Software Architecture

Bertrand Meyer
ETH Zurich, 30 March – 29 June 2005

Lecture 2:
Software quality; principles
and criteria of modularity

Agenda for today

- Software quality
- Modularity
- Reusability

Reading assignment for next week

OOSC, chapters
3: Modularity
6: Abstract data types
Software engineering

The collection of processes, methods, techniques, tools and languages for developing quality operational software.

By the way...

"Software" is not just programs. It includes processes for producing and operating the programs, as well as all related documentation,
### Software质量: 外部 vs 内部

- **外部**因素: 可见于客户
  (不仅对最终用户，还包括例如购买者)
  - *示例*: 使用的便利性，可扩展性，及时性
- **内部**因素: 可感知于开发人员
  - *示例*: 良好的编程风格，信息隐藏

只有外部因素最终算数，但内部因素使我们有可能获取它们。

### 软件质量: 产品 vs 过程

- **产品**: 结果软件的属性
  例如: 正确性，效率
- **过程**: 用于生产并“维护”软件的程序的属性

### 外部质量因素

产品质量（短期）:
- 正确性
- 坚固性
- 安全性
- 使用的便利性
- 学习的便利性
- 效率

产品质量（长期）:
- 可扩展性
- 可重用性
- 可移植性

过程质量:
- 及时性
- 成本效率
Reliability

Correctness:
The systems’ ability to perform according to specification, in cases covered by the specification

Robustness:
The systems’ ability to perform reasonably in cases not covered by the specification

Security (integrity):
The systems’ ability to protect itself against hostile use

Security

Carcassonne, 13th century

Chambord, 16th century
"I think that it’s extraordinarily important that we in computer science keep fun in computing. When it started out, it was an awful lot of fun. Of course, the paying customers got shafted every now and then, and after a while we began to take their complaints seriously. We began to feel as if we really were responsible for the successful, error-free perfect use of these machines. I don’t think we are. I think we’re responsible for stretching them, setting them off in new directions, and keeping fun in the house."

Alan Perlis, Preface to The Structure and Interpretation of Computer programs by Abelson and Sussman

- CORRECTNESS
- ROBUSTNESS
- INTEGRITY
- EASE OF USE
- REUSABILITY
- EXTENDIBILITY
- PORTABILITY
- EFFICIENCY
- ...

Correctness:
- The ability of a software system to perform according to specification, in cases defined by the specification.

Robustness:
- The ability of a software system to react in a reasonable manner to cases not covered by the specification.
Reliability

- Correctness + Robustness + Security
- Techniques will be studied in detail: typing, Design by Contract, ...

Modularity

- Reusability + Extendibility
- Favored by architectural techniques tending to ensure decentralization of modules

Some principles of modularity:
- Decomposability
- Composability
- Continuity
- Information hiding
- The open-closed principle
- The single choice principle
Decomposability

- Method helps decompose complex problems into subproblems.
- COROLLARY: Division of labor.
  - Example: Top-down design method (see next).
  - Counter-example: General initialization module.

Top-down functional design

Topmost functional abstraction

Top-down design


http://www.acm.org/classics/dec95/
**Composability**

- Method favors production of software elements that may be freely combined with each other to produce new software.

- Example: Unix shell conventions
  Program1 | Program2 | Program3

**Direct mapping**

- Method yields software systems whose modular structure remains compatible with any modular structure devised in the process of modeling the problem domain.

**Few interfaces principle**

- Every module communicates with as few others as possible.

(A)  (B)  (C)
**Small interfaces principle**

- If two modules communicate, they exchange as little information as possible.

![Diagram](image)

**Explicit interfaces principle**

- Whenever two modules $A$ and $B$ communicate, this is obvious from the text of $A$ or $B$ or both.

![Diagram](image)

**Continuity**

- Method ensures that small changes in specifications yield small changes in architecture.

  - Design method: Specification $\rightarrow$ Architecture

  - Example: Principle of Uniform Access (see next)
  - Counter-example: Programs with patterns after the physical implementation of data structures.
Uniform Access Principle

- Facilities managed by a module are accessible to its clients in the same way whether implemented by computation or by storage.

- Definition: A client of a module is any module that uses its facilities.

Uniform Access: An example

\[ \text{balance} = \text{list of deposits}.\text{total} - \text{list of withdrawals}.\text{total} \]

(A1)

\[
\begin{array}{ccc}
\text{list of deposits} & \text{list of withdrawals} & \text{balance} \\
\end{array}
\]

(A2)

\[
\begin{array}{ccc}
\text{list of deposits} & \text{list of withdrawals} \\
\end{array}
\]

Ada, Pascal, C/C++, Java, C#: Simula, Eiffel:

- \text{a.balance}
- \text{balance(a)}

Information hiding

- Underlying question: how does one "advertise" the capabilities of a module?

