Recent and Upcoming Advances in the Dyninst Toolkits

Bill Williams

Paradyn Project

Petascale Tools Workshop
Granlibakken, CA
Aug 1-Aug 4, 2016

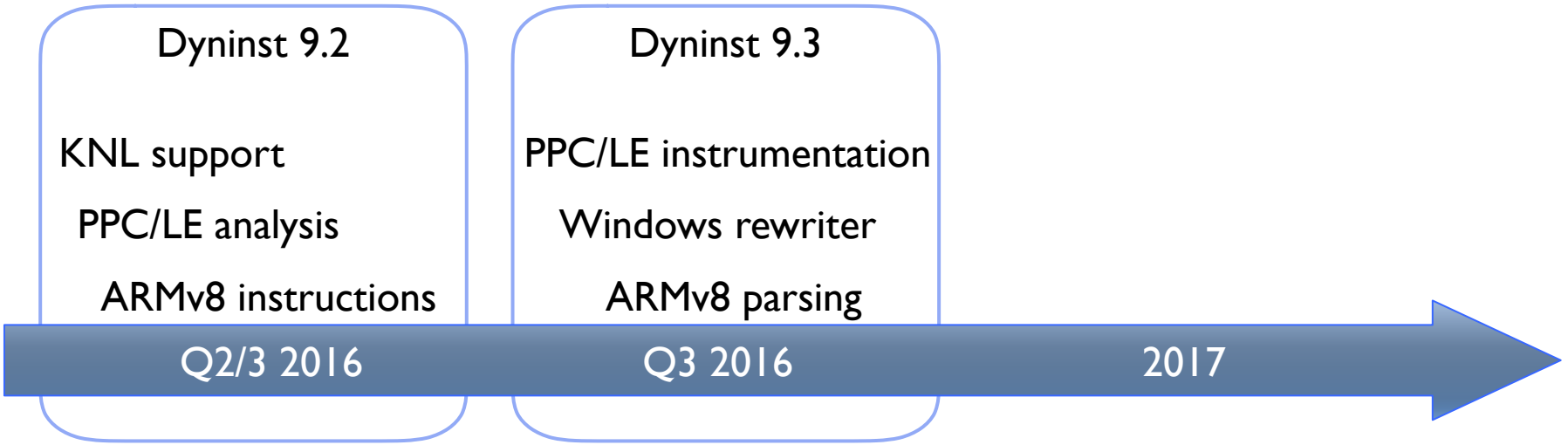
Dyninst Development Roadmap

- New platforms
- New features
- Smarter, better, faster
- Testing and robustness

