System Modelling and Design

Square Root

Revision: March 2, 2011

Ken Robinson

School of Computer Science & Engineering
The University of New South Wales, Sydney Australia

March 2, 2011

©Ken Robinson 2005-2010
mailto:k.robinson@unsw.edu.au
Outline

What is this example about?

The Problem

Contexts

Substitution

The SquareRoot machine

SquareRoot event

First refinement

Improving low and high

Second refinement

The third refinement

The fourth refinement

Alternative refinement sequence

Extracting code
This example presents the modelling (design) of a simple numerical algorithm, namely integer square root.

The focus of the development is on understanding how each step fits, so that the correctness of the development as a whole is clear from the steps.

Discharge of proof obligations gives confidence in the correctness in the final algorithm.

It is important to appreciate that our focus is not principally on numeric algorithms; square root gives us a simple starting point.

The example is interesting because it is not easy to see how to verify the initial model. The verification is finally produced by refining to a concrete model (that is an algorithm) that produces the square root.
This example presents the modelling (design) of a simple numerical algorithm, namely integer square root.

The focus of the development is on understanding how each step fits, so that the correctness of the development as a whole is clear from the steps.

Discharge of proof obligations gives confidence in the correctness in the final algorithm.

It is important to appreciate that our focus is not principally on numeric algorithms; square root gives us a simple starting point.

The example is interesting because it is not easy to see how to verify the initial model. The verification is finally produced by refining to a concrete model (that is an algorithm) that produces the square root.
This example presents the modelling (design) of a simple numerical algorithm, namely integer square root.

The focus of the development is on understanding how each step fits, so that the correctness of the development as a whole is clear from the steps.

Discharge of proof obligations gives confidence in the correctness in the final algorithm.

It is important to appreciate that our focus is not principally on numeric algorithms; square root gives us a simple starting point.

The example is interesting because it is not easy to see how to verify the initial model. The verification is finally produced by refining to a concrete model (that is an algorithm) that produces the square root.
This example presents the modelling (design) of a simple numerical algorithm, namely integer square root.

The focus of the development is on understanding how each step fits, so that the correctness of the development as a whole is clear from the steps.

Discharge of proof obligations gives confidence in the correctness in the final algorithm.

It is important to appreciate that our focus is not principally on numeric algorithms; square root gives us a simple starting point.

The example is interesting because it is not easy to see how to verify the initial model. The verification is finally produced by refining to a concrete model (that is an algorithm) that produces the square root.
What is this example about?

This example presents the modelling (design) of a simple numerical algorithm, namely integer square root.

The focus of the development is on understanding how each step fits, so that the correctness of the development as a whole is clear from the steps.

Discharge of proof obligations gives confidence in the correctness in the final algorithm.

It is important to appreciate that our focus is not principally on numeric algorithms; square root gives us a simple starting point.

The example is interesting because it is not easy to see how to verify the initial model. The verification is finally produced by refining to a concrete model (that is an algorithm) that produces the square root.
This example presents the modelling (design) of a simple numerical algorithm, namely integer square root.

The focus of the development is on understanding how each step fits, so that the correctness of the development as a whole is clear from the steps.

Discharge of proof obligations gives confidence in the correctness in the final algorithm.

It is important to appreciate that our focus is not principally on numeric algorithms; square root gives us a simple starting point.

The example is interesting because it is not easy to see how to verify the initial model. The verification is finally produced by refining to a concrete model (that is an algorithm) that produces the square root.
The Problem

The problem is to compute the integer square root of some natural number value \textit{num}.

The definition of the integer square root of \textit{num} is the largest natural number that when squared does not exceed \textit{num}, that is

\[
sqrt(num) \times sqrt(num) \leq num \quad (1)
\]
\[
(sqrt(num) + 1) \times (sqrt(num) + 1) > num \quad (2)
\]
The problem is to compute the integer square root of some natural number value $num$.

The definition of the integer square root of $num$ is the largest natural number that when squared does not exceed $num$, that is

$$\sqrt(num) \times \sqrt(num) \leq num \quad (1)$$

$$(\sqrt(num) + 1) \times (\sqrt(num) + 1) > num \quad (2)$$
The Problem

The problem is to compute the integer square root of some natural number value \( num \).

