SPARK - correctness by construction

Kim Rostgaard Christensen

DTU – Technical University of Denmark

Nov 30 2010

Outline

1. Correctness by construction
2. Design-by-contract
3. Example
4. Proving correctness
5. Gains and tradeoffs
6. Design-by-contract
7. Blocks
8. Verbatim
9. Finding documentation
10. DTU stuff

Correctness by construction

Putting engineering back into software engineering

- CbyC challenges testing and debugging
- Proves the software is correct
- Introduces a formalism
  - Elaborates requirements
  - Design-by-contract

Design-by-contract?

The fine print

- Translate requirements to a formal language
- Use this as the specification
- Hold the implementation to this
- Use automated tools
    - Not subject to human error
- Upon validation failure, either
    - The implementation is wrong (potentially)
    - The specification is wrong, redesign

Example contract?

What does it look like

```
procedure Increment (X : in out Counter_Type);
--# global Count;
--# derives
--#    Count from Count, X &
--#    X from ;
```

Proving correctness?

Quod erat demonstrandum

Gains

The good, the bad and the ugly

- Formal and systematic approach to development
- Better control
- Proof == 100% correctness (according to specification)
- Forces you to spend time on design
- Dictates modularity
- Improves maintainability

Challenges

The good, the bad and the ugly

- Formal and systematic approach to development
- Better control
- Proof == 100% correctness (according to specification)
- Forces you to spend time on design
- Dictates modularity
- Improves maintainability

Design-by-contract?

This is the first column. It occupies 40% of the text width.

This is the second column. This could be a nice image...

Use blocks to highlight your points

<The title of the block>

This is the point you want to highlight. It could be an important formula

$$a^2 + b^2 = c^2$$

Example

The example block is useful for typesetting examples consistently.

Verbatim material

If the slide contains verbatim material you must use the `fragile` option for the frame.

```
This is verbatim text
!"#%&/()=?
```

The `listings` package can be used for more fancy verbatim text and pretty printing of source code.

Beamer documentation

The Beamer userguide is available on-line at CTAN:

```
ftp://tug.ctan.org/pub/tex-archive/macros/latex/
contrib/beamer/doc/beameruserguide.pdf
```

If Beamer is installed on your system you can find the manual by running

```
mthelp beamer
```

in a Command Prompt.

The template

This presentation template is a beamer implementation of the official DTU PowerPoint template available at

http://portalen.dtu.dk/Services/Kommunikation.aspx

To follow the design guidelines completely, you should use the colors from the DTU color palette

http://portalen.dtu.dk/upload/ak/design/
dtu-farvemanual_03_07_2006.pdf

These colors are defined in the DTU beamer theme with the names shown on the next slide.

DTU colors

⬛ dtudarkgray	⬛ dtugray	⬜ dtulightgray
🟦 dtudarkblue	🟦 dtublue	🟦 dtulightblue
🟥 dtured	🟪 dtupurpur	🟪 dtupurple
🟧 dtudarkorange	🟧 dtuorange	🟨 dtuyellow
🟩 dtudarkgreen	🟩 dtugreen	