

Requirements and Automated Refinement

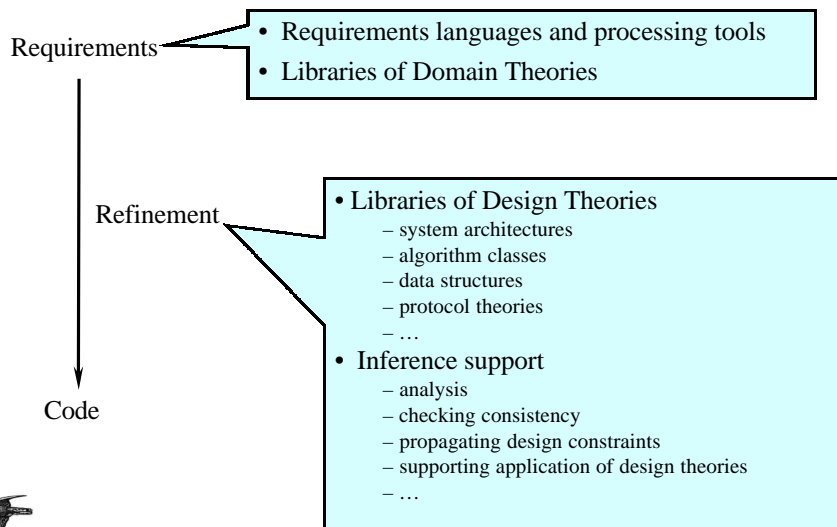
Douglas R. Smith
Kestrel Institute
Palo Alto, California

www.kestrel.edu



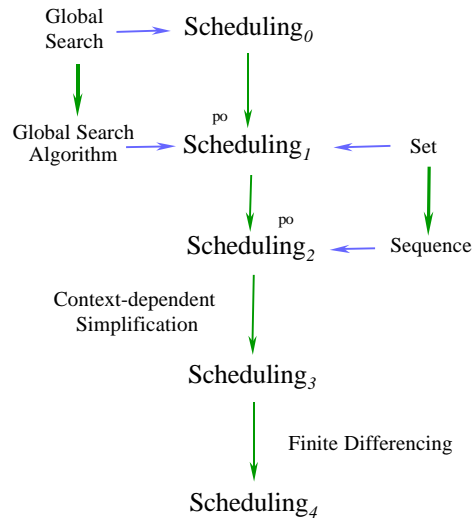
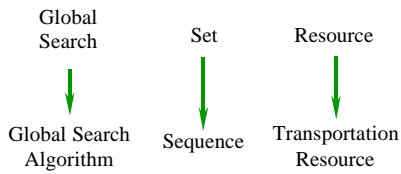
Refinement: Requirements \rightarrow Code

Generating correct-by-construction code from requirements



Constructing Refinements

1. Library of Refinements



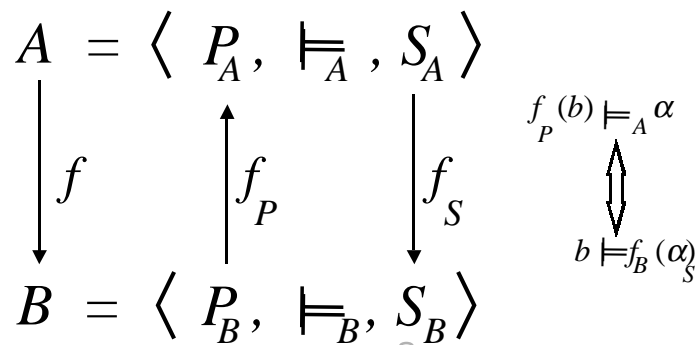
2. Library of Refinement Generators

- Rewrite Simplification
- Context-dependent Simplification
- Finite Differencing
- Case Analysis
- Partial Evaluation



Kestrel Institute

Specification Carrying Software

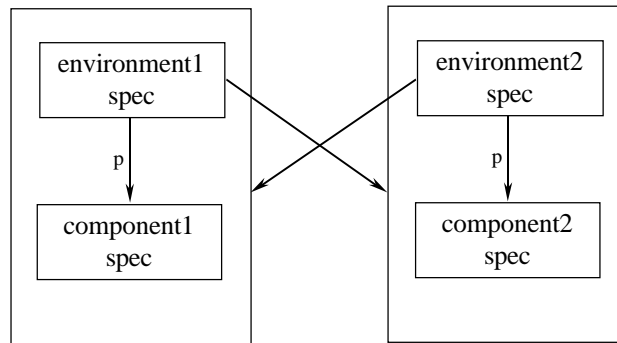


Kestrel Institute

simulates behavior

interprets structure

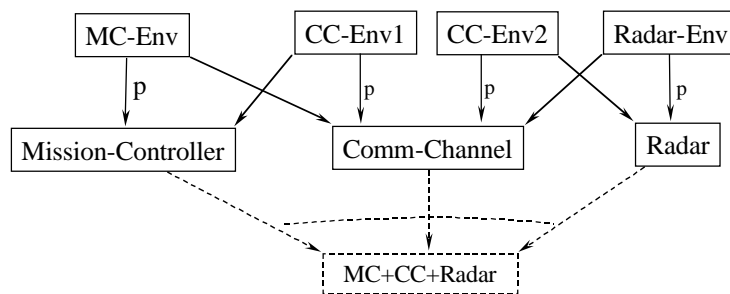
Open System Composition



colimit resolves the apparent circularity to produce the concurrent composition



System Composition



Cross-Cutting Constraints

Idea:

1. Express a cross-cutting constraint in temporal logic (or as an automaton)
2. Enforce the constraint by generating & adding code so that the new system refines the constraint