The definition of the integer square root of \( num \) is the largest natural number that when squared does not exceed \( num \), that is

\[
\sqrt{num} \times \sqrt{num} \leq num \tag{1}
\]

\[
(\sqrt{num} + 1) \times (\sqrt{num} + 1) > num \tag{2}
\]
We use a context to present a number of theorems concerning natural numbers. These will be useful for assisting the discharge of proof obligations.

**CONTEXT**

**Theories**

**AXIOMS**

\( \text{thm1: } \left( \forall n \cdot n \in \mathbb{N} \Rightarrow \left( \exists m \cdot m \in \mathbb{N} \land (n = 2 \cdot m \lor n = 2 \cdot m + 1) \right) \right) \)

\( \text{thm2: } \left( \forall n \cdot n \in \mathbb{N} \Rightarrow n < (n + 1) \cdot (n + 1) \right) \)

\( \text{thm3: } \forall m, n \cdot m \in \mathbb{N} \land n \in \mathbb{N} \land m < n \Rightarrow (m + n)/2 < n \)

\( \text{thm4: } \forall m, n \cdot m \in \mathbb{N} \land n \in \mathbb{N} \land m < n \Rightarrow (m + n)/2 \geq m \)

END
SquareRoot_ctx: context

We use another context to define a constant \( num \) that is any natural number. \( num \) is essentially used as an argument of the event \( sqrt \) in the SquareRoot machine.

This context \textit{extends} the \textit{Theories} context.

\begin{verbatim}
CONTEXT SquareRoot_ctx
EXTENDS Theories
CONSTANTS
    num
AXIOMS
    axm1: num \in \mathbb{N}
END
\end{verbatim}
Event-B has three forms of *substitution* for changing the value assigned to a variable:

1. *becomes equal:* $x := e$, $x$ becomes equal to the value of the expression $e$;

2. *becomes such that:* $x : | p$, $x$ becomes a value that satisfies the predicate $p$. Within the predicate $p$ $x$ represents the value of the variable $x$ before the substitution and $x'$ represents the value of the variable $x$ after the substitution.

3. *becomes in:* $x : \in s$, $x$ becomes any value in the set $s$

$x := x + 1$ and $x : | x' = x + 1$ are equivalent.
Substitution

Event-B has three forms of substitution for changing the value assigned to a variable:

1. becomes equal: $x := e$, $x$ becomes equal to the value of the expression $e$;

2. becomes such that: $x :| p$, $x$ becomes a value that satisfies the predicate $p$. Within the predicate $p$ $x$ represents the value of the variable $x$ before the substitution and $x'$ represents the value of the variable $x$ after the substitution.

3. becomes in: $x \in s$, $x$ becomes any value in the set $s$

$x := x + 1$ and $x :| x' = x + 1$ are equivalent.
Substitution

Event-B has three forms of *substitution* for changing the value assigned to a variable:

1. *becomes equal*: \( x := e \), \( x \) becomes equal to the value of the expression \( e \);

2. *becomes such that*: \( x :| p \), \( x \) becomes a value that satisfies the predicate \( p \). Within the predicate \( p \) \( x \) represents the value of the variable \( x \) before the substitution and \( x' \) represents the value of the variable \( x \) after the substitution.

3. *becomes in*: \( x :\in s \), \( x \) becomes any value in the set \( s \)

\( x := x + 1 \) and \( x :| x' = x + 1 \) are equivalent.
Substitution

Event-B has three forms of substitution for changing the value assigned to a variable:

1. *becomes equal*: \( x := e \), \( x \) becomes equal to the value of the expression \( e \);

2. *becomes such that*: \( x :| p \), \( x \) becomes a value that satisfies the predicate \( p \). Within the predicate \( p \) \( x \) represents the value of the variable \( x \) before the substitution and \( x' \) represents the value of the variable \( x \) after the substitution.

3. *becomes in*: \( x \in s \), \( x \) becomes any value in the set \( s \)

\( x := x + 1 \) and \( x :| x' = x + 1 \) are equivalent.
Event-B has three forms of *substitution* for changing the value assigned to a variable:

1. *becomes equal*: \( x := e \), \( x \) becomes equal to the value of the expression \( e \);

2. *becomes such that*: \( x :| p \), \( x \) becomes a value that satisfies the predicate \( p \). Within the predicate \( p \) \( x \) represents the value of the variable \( x \) before the substitution and \( x' \) represents the value of the variable \( x \) after the substitution.

3. *becomes in*: \( x \in s \), \( x \) becomes any value in the set \( s \)

\( x := x + 1 \) and \( x :| x' = x + 1 \) are equivalent.
We now develop a SquareRoot machine.