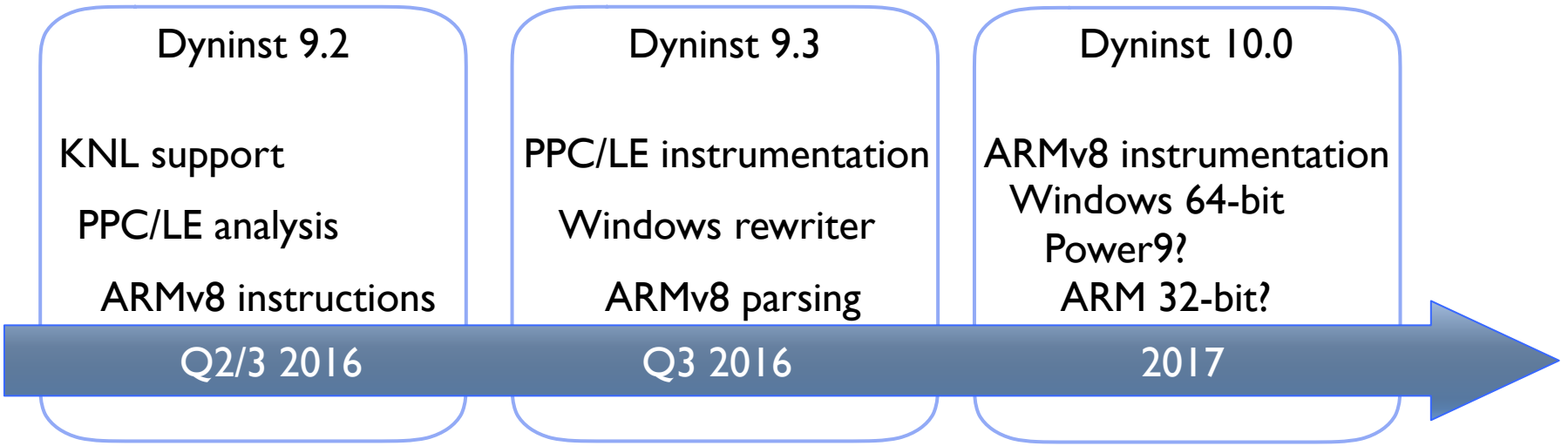
Dyninst Platforms

Dyninst Platforms

Dyninst Platforms



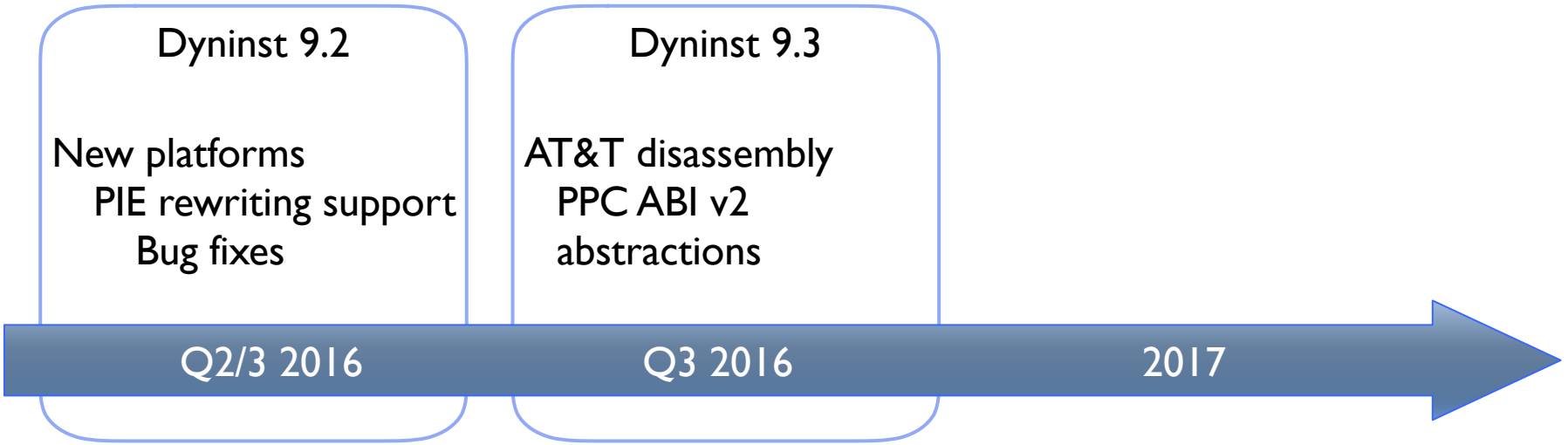
Dyninst Platforms



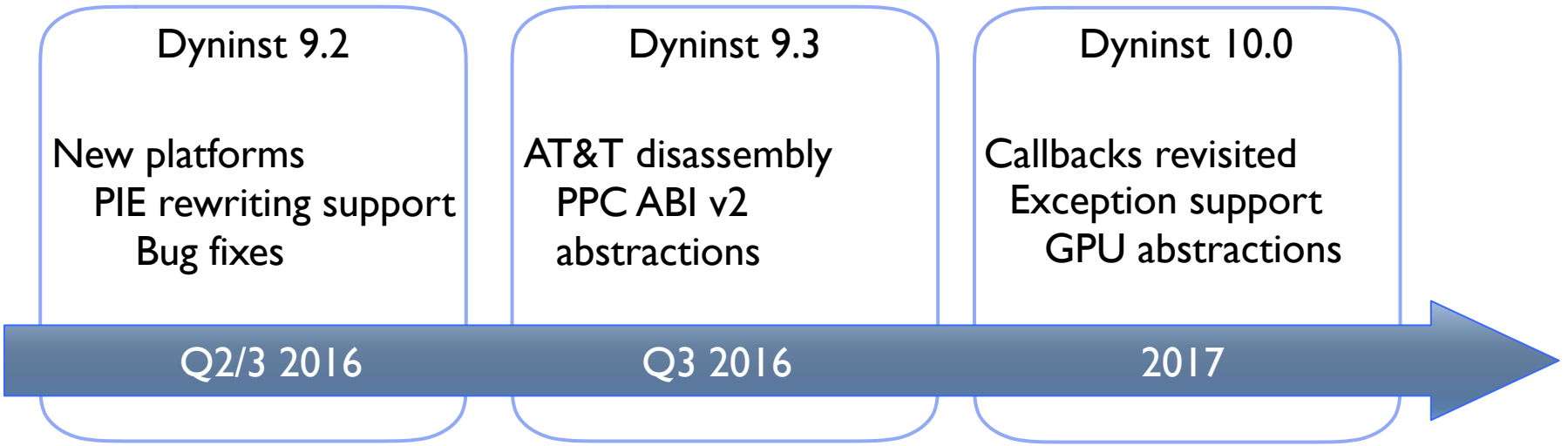
Dyninst Features

Dyninst Features

Dyninst Features



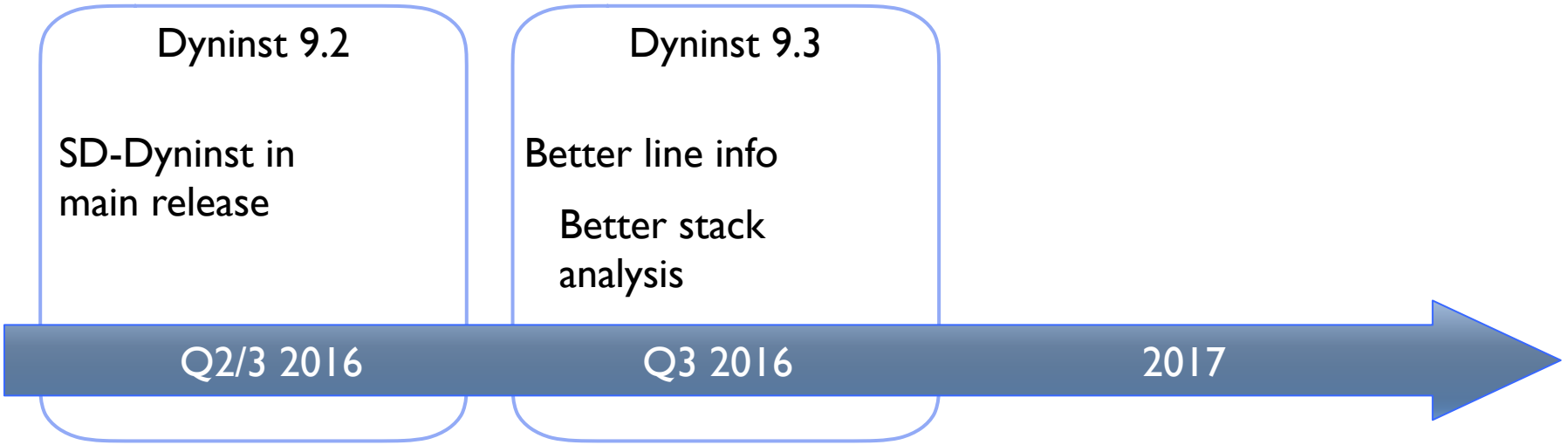
Dyninst Features



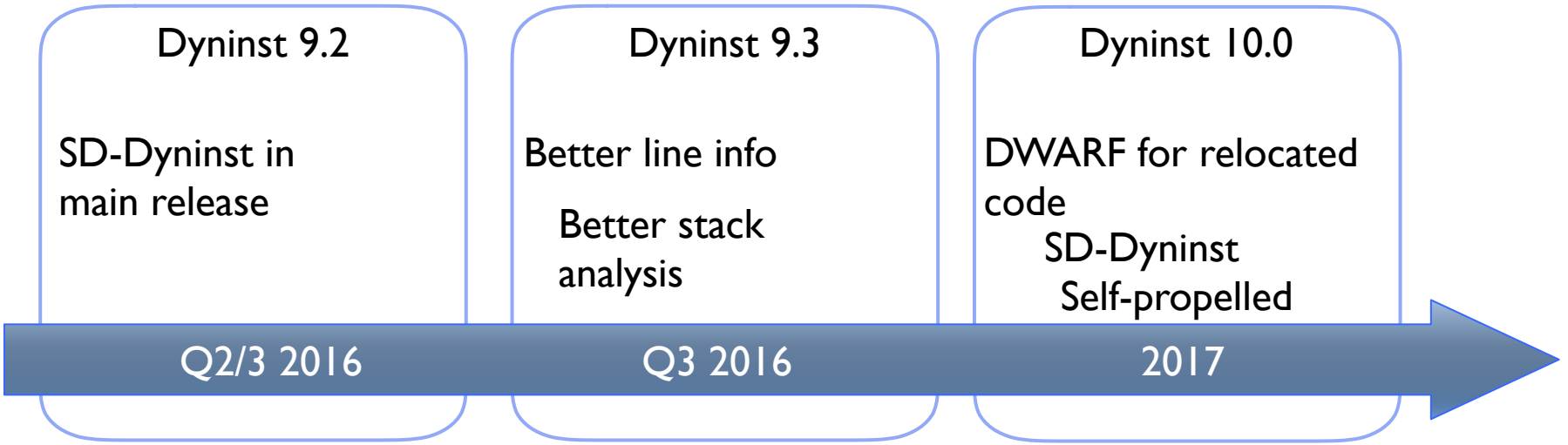
Smarter, Better, Faster

Smarter, Better, Faster

Smarter, Better, Faster



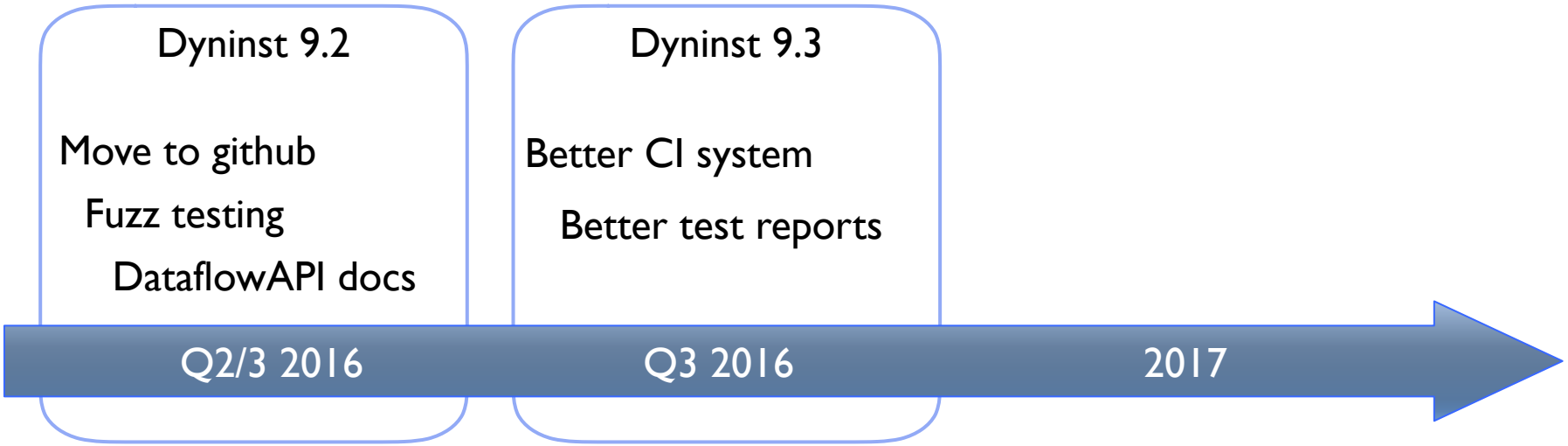
Smarter, Better, Faster



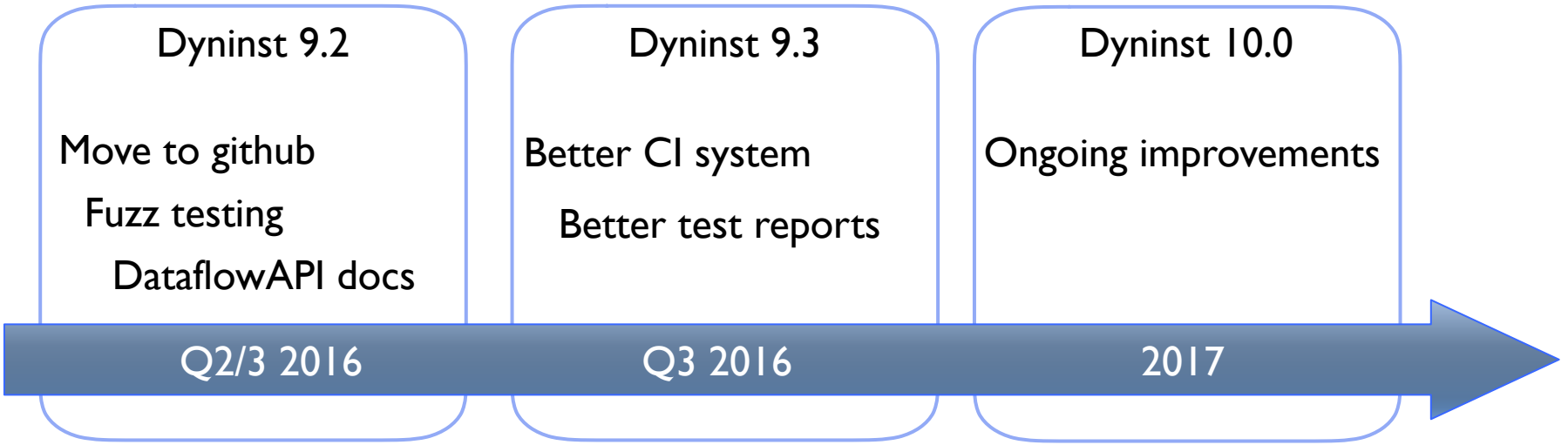
