Bugs & Debugging
How severe are bugs?

- Cost 300+ billions per year
How common are bugs

• About 10~15 bugs per 1000 lines of delivered code [Code Complete]
• About 10~20 bugs per 1000 lines of code during in-house testing, and 0.5 bugs per 1000 lines of code in released product [Microsoft]
Bug Types

• Semantic bugs
  • Logic errors
  • Typos
  • Missing corner cases
  • …

• Memory bugs
  • Buffer overflows (stack/heap)
  • Uninitialized read (read a variable before it is initialized)
  • Double free (free twice)
  • Memory Leaks (forget to free an object)
  • Dangling pointers (use a pointer after the corresponding region is freed)
  • …
  • Example buggy programs will be posted on course website

• Concurrency bugs
Bug finding tools

• Open-source / commercial tools
  • valgrind
  • coverity
• ...
Program verification tools

• “prove” that your program satisfies certain properties
  • Time consuming for large-scale software
  • Commonly used for mission-critical software
What is debugging?

• The process of looking for the root cause of a failure
How to debug; tools

• Go from symptom to root-cause

• Delta-debugging
• Slicing
• Gdb