The machine

- sees the context;
- has a variable $sqrt$ that will be used to store the square root of the constant (parameter) $num$. Initially $sqrt$ is assigned any natural number ($sqrt \in \mathbb{N}$).
MACHINE SquareRoot

SEES SquareRoot_ctx

VARIABLES

sqrt

ININVARIANTS

inv1 : sqrt ∈ \mathbb{N}

EVENTS

Initialisation

begin

act1 : sqrt ∈ \mathbb{N}

end
Event \textit{SquareRoot} \textit{≜}

begin

\textbf{act1:} \quad \text{sqrt} : | (\text{sqrt}' \in \mathbb{N})
\qquad \land \text{sqrt}' \ast \text{sqrt}' \leq \text{num}
\qquad \land \text{num} < (\text{sqrt}' + 1) \ast (\text{sqrt}' + 1))

end

END
SquareRoot event

Note the use of $\|\|$ to make a *declarative* assignment to $sqrt$ using the predicates determined earlier for the definition of $square$ root.

This form of assignment requires that $sqrt$ is assigned a value consistent with the definition of square root given in (1) and (2) above.
SquareRoot event

Note the use of $\frac{r}{r'}$ to make a *declarative* assignment to $\textit{sqrt}$ using the predicates determined earlier for the definition of *square root*.

This form of assignment requires that $\textit{sqrt}$ is assigned a value consistent with the definition of square root given in (1) and (2) above.
First refinement

The current assignment to \( \textit{sqrt} \), while obviously correct — that is consistent with the definition given in predicates 1 and 2 — is abstract. We will refine to a concrete model, that is an algorithm.

The problem with the predicate

\[
\textit{sqrt}' \times \textit{sqrt}' \leq \textit{num} \land \textit{num} < (\textit{sqrt}' + 1) \times (\textit{sqrt}' + 1)
\]

is that it contains a conjunction of two properties for \( \textit{sqrt}' \) each easy to satisfy on their own, but together much more difficult.

We split this conjunction into two predicates, each with a different variable as follows:

\[
\textit{low} \times \textit{low} \leq \textit{num}
\]

and

\[
\textit{num} < \textit{high} \times \textit{high}
\]

and contrive to bring \( \textit{low} \) and \( \textit{high} \) closer together until

\[
\textit{high} = \textit{low} + 1
\]

at which point \( \textit{low} \) will be the required square root.
First refinement

The current assignment to $sqrt$, while obviously correct —that is consistent with the definition given in predicates 1 and 2— is abstract. We will refine to a concrete model, that is an algorithm.

The problem with the predicate

$$sqrt' \ast sqrt' \leq num \land num < (sqrt' + 1) \ast (sqrt' + 1)$$

is that it contains a conjunction of two properties for $sqrt'$ each easy to satisfy on their own, but together much more difficult.

We split this conjunction into two predicates, each with a different variable as follows:

$$low \ast low \leq num$$

and

$$num < high \ast high$$

and contrive to bring $low$ and $high$ closer together until

$$high = low + 1$$

at which point $low$ will be the required square root.
First refinement

The current assignment to sqrt, while obviously correct —that is consistent with the definition given in predicates 1 and 2— is abstract. We will refine to a concrete model, that is an algorithm.

The problem with the predicate

$$\sqrt{'} \ast \sqrt{'} \leq \text{num} \land \text{num} < (\sqrt{'} + 1) \ast (\sqrt{'} + 1)$$

is that it contains a conjunction of two properties for sqrt' each easy to satisfy on their own, but together much more difficult.

We split this conjunction into two predicates, each with a different variable as follows:

$$\text{low} \ast \text{low} \leq \text{num}$$

and

$$\text{num} < \text{high} \ast \text{high}$$

and contrive to bring low and high closer together until

$$\text{high} = \text{low} + 1$$

at which point low will be the required square root.
MACHINE SquareRootR1
REFINES SquareRoot
SEES SquareRoot_ctx
VARIABLES
   sqrt
   low
   high

INvariants
inv1: low ∈ ℕ
inv2: high ∈ ℕ
inv3: low + 1 ≤ high
inv4: low * low ≤ num
inv5: num < high * high
EVENTS

