Code Review, and Automated Static Analysis Tools

SWE 261P

not test

Code Reviews

- Usually informal manual-human reviews of code
- Code review is considered a "static analysis" (that is, it is done without running the program — another term for "static analysis" is "compile-time analysis")
- Way to find potential problems early (remember the sensitivity principle)
- Microsoft has reported that code reviews is the place where most bugs are found

Best Practices for Code Reviews

- Review small portions of code at a time
- Record all feedback
- Review code independently before gathering to discuss
- Use checklists (there are tons of checklists online that can be used to start your own)

Example Checklist for Code Review

Example questions for a checklist

- Is all the code easily understood?
- Does it conform to your agreed coding conventions? These will usually cover location of braces, variable and function names, line length, indentations, formatting, and comments.
- Is there any redundant or duplicate code?
- Is the code as modular as possible?
- Can any global variables be replaced?
- Is there any commented out code?
- Do loops have a set length and correct termination conditions?
- Can any of the code be replaced with library functions?
- Can any logging or debugging code be removed?

https://www.fogcreek.com/blog/increase-defect-detection-with-our-code-review-checklist-example/

Etiquette for Code Reviews

- Code reviews can be unpleasant experiences for the reviewee
- Keep it professional and about the code (not the developer)
- Remember to notice and mention the good choices as well as the critique

Automated Code Review

- Class of tools called "Static Analyzers" that can perform some code review features

- These are considered "pessimistic" analyses (because they may mention issues that are not actual problems).

By the way, testing is considered an "optimistic" analysis, because of the "only reveals the presence of bugs, not their absence" nature.

- Examples of static analyzers:
  - FindBugs or SpotBugs
  - PMD
  - CheckStyle
  - Facebook Infer
  - SonarQube

Example Use of SpotBugs tool