Reflections on Open Source Formal Methods Tools

Joe Kiniry
DTU
August 2013

Outline

- applied formal methods, rigorous engineering, tools, and communities
- the hows and whys of tool adoption
- pedagogical vs. research vs. commercial
- non-technical & technical factors
- VDM & Overture as a case study
- technical and community recommendations

Applied FM

- **invent** formal foundations to solve a new challenge using sometimes new and sometimes old techniques
- **build** new—or extend existing—tools to witness and experiment with foundations
- **bootstrap** new tools by using old tools
- **evaluate** utility with realistic case studies
- **contribute** to the community foundations, tools, datasets, case studies
- **promote** through teaching and demonstration

Rigorous Engineering

- respect the big picture of rigorous SE
- proper engineering is unavoidable even/ especially when using formal methods
- recognize that tools are part of..
  - their own process & methodology as well as others'
  - an individual's psychology & sociology as well as the community's

Tools

- PVS, Coq, and Celf
- Simplify, CVC, Z3, and Yices
- Rodin, Overture, CZT, and eRAISE
- OpenJML, FRAMA-C, Spec#, KeY, ESC/Java2, and Code Contracts
- Why3 and Boogie
- Agda, Haskell, SPARK/ Ada, Eiffel, and Scala
- jSMTLIB and FreeBoogie
- JMLunitNG and PEX
- F*, ProVerif, UPPAAL, FDR2, SPIN, SAL, and Alloy
- Maude, CafeOBJ, and OBJ3

Communities

- communities are individuals and entities (research group, company) passionate about a particular tool or technique
- what matters about communities?
  - size, age, impact, nationality, communication, wealth, influence, motivation, artifacts, quality, memes, momentum

Tool Adoption

- adopting a tool is expensive, so we must carefully decide when to take the risk
- cost of adoption and use must be amortized over time
- why does a tool/technology get adopted?
  - solves new, real problem >
    community >
    best-in-class >
    artifacts (books, slides, examples)

Adoption Context

- reasons for adoption in teaching, research, and commercial use are quite different
  - teaching: student's best interest > artifacts for instruction > robust to abuse > community
  - research: impact opportunities > bootstrapping artifacts > community
  - commercial: paying customer today > opportunities tomorrow > community

Influencing Factors

- size
- age
- impact
- nationality
- communication
- wealth
- influence
- motivation
- artifacts
- quality
- memes
- momentum
- source
- uniqueness

VDM & Overture

- strengths
  - history, age, foundations, community, artifacts
- neutral
  - size, communication, artifacts, quality, source, motivation, uniqueness, momentum
- weaknesses
  - nationality, history, age, foundations, impact, wealth, influence, memes

Strengths

- **history:** long history, distinguished personalities
- **age:** hundreds of man years of effort, decades of refinement and evolution
- **foundations:** formally grounded with novel foundations
- **community:** good size and vitality for a formal method
- **artifacts:** tooling is within a modern platform, has a command-line, and is written in Java; pedagogical, research, and commercial demonstrators are prolific; books are very good

Neutral

- **size:** community is small and active, but contributing engineering sub-community is very small
- **communication:** a move to a modern medium but low presence in FLOSS venues
- **quality:** platform is evolving, engineering comes from few, releases are decent compared to high visibility tools
- **source:** no large, high quality and impact university or corporation pushing
- **motivation:** no industry segment, certification standard, or major corporation is demanding knowledge or use of VDM
- **uniqueness:** difficult for potential users to differentiate VDM from competitors
- **momentum:** community and tooling momentum is static

Weaknesses

- **nationality:** tools with a non-US origin have greater difficulty breaking into markets
- **history:** early commercialization of virtually all of the kingpins of formal methods has harmed their impact
- **age:** old tools and methods are viewed as out-of-date and inapplicable to new challenges
- **foundations:** non-standard logic and complex semantics makes for greater difficulty in education, training, and use
- **impact:** no modern killer application to date
- **wealth:** research and commercial funding for formal methods waxes and wanes, but is never large
- **influence:** no highly influential party has rallied behind VDM
- **memes:** no chatter on social media

Recommendations

- **age:** prove that VDM is applicable
- **impact:** apply VDM to solve a modern critical, unsolved/unsolvable problem
- **influence:** convince a high profile company to buy-in to the VDM agenda via financial and in-kind contribution
- **nationality:** get a top 10 university in the USA as an active partner
- **memes:** foster chatter by active seeding