

Scalability
Scales well
Caching
Domain refinement

Can be hard to see reason a warning is generated.