ESCJ 15:
Design issues for ESC/Java

April 2nd, 1997

- Private variables in spec's?
- Modifies clauses?
- Specifications for interfaces?
- Vector-bounds checking?
- Monitor invariants?
- Module-initialization checking?
- Abstract state?

Iterative design process

- Claim:

  We should navigate this design space by trial-and-error, getting feedback from the field.

- Implication:

  We should be less concerned with the particulars of the first version of the tool and very concerned that what we build can be easily modified

Look at design-space breadth first

- Identify what's likely to be stable
  - Java syntax
  - Translation to guarded commands [?]
- Anticipate what's likely to change
  - Desugaring of specifications
  - "Additional" annotations (e.g., invariants, LL)

Implications for user manual

- Limit time spent designing annotations
- Don’t use as primary basis for building checker