Initialisation

begin

act1: \( \text{sqrt} \in \mathbb{N} \)

act2: \( \text{low} : \mid (\text{low}' \in \mathbb{N} \land \text{low}' \times \text{low}' \leq \text{num}) \)

act3: \( \text{high} : \mid (\text{high}' \in \mathbb{N} \land \text{num} < \text{high}' \times \text{high}') \)

end
Event \( SquareRoot \uparrow \)
refines \( SquareRoot \)
when
\[ grd1 : \; \text{low} + 1 = \text{high} \]
then
\[ act1 : \; \text{sqrt} := \text{low} \]
end
Event  \emph{Improve}  \triangleright

\textbf{Status} convergent

\begin{align*}
\text{any} & \quad l \\
\text{any} & \quad h \\
\text{when} & \end{align*}

\begin{align*}
grd1 & : \quad \text{low} + 1 \neq \text{high} \\
grd2 & : \quad l \in \mathbb{N} \land \text{low} \leq l \land l \ast l \leq \text{num} \\
grd3 & : \quad h \in \mathbb{N} \land h \leq \text{high} \land \text{num} < h \ast h \\
grd4 & : \quad l + 1 \leq h \\
grd5 & : \quad h - l < \text{high} - \text{low} \\
\text{then} & \\
\text{act1} & : \quad \text{low}, \text{high} := l, h \\
\text{end} & \\
\end{align*}
VARIANT

high – low

END
Improving low and high

As shown in the above, the refinement of $SquareRoot$ fires only when $low + 1 = high$. We need a new event to bring that about.

We introduce a new event $Improve$ that brings $low$ and $high$ closer together, while maintaining the invariant relation on those variables.

It is important to observe the parameters $l$ and $h$ together with appropriate guards (constraints) that describe necessary properties, without perhaps knowledge of how those parameters can be instantiated. This style of specification is sometimes called declarative.
Improving low and high

As shown in the above, the refinement of $SquareRoot$ fires only when $\textit{low} + 1 = \textit{high}$. We need a new event to bring that about.

We introduce a new event $\textit{Improve}$ that brings $\textit{low}$ and $\textit{high}$ closer together, while maintaining the invariant relation on those variables.

It is important to observe the parameters $l$ and $h$ together with appropriate guards (constraints) that describe necessary properties, without perhaps knowledge of how those parameters can be instantiated. This style of specification is sometimes called \textit{declarative}. 
Improving low and high

As shown in the above, the refinement of \textit{SquareRoot} fires only when \textit{low} + 1 = \textit{high}. We need a new event to bring that about.

We introduce a new event \textit{Improve} that brings \textit{low} and \textit{high} closer together, while maintaining the invariant relation on those variables.

It is important to observe the parameters \textit{l} and \textit{h} together with appropriate guards (constraints) that describe necessary properties, without perhaps knowledge of how those parameters can be instantiated. This style of specification is sometimes called \textit{declarative}. 
The specification of *Improve* is abstract, simply requiring that either *low* is increased, or *high* is decreased, or both, without showing how that may be achieved concretely.

In order to ensure that *SquareRoot* will eventually fire, the new event must be convergent, that is it must terminate in a finite number of firings. We give a variant expression, which must yield a natural number value that is guaranteed to decrease on each execution of *Improve*.

Since either *low* is increased or *high* is decreased and \( low + 1 \leq high \) an adequate expression is \( high - low \).
The specification of *Improve* is abstract, simply requiring that either \textit{low} is increased, or \textit{high} is decreased, or both, without showing how that may be achieved concretely.

In order to ensure that *SquareRoot* will eventually fire, the new event must be convergent, that is it must terminate in a finite number of firings. We give a variant expression, which must yield a natural number value that is guaranteed to decrease on each execution of *Improve*.

Since either \textit{low} is increased or \textit{high} is decreased and \textit{low} + 1 \leq \textit{high}

an adequate expression is \textit{high} – \textit{low}. 
The specification of *Improve* is abstract, simply requiring that either *low* is increased, or *high* is decreased, or both, without showing how that may be achieved concretely.

In order to ensure that *SquareRoot* will eventually fire, the new event must be convergent, that is it must terminate in a finite number of firings. We give a variant expression, which must yield a natural number value that is guaranteed to decrease on each execution of *Improve*.

Since either *low* is increased or *high* is decreased and \( low + 1 \leq high \) an adequate expression is \( high - low \).
We now do a second refinement in which we refine the *Improve* event, mapping out how we can produce a better value of *low* or *high*. The idea is to take a value *mid* that is strictly between *low* and *high* and test whether *mid* is a better replacement for *low* or *high* and replace those values accordingly.

