Softwaretechnik

Lecture 13: Design by Contract

Peter Thiemann

University of Freiburg, Germany

25.06.2012

Table of Contents

Contracts for Procedural Programs

Reminder: Underlying Idea

Transfer the notion of contract between business partners to software engineering

What is a contract?

A binding agreement that explicitly states the **obligations** and the **benefits** of each partner

Example: Contract between Builder and Landowner

	Obligations	**Benefits**
Landowner	Provide 5 acres of land; pay for building if completed in time	Get building in less than six months
Builder	Build house on provided land in less than six month	No need to do anything if provided land is smaller than 5 acres; Receive payment if house finished in time

Who are the contract partners in SE?

Partners can be modules/procedures, objects/methods, components/operations, ...

In terms of software architecture, the partners are the components and each connector may carry a contract.

Contracts for Procedural Programs

- Goal: Specification of imperative procedures
- Approach: give **assertions** about the procedure
  - Precondition
    - must be true on entry
    - ensured by caller of procedure
  - Postcondition
    - must be true on exit
    - ensured by procedure **if it terminates**
- **Precondition**(*State*) $\Rightarrow$ **Postcondition**(**procedure**(*State*))
- Notation: {**Precondition**} **procedure** {**Postcondition**}
- Assertions stated in first-order predicate logic

Example

Consider the following procedure:

```
/**
 * @param a an integer
 * @returns integer square root of a
 */
int root (int a) {
  int i = 0;
  int k = 1;
  int sum = 1;
  while (sum <= a) {
    k = k+2;
    i = i+1;
    sum = sum+k;
  }
  return i;
}
```

Specification of root

- types guaranteed by compiler: $\mathtt{a} \in \mathtt{integer}$ and $\mathtt{root} \in \mathtt{integer}$ (the result)

1. root as a partial function
   Precondition: $\mathtt{a} \geq 0$
   Postcondition: $\mathtt{root} * \mathtt{root} \leq \mathtt{a} < (\mathtt{root} + 1) * (\mathtt{root} + 1)$
2. root as a total function
   Precondition: **true**
   Postcondition:

$$
\begin{array}{lcl}
(\mathtt{a} \geq 0 & \Rightarrow & \mathtt{root} * \mathtt{root} \leq \mathtt{a} < (\mathtt{root} + 1) * (\mathtt{root} + 1)) \\
\wedge & & \\
(\mathtt{a} < 0 & \Rightarrow & \mathtt{root} = 0)
\end{array}
$$

Weakness and Strength

Goal:

- find weakest precondition
  a precondition that is implied by all other preconditions
  highest demand on procedure
  largest domain of procedure
  (Q: what if precondition = **false**?)
- find strongest postcondition
  a postcondition that implies all other postconditions
  smallest range of procedure
  (Q: what if postcondition = **true**?)

Met by "root as a total function":

- **true** is weakest possible precondition
- "defensive programming"

Example (Weakness and Strength)

Consider root as a function over integers

Precondition: **true**

Postcondition:

$$\begin{array}{l}(\mathtt{a} \geq 0 \quad \Rightarrow \quad \mathtt{root} * \mathtt{root} \leq \mathtt{a} < (\mathtt{root} + 1) * (\mathtt{root} + 1)) \\ \wedge \\ (\mathtt{a} < 0 \quad \Rightarrow \quad \mathtt{root} = 0)\end{array}$$

- **true** is the weakest precondition
- The postcondition can be strengthened to

$$\begin{array}{lll}(\mathtt{root} \geq 0) \;\wedge & & \\ (\mathtt{a} \geq 0 & \Rightarrow & \mathtt{root} * \mathtt{root} \leq \mathtt{a} < (\mathtt{root} + 1) * (\mathtt{root} + 1)) \;\wedge \\ (\mathtt{a} < 0 & \Rightarrow & \mathtt{root} = 0)\end{array}$$

An Example

Insert an element in a table of fixed size

```
class TABLE<T> {
  int capacity; // size of table
  int count; // number of elements in table
  T get (String key) {...}
  void put (T element, String key);
}
```

Precondition: table is not full

$$\texttt{count} < \texttt{capacity}$$

Postcondition: new element in table, count updated

$$\begin{array}{ll} & \texttt{count} \leq \texttt{capacity} \\ \wedge & \texttt{get}(\texttt{key}) = \texttt{element} \\ \wedge & \texttt{count} = \textbf{old}\ \texttt{count} + 1 \end{array}$$

