Assert early and assert often

Practical hints on effective asserting

Tony Hoare

Techfest February 2002

Benefits of assertions today…

- Test probes
- Program documentation
- Interface specification
- Code optimisation
- Defect tracking
- Reduction of noise from analysis
- Hardening of retail code

… and more tomorrow

- Accuracy of program analysis
- Test case generation/prioritisation
- Post-mortem dump-cracking
- Concurrency safety
- Validation of security
- Programming language design

Engineering test probes

- Analogy: engine on a test bench
- Instrumented at internal interfaces
- To test tolerances continuously
- And avoid test to destruction
- Opportunity to improve quality by tightening the tolerances

Macros

```
#ifdef DEBUG
#define CHECK(b,str) {
 if (b) { }
 else {report (str);
   assert (false)}    }
#else #define CHECK(b,str)
#endif
```

Explanations

- CHECK(assertion, "reason why I think the assertion is true")
- Otherwise it's easy to forget.
- Helps both writer and reader.
- Pinpoints risk of similar errors
- Helps to avoid them in future

Other variants

• VSASSERT	Visual Studio
• MsoAssert	Office
• Debug.Assert	C#
• …	

Documentation

- Protection for system against future changes

```
if (a >= b){ .. a++ ; .. };
   .. ..
 CHECK(a != b, 'a has just
 been  incremented to avoid
 equality') ;
 x = c/(a - b)
```

Assumptions

- Used only during early test

```
SIMPLIFYING_ASSUMPTION
(strlen(input) < MAX_PATH,
  "not yet checking for
  overflow'')
```

- Failure indicates test was irrelevant
- Prohibited in ship code

Compile-time

-
  ```
  #define COMPILE_TIME_CHECK (b)
  extern dummy[(b)?1:-1]
  ```
- Generates report at compile time

-
  ```
  COMPILE_TIME_CHECK   (sizeof(x)
  ==sizeof(y), 'addition
  undefined for arrays of
  different sizes)
  ```

Invariants

- True of every object …
- …before and after every method call
- `bool invariant ( )`
  {…tests that list is circular…}

Invariants

- Integrity checking
- Software audits
- Post-mortem dump-cracking.

Interface assertions

- Useful to implementer and all users
- Used again on each release
- Reduce need to examine code
- Aid the unit test of each module
- Permit modular analysis and proof

Preconditions

```
void insert(node *n){
 PRECONDITION ( n != NULL &&
 invariant(), ‘don’t insert a
 non-existent object’);
 SIMPLIFYING-ASSUMPTION
              (find(n)== 0);
   .. .. ..
```

Post-conditions

```
  .. ..
POST_CONDITION ( find(n)&&
  invariant(), ‘the inserted
object will be found in the
list’)
 }
```

- obligation on method writer to verify

Optimisation

```
switch (condition) {
  case 0:  .. ..   ; break;
  case 1:   .. ..   ;break;
  default: UNREACHABLE(‘condition
   is really a boolean’);}
```

- Compiler emits less code

Defect tracking

- Office Watson keys defects by assertions
- Integrates with RAID data base
- Identifies bugs across builds/releases
- Integral to the programming process

PREFIX_ASSUME

- Reduces PREFIX noise
- pointer = find (something);
  PREFIX_ASSUME (pointer != NULL,
  “see the insertion three lines back”);
  … pointer ->mumble = blat …

Rugged code in retail

- VSASSERT assertions are ignored
- VsVerifyThrow … generate exception
- VsVerify …user chooses

Life of an assertion

- Design discussions: record decisions
- Project planning: interface contracts
- Test planning: harness design
- Test case selection: violate post-conditions
- Coding: correctness concerns
- Prototyping: simplifying assumptions

… continued

- In later release: detect regression
- Defect tracking: fault classification
- In retail: crash-proofing
- Defect analysis: dump-cracking
- Evolution of legacy: documentation

Conclusion

Assert early,

assert often,

and assert more strongly every time.

Apologies to…

'Vote early, vote often'

is the Politishun' s golden rule.

Josh Billings

American humorist, 1816-85.

Acknowledgements
thoare@microsoft.com

Rick Andrews, Chris Antos, Tom Ball, Pete Collins, Terry Crowley, Mike Daly, Robert Deline, John Douceur, Sean Edmison, Kirk Glerum, David Greenspoon, Yuri Gurevich, Martyn Lovell, Bertrand Meyer, Jon Pincus, Harry Robinson, Hannes Ruescher, Marc Shapiro, Kevin Schofield, Wolfram Schulte, David Schwartz, Amitabh Srivastava, David Stutz, James Tierney