We know that such a value exists because *low* + 1 ≤ *high* and also *low* + 1 ≠ *high*, so *low* + 1 < *high* implying that there is at least one value between *low* and *high*.

In this refinement *Improve* is refined two ways into *Improve*1 and *Improve*2 depending on whether *low* or *high* is improved, respectively.

**Witnesses:** The refinements of *Improve* have eliminated the parameters *l* and *h*, so we are required to show how those parameters are represented by the refinement. This is achieved by the *with* clause, which shows the values of those parameters.
MACHINE SquareRootR2
REFINES SquareRootR1
SEES SquareRoot_ctx

VARIABLES

sqrt
low
high
EVENTS

Initialisation

begin

act1: \texttt{sqrt} \in \mathbb{N}

act2: \texttt{low} :| (\texttt{low'} \in \mathbb{N} \land \texttt{low'} \ast \texttt{low'} \leq \texttt{num})

act3: \texttt{high} :| (\texttt{high'} \in \mathbb{N} \land \texttt{num} < \texttt{high'} \ast \texttt{high'})

end
Event \textit{SquareRoot} \sqsupseteq 
refines \textit{SquareRoot} 
when 
grd1 : \textit{low} + 1 = \textit{high} 
then 
act1 : \textit{sqrt} := \textit{low} 
end
Event  $\text{Improve1} \sqsupset
$
refines $\text{Improve}$

any  $m$

when

grd1 : $\text{low + 1} \neq \text{high}$
grd2 : $m \in \mathbb{N}$
grd3 : $\text{low} < m \land m < \text{high}$
grd4 : $m \ast m \leq \text{num}$

with

  $l : l = m$
  $h : h = \text{high}$

then

act1 : $\text{low} := m$

end
Event \( \text{Improve2} \equiv \)
refines \( \text{Improve} \)
any \( m \)
when
\( \text{grd1: low + 1 } \neq \text{high} \)
\( \text{grd2: } m \in \mathbb{N} \)
\( \text{grd3: low } < m \land m < \text{high} \)
\( \text{grd4: num } < m \ast m \)
with
\( l: l = \text{low} \)
\( h: h = m \)
then
\( \text{act1: high := m} \)
end
\( \text{END} \)
The third refinement

The third refinement refines the abstract specifications to concrete expressions.

1. We compute the initial values of \( low \) and \( high \) as 0 and \( num + 1 \) respectively. We could find better initial values, but since the performance is going to be logarithmic, it may not be worth the expense of more complicated computations.

2. In \( SquareRootR3 \) we refine \( Improve \) two ways, each with a parameter \( m \) set to the value \( (low + high)/2 \), that is we introduce the midpoint value between \( low \) and \( high \).

This is not the only option, we could have used \( low + 1 \) or \( high - 1 \); any value that is strictly between —and not equal to— \( low \) and \( high \).

The difference is one of performance, not correctness. Taking the mid point will give logarithmic performance, while incrementing or decrementing will give linear performance.
The third refinement

The third refinement refines the abstract specifications to concrete expressions.

1. We compute the initial values of \( \text{low} \) and \( \text{high} \) as 0 and \( \text{num} + 1 \) respectively. We could find better initial values, but since the performance is going to be logarithmic, it may not be worth the expense of more complicated computations.

2. In \( \text{SquareRootR3} \) we refine \( \text{Improve} \) two ways, each with a parameter \( m \) set to the value \( (\text{low} + \text{high})/2 \), that is we introduce the midpoint value between \( \text{low} \) and \( \text{high} \).

This is not the only option, we could have used \( \text{low} + 1 \) or \( \text{high} - 1 \); any value that is strictly between —and not equal to— \( \text{low} \) and \( \text{high} \).

The difference is one of performance, not correctness. Taking the mid point will give logarithmic performance, while incrementing or decrementing will give linear performance.
The third refinement

The third refinement refines the abstract specifications to concrete expressions.

1. We compute the initial values of $low$ and $high$ as 0 and $num + 1$ respectively. We could find better initial values, but since the performance is going to be logarithmic, it may not be worth the expense of more complicated computations.

2. In $SquareRootR3$ we refine $Improve$ two ways, each with a parameter $m$ set to the value $(low + high)/2$, that is we introduce the midpoint value between $low$ and $high$.