	Obligations	**Benefits**
Caller	Call `put` only on non-full table	Get modified table in which `element` is associated with `key`
Procedure	Insert `element` in table so that it may be retrieved through `key`	No need to deal with the case where table is full before insertion

Contracts for Object-Oriented Programs

Contracts for Object-Oriented Programs

Contracts for methods have additional complications

- local state
  receiving object's state must be specified
- inheritance and dynamic method dispatch
  receiving object's type may be different than statically expected;
  method may be overridden

Local State ⇒ Class Invariant

- class invariant *INV* is predicate that holds for all objects of the class

⇒ must be established by all constructors

⇒ must be maintained by all visible methods

Pre- and Postconditions for Methods

- constructor methods c

$$\{\mathbf{Pre}_c\}\ c\ \{INV\}$$

- visible methods m

$$\{\mathbf{Pre}_m \wedge INV\}\ m\ \{\mathbf{Post}_m \wedge INV\}$$

Table example revisited

- count and capacity are instance variables of class TABLE
- $\mathit{INV}_{\texttt{TABLE}}$ is $\texttt{count} \le \texttt{capacity}$
- specification of `void put (T element, String key)`

  Precondition:

  $$\texttt{count} < \texttt{capacity}$$

  Postcondition:

  $$\texttt{get}(\texttt{key}) = \texttt{element} \wedge \texttt{count} = \textbf{old}\ \texttt{count} + 1$$

Inheritance and Dynamic Binding

- Subclass may override a method definition
- Effect on specification:
  - Subclass may have different invariant
  - Redefined methods may
    - have different pre- and postconditions
    - raise different exceptions
    - $\Rightarrow$ *method specialization*
- Relation to invariant and pre-, postconditions in base class?
- Guideline: *No surprises requirement* (Wing, FMOODS 1997)
  Properties that users rely on to hold of an object of type T should hold even if the object is actually a member of a subtype S of T.

Invariant of a Subclass

Suppose

class MYTABLE **extends** TABLE ...

- each property expected of a `TABLE` object should also be granted by a `MYTABLE` object
- if o has type `MYTABLE` then $INV_{\texttt{TABLE}}$ must hold for o

$\Rightarrow$ $INV_{\texttt{MYTABLE}} \Rightarrow INV_{\texttt{TABLE}}$

- Example: `MYTABLE` might be a hash table with invariant

$$INV_{\texttt{MYTABLE}} \equiv \texttt{count} \leq \texttt{capacity}/3$$

Method Specialization

If `MYTABLE` redefines `put` then ...

- the new **precondition must be weaker** and
- the new **postcondition must be stronger**

because in

```
TABLE cast = new MYTABLE (150);
...
cast.put (new Terminator (3), "Arnie");
```

the caller

- only guaranties $\mathbf{Pre}_{\texttt{put},\texttt{Table}}$
- and expects $\mathbf{Post}_{\texttt{put},\texttt{Table}}$

Requirements for Method Specialization

Suppose class T defines method m with assertions $\mathbf{Pre}_{T,m}$ and $\mathbf{Post}_{T,m}$ throwing exceptions $\mathbf{Exc}_{T,m}$. If class S extends class T and redefines m then the redefinition is a sound method specialization if

- $\mathbf{Pre}_{T,m} \Rightarrow \mathbf{Pre}_{S,m}$ and
- $\mathbf{Post}_{S,m} \Rightarrow \mathbf{Post}_{T,m}$ and
- $\mathbf{Exc}_{S,m} \subseteq \mathbf{Exc}_{T,m}$
  each exception thrown by $S.m$ may also be thrown by $T.m$

Example: MYTABLE.put

- $\textbf{Pre}_{\texttt{MYTABLE,put}} \equiv \texttt{count} < \texttt{capacity}/3$
  not a sound method specialization because it is not implied by $\texttt{count} < \texttt{capacity}$.
- MYTABLE may automatically resize the table, so that $\textbf{Pre}_{\texttt{MYTABLE,put}} \equiv \textbf{true}$ a sound method specialization because $\texttt{count} < \texttt{capacity} \Rightarrow \textbf{true}$!
- Suppose MYTABLE adds a new instance variable T lastInserted that holds the last value inserted into the table.