- Every module should be known to the outside world through an official, "public" interface.

- The rest of the module's properties comprises its "secrets".

- It should be impossible to access the secrets from the outside.
### Information Hiding Principle

- The designer of every module must select a subset of the module’s properties as the official information about the module, to be made available to authors of client modules.

### Information hiding

- Justifications:
  - Continuity
  - Decomposability
The Open-Closed Principle

- Modules should be open and closed.

- Definitions:
  - Open module: May be extended.
  - Closed module: Usable by clients. May be approved, baselined and (if program unit) compiled.

- The rationales are complementary:
  - For closing a module (manager's perspective): Clients need it now.
  - For keeping modules open (developer's perspective): One frequently overlooks aspects of the problem.

An object has an interface

An object has an implementation
Information hiding

The Open-Closed principle

Closing modules prematurely

(type PUBLICATION = record
  author, title: STRING;
  publication_year: INTEGER
  case pubtype: (book, journal, conference) of
    book: (publisher: STRING);
    journal: (editor: STRING);
    conference: (place, chair: STRING)
  end
end

Use in clients:

  p: PUBLICATION;
  case p.pubtype of
    book: ... p.publisher ...;
    journal: ... p.editor ...;
    conference: ... p.place ...
The Single Choice principle

- Whenever a software system must support a set of alternatives, one and only one module in the system should know their exhaustive list.
- Editor: set of commands (insert, delete etc.)
- Graphics system: set of figure types (rectangle, circle etc.)
- Compiler: set of language constructs (instruction, loop, expression etc.)

Reusability issues

- Organizational and managerial issues:
  - (Not covered here.)

- Technical issues: what form of components?
  - Routine libraries
  - Packages (Ada)
  - Class libraries
  - What form of classes?

Reusability: Technical issues

- The general pattern for a searching routine:

  ```
  has (t: TABLE; x: ELEMENT): BOOLEAN is
  -- Does item x appear in table t?
  local
  pos: POSITION
  do
    from pos := initial_position (t, x)
    until exhausted (t, pos) or else found (t, x, pos)
    loop
      pos := next (t, x, pos)
      if found (t, x, pos) then
        Result := found (t, x, pos)
    end
  end
  ```
Issues for a general searching module

- **Type variation:**
  - What are the table elements?

- **Routine grouping:**
  - A searching routine is not enough: it should be coupled with routines for table creation, insertion, deletion etc.

- **Implementation variation:**
  - Many possible choices of data structures and algorithms: sequential table (sorted or unsorted), array, binary search tree, file, ...

Issues

- **Representation independence:**
  - Can a client request an operation such as table search (has) without knowing what implementation is used internally?

  \[ \text{has} \ (t1, y) \]

Issues

- **Factoring out commonality:**
  - How can the author of supplier modules take advantage of commonality within a subset of the possible implementations?
  - Example: the set of sequential table implementations.
  - A common routine text for `has`:

    ```
    \text{has} \ (\ldots; \ x; \ T) :: \text{BOOLEAN} \ = \\
    \begin{array}{l}
    \text{-- Does x appear in the table?} \\
    \text{do} \\
    \text{from} \\
    \text{start} \\
    \text{until} \\
    \text{after} \\
    \text{otherwise} \\
    \text{found} \\
    \text{loop} \\
    \text{forth} \\
    \text{end} \\
    \text{Result} := \text{found} \ (x) \\
    \text{end} \\
    \end{array}
    ```
Factoring out commonality

Implementation variants

<table>
<thead>
<tr>
<th>start</th>
<th>forth</th>
<th>after</th>
<th>found (x)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Array</td>
<td>i := 1</td>
<td>i := i + 1</td>
<td>i &gt; count</td>
</tr>
<tr>
<td>Linked list</td>
<td>c := first.next</td>
<td>c := c.next</td>
<td>c = Void</td>
</tr>
<tr>
<td>File</td>
<td>rewind</td>
<td>read</td>
<td>end_of_file</td>
</tr>
</tbody>
</table>
Encapsulation languages ("Object-based")

- Ada, Modula-2, CLU...
- **Basic idea:** gather a group of routines serving a related purpose, such as `has`, `insert`, `remove` etc., together with the appropriate data structure descriptions.
- This addresses the Related Routines issue.
- **Advantages:**
  - For supplier author: Get everything under one roof. Simplifies configuration management, change of implementation, addition of new primitives.
  - For client author: Find everything at one place. Simplifies search for existing routines, requests for extensions.

Complementary material

- OOSC2:
  - Chapter 3: Modularity
  - Chapter 4: Approaches to reusability

End of lecture 2