Principled Programming

Introduction to Coding in Any Imperative Language

Tim Teitelbaum

Emeritus Professor
Department of Computer Science
Cornell University

Specifications and Implementations

We describe the specification of various kinds of programming-language constructs, and how their implementations contribute to a program that meets its requirements:

- *Statements*, which define effects.
- *Declarations*, which create program variables.
- *Methods*, which group *statements* and *declarations* into meaningful operations.
- *Classes*, which aggregate *methods* and *declarations* into coherent modules.

Programs serve a purpose. They satisfy a requirement.

Programs serve a purpose. They satisfy a requirement.

Some requirements are small: Square a number.

Some requirements are large: Control a rocket to the moon.

Regardless, our goal is to write a program that satisfies a requirement.

A specification, written as comment, is a precise articulation of a requirement.

```
/* Specification. */
```

An implementation, indented beneath it, says how meet the requirement.

```
/* Specification. */
   Implementation
```

Statement Specifications

Implementations

Statement Specifications

Implementations

Write specifications as imperatives that say what must be accomplished.

```
/* Specification. */
   Implementation
```

Example

```
/* Specification. */
   Implementation
```

Write specifications as imperatives that say what must be accomplished.

```
/* Specification. */
   Implementation
```

Example

```
/* Output the square of an integer that is provided as input. */
   Implementation
```

Write implementations that say how to do so.

```
/* Specification. */
   Implementation
```

Example

```
/* Output the square of an integer that is provided as input. */
   int n = in.nextInt();
   System.out.println( n*n );
```

Statement Specifications

Implementations

A given specification can be implemented in multiple ways.

```
/* Specification. */
   Implementation
```

Example

```
/* Output the square of an integer that is provided as input. */
   int n = in.nextInt();
   /* Let s be the square of n. */
   System.out.println( s );
```

A given specification can be implemented in multiple ways.

```
/* Specification. */
   Implementation
```

Example

```
/* Output the square of an integer that is provided as input. */
   int n = in.nextInt();
   /* Let s be the square of n. */
      s = n*n;
   System.out.println( s );
```

Statement Specifications

Implementations

A given specification can be implemented in multiple ways.

```
/* Specification. */
   Implementation
```

Example

```
/* Output the square of an integer that is provided as input. */
   int n = in.nextInt();
   /* Let s be the square of n. */
      int m = Math.abs(n);
      int s = 0;
      for (int k=0; k<m; k++) s = s + m;
   System.out.println( s );
```

Specification Style

Write specifications as imperatives.

```
/* Output the square of an integer that is provided as input. */
   int n = in.nextInt(); System.out.println( n*n );
```

Avoid meandering descriptions.

Be succinct. Eliminate needless words.

```
/* Output the square of an integer that is provided as input. */
   int n = in.nextInt(); System.out.println( n*n );
```

☞ **Repeatedly improve comments by relentless copy editing.**

Statement Specifications

Specification Style

By convention, state input before output.

```
/* Input an integer, and output the square of that integer. */
   int n = in.nextInt(); System.out.println( n*n );
```

Use pronouns.

```
/* Input an integer, and output its square. */
   int n = in.nextInt(); System.out.println( n*n );
```

Use letters as pronouns.

```
/* Input integer k, and output k squared. */
   int n = in.nextInt(); System.out.println( n*n );
```

Statement Specifications

Specification Style

Use letters as pronouns.

```
/* Input integer j, and output j squared. */
   int n = in.nextInt(); System.out.println( n*n );
```

The scope of such a pronoun is local to the specification.

Use letters as pronouns, or as the names of variables.

```
/* Input integer n, and output n squared. */
   int n = in.nextInt(); System.out.println( n*n );
```

Statement Specifications

Specification Style

Use letters as pronouns, or as the names of variables.

```
/* Input integer n, and output n squared. */
   System.out.println( Math.pow(in.nextInt(),2) );
```

But in this implementation there is no variable n, so n is a pronoun.

Statement Specifications

Specification Style

Use programming-language *expressions*, if you wish.

```
/* Input integer n, and output n*n. */
   int n = in.nextInt(); System.out.println( n*n );
```

But an *expression* in a specification isn't necessarily computed.

```
/* Input integer x, and output the number n such that n*n=x. */
   System.out.println( Math.sqrt(in.nextInt()) );
```

Suppose, in a program, you need to exchange the values of variables x and y.

```
Program
```

Statement Specifications

Specs as Higher-Level Code

Write the specification as if in a higher-level programming language.

```
/* Swap x and y. */
```

☞ **Write comments as an integral part of the coding process, not as afterthoughts.**

Defer implementation so you don't get distracted. Move on to other matters.

```
/* Swap x and y. */
```

other matters

☞ **Write comments as an integral part of the coding process, not as afterthoughts.**

Or implement it now, if simple enough to not get distracted.

```
/* Swap x and y. */
   int temp = x;
   x = y;
   y = temp;
```

other matters

☞ **Write comments as an integral part of the coding process, not as afterthoughts.**

Then ignore it in considering the specification’s relationship to other matters.

```
/* Swap x and y. */
   int temp = x;
   x = y;
   y = temp;
```

other matters

Let your eye skip over the indented implementation

☞ **Write comments as an integral part of the coding process, not as afterthoughts.**

Then ignore it in considering the specification's relationship to other matters.

```
/* Swap x and y. */
   ...
```

other matters

Let your eye skip over the indented implementation as if it were elided.