$$\begin{aligned}\textbf{Post}_{\texttt{MYTABLE,put}} \equiv \quad & \texttt{item(key)} = \texttt{element} \\ \wedge \quad & \texttt{count} = \textbf{old}\ \texttt{count} + 1 \\ \wedge \quad & \texttt{lastInserted} = \texttt{element}\end{aligned}$$

  is sound method specialization because
  $\textbf{Post}_{\texttt{MYTABLE,put}} \Rightarrow \textbf{Post}_{\texttt{TABLE,insert}}$

Interlude: Method Specialization in Java 5

- Overriding methods in Java 5 only allows specialization of the result type. (It can be replaced by a subtype).
- The parameter types muss stay unchanged (why?)

Example : Assume A **extends** B

```
class C {
  A m () {
    return new A();
  }
}
class D extends C {
  B m () { // overrides method C.m()
    return new B();
  }
}
```

Contract Monitoring

Contract Monitoring

- What happens if a system's execution violates an assertion at run time?
- A violating execution runs outside the system's specification.
- The system's reaction may be **arbitrary**
  - crash
  - continue

Contract Monitoring

- What happens if a system's execution violates an assertion at run time?
- A violating execution runs outside the system's specification.
- The system's reaction may be **arbitrary**
  - crash
  - continue

Contract Monitoring

- evaluates assertions at run time
- raises an exception indicating any violation
- assign blame for the violation

Contract Monitoring

- What happens if a system's execution violates an assertion at run time?
- A violating execution runs outside the system's specification.
- The system's reaction may be **arbitrary**
  - crash
  - continue

Contract Monitoring

- evaluates assertions at run time
- raises an exception indicating any violation
- assign blame for the violation

Why monitor?

- Debugging (with different levels of monitoring)
- Software fault tolerance (*e.g.*, α and β releases)

What can go wrong

precondition: evaluate assertion on entry
identifies problem in the caller

postcondition: evaluate assertion on exit
identifies problem in the callee

invariant: evaluate assertion on entry and exit
problem in the callee's class

hierarchy: unsound method specialization
need to check (for all superclasses T of S)

- $\mathbf{Pre}_{T,m} \Rightarrow \mathbf{Pre}_{S,m}$ on entry and
- $\mathbf{Post}_{S,m} \Rightarrow \mathbf{Post}_{T,m}$ on exit

how?

Hierarchy Checking

Suppose `class` S `extends` T and overrides a method m.
Let $T\ x = $ `new` $S()$ and consider $x.m()$

- on entry
  - if $\mathbf{Pre}_{T,m}$ holds, then $\mathbf{Pre}_{S,m}$ must hold, too
  - $\mathbf{Pre}_{S,m}$ must hold
- on exit
  - $\mathbf{Post}_{S,m}$ must hold
  - if $\mathbf{Post}_{S,m}$ holds, then $\mathbf{Post}_{T,m}$ must hold, too
- in general: cascade of implications between S and T
- pre- and postcondition only checked for S!
- If the precondition of S is not fulfilled, but the one of T is, then this is a wrong method specialization.

Examples

```
interface IConsole {
  int getMaxSize();
    @post { getMaxSize > 0 }
  void display (String s);
    @pre { s.length () < this.getMaxSize() }
}

class Console implements IConsole {
  int getMaxSize () { ... }
    @post { getMaxSize > 0 }
  void display (String s) { ... }
    @pre { s.length () < this.getMaxSize() }
```

A Good Extension

```
class RunningConsole extends Console {
  void display (String s) {
    ...
    super.display(String. substring (s, ..., ... + getMaxSize()))
    ...
  }
    @pre { true }
}
```

A Bad Extension

```
class PrefixedConsole extends Console {
  String getPrefix() {
    return ">> ";
  }
  void display (String s) {
    super.display (this.getPrefix() + s);
  }
    @pre { s.length() < this.getMaxSize() - this.getPrefix().length() }
}
```

- caller may only guarantee `IConsole`'s precondition
- Console.display can be called with to long argument
- blame the programmer of `PrefixedConsole`!