This is not the only option, we could have used $low + 1$ or $high − 1$; any value that is strictly between —and not equal to— $low$ and $high$.

The difference is one of performance, not correctness. Taking the mid point will give logarithmic performance, while incrementing or decrementing will give linear performance.
The third refinement

The third refinement refines the abstract specifications to concrete expressions.

1. We compute the initial values of low and high as 0 and num + 1 respectively. We could find better initial values, but since the performance is going to be logarithmic, it may not be worth the expense of more complicated computations.

2. In SquareRootR3 we refine improve two ways, each with a parameter m set to the value (low + high)/2, that is we introduce the midpoint value between low and high. This is not the only option, we could have used low + 1 or high – 1; any value that is strictly between —and not equal to— low and high.

The difference is one of performance, not correctness. Taking the mid point will give logarithmic performance, while incrementing or decrementing will give linear performance.
The third refinement

The third refinement refines the abstract specifications to concrete expressions.

1. We compute the initial values of low and high as 0 and num + 1 respectively. We could find better initial values, but since the performance is going to be logarithmic, it may not be worth the expense of more complicated computations.

2. In SquareRootR3 we refine Improve two ways, each with a parameter m set to the value \((low + high)/2\), that is we introduce the midpoint value between low and high. This is not the only option, we could have used low + 1 or high − 1; any value that is strictly between —and not equal to— low and high. The difference is one of performance, not correctness. Taking the mid point will give logarithmic performance, while incrementing or decrementing will give linear performance.
MACHINE SquareRootR3
REFINES SquareRootR2
SEES SquareRoot_ctx
VARIABLES
  sqrt
  low
  high
EVENTS

Initialisation

begin

act1: \texttt{sqrt} \in \mathbb{N}

act2: \texttt{low} := 0

act3: \texttt{high} := \texttt{num} + 1

end
Event  \( \text{SquareRoot} \Rightarrow \)
refines  \( \text{SquareRoot} \)
when
\[ \text{grd1} : \quad \text{low} + 1 = \text{high} \]
then
\[ \text{act1} : \quad \text{sqrt} := \text{low} \]
end
Event \textit{Improve1} \cong
defines \textit{Improve1}
  any \quad m
  when
  \text{grd1} : \textit{low} + 1 \neq \textit{high}
  \text{grd2} : m = (\textit{low} + \textit{high})/2
  \text{grd3} : m \ast m \leq \textit{num}
  then
  \text{act1} : \textit{low} := m
  end
Event $Improve2$ ☉
refines $Improve2$

any $m$
when

$grd1$: $low + 1 \neq high$
$grd2$: $m = (low + high)/2$
$grd3$: $num < m \ast m$

then

$act1$: $high := m$

end

END
In the third refinement we still have an abstract element in the form of the parameter $m$ to the events $\text{Improve}1$ and $\text{Improve}2$.

The value of $m$ has to be produced, nondeterministically, to satisfy the guards of $\text{Improve}1$.

In $\text{SquareRootR4}$ we introduce another variable, $\text{mid}$, to replace the parameter $m$. 

The fourth refinement
The fourth refinement

In the third refinement we still have an abstract element in the form of the parameter $m$ to the events $Improve1$ and $Improve2$.

The value of $m$ has to be produced, nondeterministically, to satisfy the guards of $Improve1$.

In $SquareRootR4$ we introduce another variable, $mid$, to replace the parameter $m$. 
The fourth refinement

In the third refinement we still have an abstract element in the form of the parameter $m$ to the events $Improve1$ and $Improve2$.

The value of $m$ has to be produced, nondeterministically, to satisfy the guards of $Improve1$.

In $SquareRootR4$ we introduce another variable, $mid$, to replace the parameter $m$. 
MACHINE SquareRootR4
REFINES SquareRootR3
SEES SquareRoot_ctx
VARIABLES
  sqrt
  low
  high
  mid

INVARIANTS
  inv1: mid = (low + high)/2
EVENTS

Initialisation

begin

act1 : $\sqrt{\cdot} \in \mathbb{N}$

act2 : $low := 0$

act3 : $high := num + 1$

act4 : $mid := (num + 1)/2$

end
Event  $\textit{SquareRoot} \supseteq$
refines  $\textit{SquareRoot}$
when
$\text{grd1} : \textit{low} + 1 = \textit{high}$
then
$\text{act1} : \textit{sqrt} := \textit{low}$
end
Event \textit{Improve1} \Unrefines \textit{Improve1} 
refines \textit{Improve1} when

