

Contract-based Software Development

Rasmus Guldberg Pedersen

January 2015

Overview

1 Code Contracts

2 Verification

- Side-effects
- Validity
- Conceptual

3 Testing

Code Contracts

Is Code contract a tool supporting verification or test, or both?
Discuss and give examples.

Code Contracts (.NET tool)

Express preconditions, postconditions and object invariants for:

Code Contracts (.NET tool)

Express preconditions, postconditions and object invariants for:

- Static analysis

Code Contracts (.NET tool)

Express preconditions, postconditions and object invariants for:

- Static analysis
- Documentation

Code Contracts (.NET tool)

Express preconditions, postconditions and object invariants for:

- Static analysis
- Documentation
- Runtime checking

Managing side-effects

Can NOT do

- Enforce pureness

Managing side-effects

Can NOT do

- Enforce pureness
- Capture all side-effects in postconditions

Managing side-effects

Can NOT do

- Enforce pureness
- Capture all side-effects in postconditions
- Enforce method calls

Managing side-effects

Can NOT do

- Enforce pureness
- Capture all side-effects in postconditions
- Enforce method calls

Can do

- Calls in contracts are “pure”

Validity of assertions

$$\{Q\}S\{R\}$$

Conceptual

Verify our conception model

Testing

- Doesn't exercise code

Testing

- Doesn't exercise code
- Fail early

Testing

- Doesn't exercise code
- Fail early
- Test promises

The End

*“Testing shows the presence, not the absence of bugs.”
— Edsger W. Dijkstra*