Properties of Monitoring

- Assertions can be arbitrary side effect-free boolean expressions
- Instrumentation for monitoring can be generated from the assertions
- Monitoring can only prove the presence of violations, not their absence
- Absence of violations can only be guaranteed by formal verification

Verification of Contracts

Verification of Contracts

- Given: Specification of imperative **procedure** by **Precondition** and **Postcondition**
- Goal: Formal proof for
  Precondition(*State*) ⇒ **Postcondition**(**procedure**(*State*))
- Method: **Hoare Logic**, *i.e.*, a proof system for **Hoare triples** of the form

  {**Precondition**} **procedure** {**Postcondition**}

- named after C.A.R. Hoare, the inventor of Quicksort, CSP, and many other
- here: method bodies, no recursion, no pointers (extensions exist)

Syntax

$$
\begin{array}{lcll}
E & ::= & c \mid x \mid E + E \mid \ldots & \text{expressions} \\
B, P, Q & ::= & \neg B \mid P \wedge Q \mid P \vee Q & \text{boolean expressions} \\
 & \mid & E = E \mid E \leq E \mid \ldots & \\
C, D & ::= & x{=}E & \text{assignment} \\
 & \mid & C;D & \text{sequence} \\
 & \mid & \texttt{if } B \texttt{ then } C \texttt{ else } D & \text{conditional} \\
 & \mid & \texttt{while } B \texttt{ do } C & \text{iteration} \\
 & & & \\
\mathcal{H} & ::= & \{P\}C\{Q\} & \text{Hoare triples}
\end{array}
$$

- (boolean) expressions are free of side effects

Semantics — Domains and Types

$$\begin{array}{lcl} \mathit{BValue} & = & \mathtt{true} \mid \mathtt{false} \\ \mathit{IValue} & = & 0 \mid 1 \mid \dots \\ \sigma \in \mathit{State} & = & \mathit{Variable} \to \mathit{Value} \end{array}$$

$$\begin{array}{lcl} \mathcal{E}[\![]\!] & : & \mathit{Expression} \times \mathit{State} \to \mathit{IValue} \\ \mathcal{B}[\![]\!] & : & \mathit{BoolExpression} \times \mathit{State} \to \mathit{BValue} \\ \mathcal{S}[\![]\!] & : & \mathit{State}_\perp \to \mathit{State}_\perp \end{array}$$

- $\mathit{State}_\perp := \mathit{State} \cup \{\perp\}$
- result $\perp$ indicates non-termination

Semantics — Expressions

$$
\begin{array}{lcl}
\mathcal{E}[\![c]\!]\sigma & = & c \\
\mathcal{E}[\![x]\!]\sigma & = & \sigma(x) \\
\mathcal{E}[\![E+F]\!]\sigma & = & \mathcal{E}[\![E]\!]\sigma + \mathcal{E}[\![F]\!]\sigma \\
\ldots & & \\
\mathcal{B}[\![E=F]\!]\sigma & = & \mathcal{E}[\![E]\!]\sigma = \mathcal{E}[\![F]\!]\sigma \\
\mathcal{B}[\![\neg B]\!]\sigma & = & \neg\mathcal{B}[\![B]\!]\sigma \\
\ldots & &
\end{array}
$$

Semantics — Statements

$$
\begin{array}{lcl}
\mathcal{S}[\![C]\!]\bot & = & \bot \\
\mathcal{S}[\![\texttt{skip}]\!]\sigma & = & \sigma \\
\mathcal{S}[\![x{=}E]\!]\sigma & = & \sigma[x \mapsto \mathcal{E}[\![E]\!]\sigma] \\
\mathcal{S}[\![C;D]\!]\sigma & = & \mathcal{S}[\![D]\!](\mathcal{S}[\![C]\!]\sigma) \\
\mathcal{S}[\![\texttt{if }B\texttt{ then }C\texttt{ else }D]\!]\sigma & = & \mathcal{B}[\![B]\!]\sigma = \texttt{true} \to \mathcal{S}[\![C]\!]\sigma\ ,\ \mathcal{S}[\![D]\!]\sigma \\
\mathcal{S}[\![\texttt{while }B\texttt{ do }C]\!]\sigma & = & F(\sigma) \\
\qquad\qquad \textit{where} \quad F(\sigma) & = & \mathcal{B}[\![B]\!]\sigma = \texttt{true} \to F(\mathcal{S}[\![C]\!]\sigma)\ ,\ \sigma
\end{array}
$$