Testing and Robustness

Testing and Robustness

Testing and Robustness



Testing and Robustness



Github and Community Engagement

- Open bug tracker
- Easier to verify contributions
- Turnkey release system
- Increased activity
  - Number of commits
  - Number of committers
  - Transparent discussions

Outside contributions (current and future)

- Architecture-independent binary analysis
- Improvements in continuous integration
- Much code cleanup
- External build and test machines
- More and better bug reports
- More collaborative bug fixes

Release 9.2.1

- Line information fixes
  - Correctness (virtual functions, Fortran)
  - Speed
- PPC64 rewriting fixes
  - Generate more robust intermodule calls
- Crash bugs fixed
- Windows stack walking fixes

Dyninst 9.3

- PPC ABI v2
- Uniform AT&T disassembly
- ARM64 instruction semantics
- Complete ParseAPI on ARM64
- Windows rewriter

Fuzz testing instructions

- Started in Dyninst 9.1
- Integral in ARM implementation
- Allowed rapid, accurate catch-up on x86

ARM semantics: interface

Provides overridable function for each element of semantic pseudocode:

- Assignment
- Bit field extraction
- Sign/zero extension
- Math
- If/then/else
- Register access
- Memory access

ARM semantics: construction

Translate book pseudocode to ROSE policy class

- Build Bison grammar from XML to C++
- Start with elements for common instructions
- Apply to ParseAPI
- Iterate

Software info

- Main project page: https://github.com/dyninst/dyninst
  - Issue tracker
  - Releases and manuals
  - Coming soon: test results
- LGPL
- Contributions welcome