\text{grd1} : \text{low} + 1 \neq \text{high}
\text{grd2} : \text{mid} \ast \text{mid} \leq \text{num}

with

\text{m} : \text{m} = \text{mid}

then

\text{act1} : \text{low} := \text{mid}
\text{act2} : \text{mid} := (\text{mid} + \text{high})/2

end
Event \textit{Improve2} \equiv 
refines \textit{Improve2} 
when 
grd1: \textit{low} + 1 \neq \textit{high} 
grd2: \textit{num} < \textit{mid} \ast \textit{mid} 
with 
m: m = \textit{mid} 
then 
act1: \textit{high} := \textit{mid} 
act2: \textit{mid} := (\textit{low} + \textit{mid})/2 
end 
END
Instead of the refinement sequence $\text{SquarerootR3A}, \text{SquarerootR4}$, we could have effectively gone directly to $\text{SquareRootR4}$ from $\text{SquareRootR2}$ and this is shown in $\text{SquareRootR3B}$.

**Historical note:** the presentation sequence of a model development is frequently different to the chronological sequence. Refinement to $\text{SquarerootR3B}$ was the original refinement step from $\text{SquarerootR2}$. The extra step via $\text{SquarerootR3A}$ to $\text{SquarerootR4}$ was added later.
MACHINE SquareRootR3B
REFINES SquareRootR2
SEES SquareRoot_ctx

VARIABLES
\[ \text{sqrt}, \text{low}, \text{high}, \text{mid} \]

INvariants
\[ \text{inv1: } \text{mid} \in \mathbb{N} \]
\[ \text{inv2: } \text{mid} = (\text{low} + \text{high})/2 \]
\[ \text{inv3: } \text{low} \leq \text{mid} \]
\[ \text{inv4: } \text{mid} < \text{high} \]
EVENTS

Initialisation

begin

act1: $sqrt \in \mathbb{N}$
act2: $low := 0$
act3: $high := num + 1$
act4: $mid := (num + 1)/2$

end
Event $SquareRoot \equiv$
refines $SquareRoot$
when
$grd1: low + 1 = high$
then
$act1: sqrt := low$
end
Event \( \text{Improve1} \supseteq \)
refines \( \text{Improve1} \)
when
\[ \text{grd1} : \; low + 1 \neq high \]
\[ \text{grd2} : \; mid \times mid \leq num \]
with
\[ m : \; m = mid \]
then
\[ \text{act1} : \; low := mid \]
\[ \text{act2} : \; mid := (mid + high)/2 \]
end
Event \textit{Improve2} \refines \textit{Improve2}

when

grd1: \textit{low} + 1 \neq \textit{high}

grd2: \textit{num} < \textit{mid} \ast \textit{mid}

with

m: \textit{m} = \textit{mid}

then

act1: \textit{high} := \textit{mid}

act2: \textit{mid} := (\textit{low} + \textit{mid})/2

end

END
If the final refinement is examined carefully, it is clear that the events can be replaced by a loop:

- the subsidiary events $Improve_1$ and $Improve_2$ execute until $low + 1 = high$
- at which point the loop terminates and the final square root is computed.

Thus we can manually refine the final refinement to the following pseudo code.
If the final refinement is examined carefully, it is clear that the events can be replaced by a loop:

- the subsidiary events $\textit{Improve1}$ and $\textit{Improve2}$ execute until $low + 1 = high$
- at which point the loop terminates and the final square root is computed.

Thus we can manually refine the final refinement to the following pseudo code.
If the final refinement is examined carefully, it is clear that the events can be replaced by a loop:

- the subsidiary events $\text{Improve1}$ and $\text{Improve2}$ execute until $\text{low} + 1 = \text{high}$
- at which point the loop terminates and the final square root is computed.

Thus we can manually refine the final refinement to the following pseudo code.
Extracting code

If the final refinement is examined carefully, it is clear that the events can be replaced by a loop:

- the subsidiary events $Improve1$ and $Improve2$ execute until $low + 1 = high$
- at which point the loop terminates and the final square root is computed.

Thus we can manually refine the final refinement to the following pseudo code.
low := 0;
high := num + 1;

while low + 1 ≠ high {
    mid := (low + high)/2
    if mid * mid ≤ num{
        low := mid
    }
    else high := mid
}

sqrt := low