- McCarthy conditional: $b \to e_1, e_2$

Proving a Hoare triple

$$\{P\}\ C\ \{Q\}$$

- holds if $(\forall \sigma \in \mathit{State})\ P(\sigma) \Rightarrow (Q(\mathcal{S}[\![C]\!]\sigma) \vee \mathcal{S}[\![C]\!]\sigma = \bot)$
  (partial correctness)
- alternative reading/notation: $P, Q \subseteq \mathit{State}$
  $\{P\}\ C\ \{Q\} \equiv \mathcal{S}[\![C]\!]P \subseteq Q \cup \bot$
- reading predicates as boolean expressions
  $\mathcal{B}[\![P]\!]\sigma = \texttt{true} \Rightarrow (\mathcal{B}[\![Q]\!](\mathcal{S}[\![C]\!]\sigma) = \texttt{true} \vee \mathcal{S}[\![C]\!]\sigma = \bot)$

Proof Rules for Hoare Triples

- Proving that $\{P\}\ C\ \{Q\}$ holds directly from the definition is tedious
- Instead: define axioms and inferences rules
- Construct a derivation to prove the triple
- Choice of axioms and rules guided by structure of C

Skip Axiom

$$\{P\}\ \texttt{skip}\ \{P\}$$

Skip Axiom

$$\{P\}\ \texttt{skip}\ \{P\}$$

Correctness

- $\mathcal{S}[\![\texttt{skip}]\!]\sigma = \sigma$
- $\mathcal{S}[\![\texttt{skip}]\!]P = P$

Assignment Axiom

$$\{P[x \mapsto E]\}\ x = E\ \{P\}$$

Examples:

- $\{1 == 1\}\ x = 1\ \{x == 1\}$
- $\{odd(1)\}\ x = 1\ \{odd(x)\}$
- $\{x == 2 * y + 1\}\ y = 2 * y\ \{x == y + 1\}$

Assignment Axiom — Correctness

$$\{P[x \mapsto E]\}\ x = E\ \{P\}$$

- Semantics $\mathcal{S}[\![x{=}E]\!]\sigma = \sigma[x \mapsto \mathcal{E}[\![E]\!]\sigma]$
- Have to show
  $\mathcal{B}[\![P[x \mapsto E]]\!]\sigma = \texttt{true} \Rightarrow$
  $(\mathcal{B}[\![P]\!](\mathcal{S}[\![x = E]\!]\sigma) = \texttt{true} \vee \mathcal{S}[\![x = E]\!]\sigma = \bot)$
- By induction on P; result of $\mathcal{B}[\![E' \rho E'']\!]\sigma$ must remain the same; result of $\mathcal{E}[\![E']\!]\sigma$ must remain the same
- Sufficient to show $\mathcal{E}[\![E'[x \mapsto E]]\!]\sigma = \mathcal{E}[\![E']\!]\sigma[x \mapsto \mathcal{E}[\![E]\!]\sigma]$
- Holds because $\mathcal{E}[\![x[x \mapsto E]]\!]\sigma = \mathcal{E}[\![E]\!]\sigma = \mathcal{E}[\![x]\!]\sigma[x \mapsto \mathcal{E}[\![E]\!]\sigma]$

Sequence Rule

$$\frac{\{P\}\ C\ \{R\} \qquad \{R\}\ D\ \{Q\}}{\{P\}\ C;D\ \{Q\}}$$

Example:

$$\frac{\{x == 2*y+1\}\ y = 2*y\ \{x == y+1\} \qquad \{x == y+1\}\ y = y+1\ \{x == y\}}{\{x == 2*y+1\}\ y = 2*y; y = y+1\ \{x == y\}}$$

Sequence Rule

$$\frac{\{P\}\ C\ \{R\} \qquad \{R\}\ D\ \{Q\}}{\{P\}\ C;D\ \{Q\}}$$

Example:

$$\frac{\{x == 2 * y + 1\}\ y = 2 * y\ \{x == y + 1\} \qquad \{x == y + 1\}\ y = y + 1\ \{x == y\}}{\{x == 2 * y + 1\}\ y = 2 * y; y = y + 1\ \{x == y\}}$$

Correctness

- If $\sigma \in P$ then $\sigma' = \mathcal{S}[\![C]\!]\sigma \in R \cup \{\bot\}$
- If $\sigma' = \bot$ then $\mathcal{S}[\![D]\!]\bot = \bot$
- If $\sigma' \in R$ then $\mathcal{S}[\![D]\!]\sigma' \in Q \cup \{\bot\}$
- Hence: $\sigma \in P \Rightarrow \mathcal{S}[\![C; D]\!]\sigma \in Q \cup \{\bot\}$

