

David Cok – Eastman Kodak

DAVID.COK@KODAK.COM

Vision: Static checking that adds value and that is practical in large-scale SW *(and somewhat complete...)*

➤ **easy-to-use, easy-to-learn, reliable, efficient, understandable, widespread, reasonable cost, supported, ...**

Current contribution: What is the usefulness and limit of JML and ESC/Java2?

➤ **How far from low-level bug detection toward the purpose of a program can we annotate and check?**

Semantics/Completeness

- **Model variables, methods, abstraction**
- **Purity**
- **Frame conditions -aliasing**
- **Exceptions**
- **String**
- **Annotations to help proofs of termination**
- **Initialization**
- **Arithmetic**
- **Detection of inconsistencies**
- **Loops, induction?**
- **...**

Usability

- **Understandable counterexamples**
- **Case studies**
- **More experience**
- **Integration with tools**
- **More complete library coverage**
- **Prover issues (e.g. quantifiers)**
- **Performance**
- **Integration with workflow**
- **...**