Conditional Rule

$$\frac{\{P \wedge B\}\ C\ \{Q\} \qquad \{P \wedge \neg B\}\ D\ \{Q\}}{\{P\}\ \texttt{if}\ B\ \texttt{then}\ C\ \texttt{else}\ D\ \{Q\}}$$

Conditional Rule

$$\frac{\{P \wedge B\}\ C\ \{Q\} \qquad \{P \wedge \neg B\}\ D\ \{Q\}}{\{P\}\ \texttt{if}\ B\ \texttt{then}\ C\ \texttt{else}\ D\ \{Q\}}$$

Correctness

- Show: $\sigma \in P$ implies $\mathcal{S}[\![\texttt{if}\ B\ \texttt{then}\ C\ \texttt{else}\ D]\!] \in Q \cup \{\bot\}$
- Exercize

Conditional Rule — Issues

Examples:

$$\frac{\{P \wedge x < 0\}\ z = -x\ \{z == |x|\} \qquad \{P \wedge x \geq 0\}\ z = x\ \{z == |x|\}}{\{P\}\ \texttt{if}\ x < 0\ \texttt{then}\ z = -x\ \texttt{else}\ z = x\ \{z == |x|\}}$$

- incomplete!
- precondition for $z = -x$ should be $(z == |x|)[z \mapsto -x] \equiv -x == |x|$

$\Rightarrow$ need *logical rules*

Logical Rules

- weaken precondition

$$\frac{P' \Rightarrow P \qquad \{P\}\ C\ \{Q\}}{\{P'\}\ C\ \{Q\}}$$

- strengthen postcondition

$$\frac{\{P\}\ C\ \{Q\} \qquad Q \Rightarrow Q'}{\{P\}\ C\ \{Q'\}}$$

- Example needs strengthening: $P \wedge x < 0 \Rightarrow -x == |x|$
- holds if $P \equiv$ **true**!
- similarly: $P \wedge x \geq 0 \Rightarrow x == |x|$

Logical Rules

- weaken precondition

$$\frac{P' \Rightarrow P \qquad \{P\}\ C\ \{Q\}}{\{P'\}\ C\ \{Q\}}$$

- strengthen postcondition

$$\frac{\{P\}\ C\ \{Q\} \qquad Q \Rightarrow Q'}{\{P\}\ C\ \{Q'\}}$$

- Example needs strengthening: $P \wedge x < 0 \Rightarrow -x == |x|$
- holds if $P \equiv$ **true**!
- similarly: $P \wedge x \geq 0 \Rightarrow x == |x|$

Correctness

$P' \Rightarrow P$ iff $P' \subseteq P$ (as set of states)

Completed example:

$$\mathcal{D}_1 = \frac{x < 0 \Rightarrow -x == |x| \qquad \{-x == |x|\}\ z = -x\ \{z == |x|\}}{\{x < 0\}\ z = -x\ \{z == |x|\}}$$

$$\mathcal{D}_2 = \frac{x \geq 0 \Rightarrow x == |x| \qquad \{x == |x|\}\ z = x\ \{z == |x|\}}{\{x \geq 0\}\ z = x\ \{z == |x|\}}$$

$$\frac{\dfrac{\mathcal{D}_1}{\{x < 0\}\ z = -x\ \{z == |x|\}} \qquad \dfrac{\mathcal{D}_2}{\{x \geq 0\}\ z = x\ \{z == |x|\}}}{\{\textbf{true}\}\ \texttt{if}\ x < 0\ \texttt{then}\ z = -x\ \texttt{else}\ z = x\ \{z == |x|\}}$$

While Rule

$$\frac{\{P \land B\}\ C\ \{P\}}{\{P\}\ \texttt{while}\ B\ \texttt{do}\ C\ \{P \land \neg B\}}$$

- P is *loop invariant*

Example: try to prove

```
{ a>=0 /\ i==0 /\ k==1 /\ sum==1 }
while sum <= a do
  k = k+2;
  i = i+1;
  sum = sum+k
{ i*i <= a /\ a < (i+1)*(i+1) }
```

$\Rightarrow$ while rule not directly applicable ...

While Rule

Step 1: Find the loop invariant

```
a>=0 /\ i==0 /\ k==1 /\ sum==1
=>
i*i<=a /\ i>=0 /\ k==2*i+1 /\ sum==(i+1)*(i+1)
```

- $P \equiv i * i \leq a \wedge i \geq 0 \wedge k == 2 * i + 1 \wedge sum == (i + 1) * (i + 1)$ holds on entry to the loop
- To prove that P is an invariant, requires to prove that $\{P \wedge sum \leq a\}\ k = k + 2; i = i + 1; sum = sum + k\ \{P\}$
- It follows by the sequence rule and weakening:

Proof of loop invariance

```
{ i*i<=a /\ i>=0   /\ k==2*i+1     /\ sum==(i+1)*(i+1) /\ sum<=a }
{           i>=0   /\ k+2==2+2*i+1 /\ sum==(i+1)*(i+1) /\ sum<=a }
k = k+2
{           i>=0   /\ k==2+2*i+1   /\ sum==(i+1)*(i+1) /\ sum<=a }
{           i+1>=1 /\ k==2*(i+1)+1 /\ sum==(i+1)*(i+1) /\ sum<=a }
i = i+1
{           i>=1   /\ k==2*i+1     /\ sum==i*i         /\ sum<=a }
{ i*i<=a /\ i>=1   /\ k==2*i+1     /\ sum+k==i*i+k     /\ sum+k<=a+k }
sum = sum+k
{ i*i<=a /\ i>=1   /\ k==2*i+1     /\ sum==i*i+k       /\ sum<=a+k }
{ i*i<=a /\ i>=1   /\ k==2*i+1     /\ sum==i*i+2*i+1   /\ sum<=a+k }
{ i*i<=a /\ i>=1   /\ k==2*i+1     /\ sum==(i+1)*(i+1) /\ sum<=a+k }
{ i*i<=a /\ i>=0   /\ k==2*i+1     /\ sum==(i+1)*(i+1) }
```

Step 2: Apply the while rule

$$\frac{\{P \wedge sum \leq a\}\ k = k + 2; i = i + 1; sum = sum + k\ \{P\}}{\{P\}\ \texttt{while}\ sum \leq a\ \texttt{do}\ k = k + 2; i = i + 1; sum = sum + k\ \{P \wedge sum > a\}}$$

Now, $P \wedge sum > a$ is

```
  { i*i<=a /\ i>=0   /\ k==2*i+1   /\ sum==(i+1)*(i+1) /\ sum>a }
implies
  { i*i<=a /\ a<(i+1)*(i+1) }
```

Correctness of While-Rule

$$\frac{\{P \wedge B\}\ C\ \{P\}}{\{P\}\ \texttt{while}\ B\ \texttt{do}\ C\ \{P \wedge \neg B\}}$$

- Consider $\mathcal{S}[\![\texttt{while}\ B\ \texttt{do}\ C]\!]\sigma = F(\sigma)$
  where $F(\sigma) = \mathcal{B}[\![B]\!]\sigma = \texttt{true} \rightarrow F(\mathcal{S}[\![C]\!]\sigma), \sigma$
- Case $\forall n \in \mathbb{N}$, $\mathcal{B}[\![B]\!](\mathcal{S}[\![C]\!]^{(n)}\sigma) = \texttt{true}$: set $F(\sigma) = \bot$.
- Case $\exists n \in \mathbb{N}$, $\mathcal{B}[\![B]\!](\mathcal{S}[\![C]\!]^{(n)}\sigma) = \texttt{false}$: let n_0 be minimal
- Let $\sigma \in P = (P \wedge B) \uplus (P \wedge \neg B)$
- Case $n_0 = 0$: $\sigma \in P \wedge \neg B$, then $F(\sigma) = \sigma \in P \wedge \neg B$. OK.
- Case $n_0 > 0$: $\sigma \in P \wedge B$, then $\sigma' = \mathcal{S}[\![C]\!]\sigma \in P \cup \{\bot\}$ by assumption.
  By induction, $F(\sigma') = \mathcal{S}[\![C]\!]^{(n_0-1)}\sigma' \in P \wedge \neg B \cup \{\bot\}$

Properties of Formal Verification

- requires more restrictions on assertions (e.g., use a certain logic) than monitoring
- full compliance of code with specification can be guaranteed
- scalability is a challenging research topic:
  - full automatization
  - manageable for small/medium examples
  - large examples require manual interaction
  - real programs use arrays and dynamic datastructures (pointers, objects)