☞ **Write comments as an integral part of the coding process, not as afterthoughts.**

An implementation can include another specification

```
/* Swap x and y. */
   /* Declare int variable temp and initialize it to x. */
   x = y;
   y = temp;
```

other matters

which is then implemented.

```
/* Swap x and y. */
    /* Declare int variable temp and initialize it to x. */
       int temp = x;
    x = y;
    y = temp;
```

other matters

A specification faces two directions, like the Roman god Janus.

```
/* Swap x and y. */
   /* Declare int variable temp and initialize it to x. */
      int temp = x;
   x = y;
   y = temp;
```

other matters

Outward, it is part of the implementation of an encompassing specification.

```
/* Swap x and y. */
   /* Declare int variable temp and initialize it to x. */
      int temp = x;
   x = y;
   y = temp;
```

other matters

Inward, it is a specification that is being implemented.

```
/* Swap x and y. */
   /* Declare int variable temp and initialize it to x. */
   int temp = x;
   x = y;
   y = temp;
```

other matters

Avoid redundant specifications that say the obvious.

```
/* Declare int variable temp and initialize it to x. */
   int temp = x;
```

other matters

☞ **Omit specifications whose implementations are at least as brief and clear as the specification itself.**

Avoid redundant specifications that say the obvious.

```
int temp = x;
```

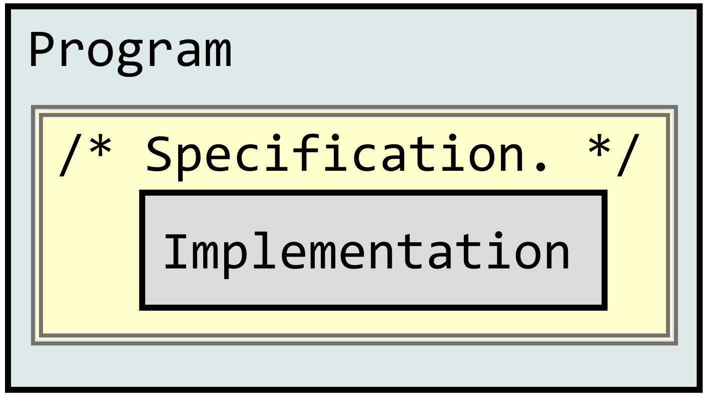
other matters

☞ **Omit specifications whose implementations are at least as brief and clear as the specification itself.**

Statement Specifications

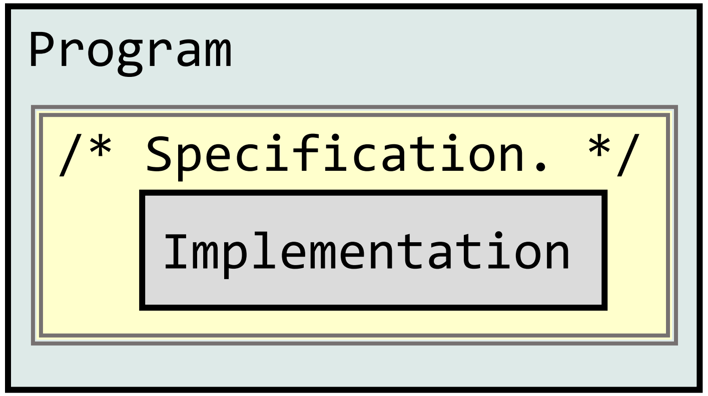
What? Not How?

A specification is a contract with the rest of the program that says *what* must be accomplished, not *how* to do so.



Proviso: As long as the program does this and that.
Promise: The specification (and its implementation) will do thus and such.

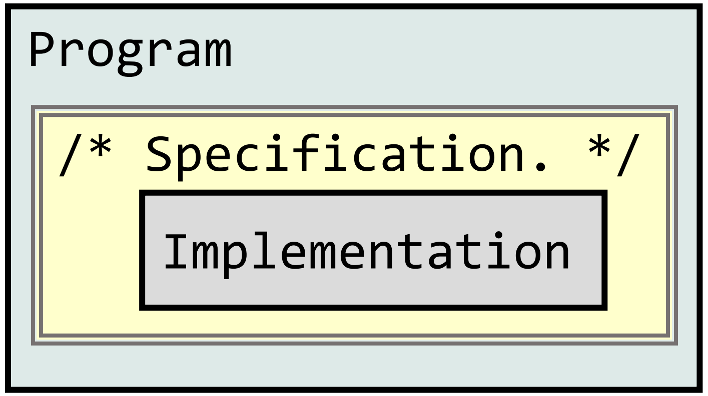
A specification helps to control complexity.



The contract (double line) partitions code into the specification and its implementation (on the one hand), and the rest of the program (on the other).

Statement Specifications
What? Not How?

A specification is both constraining and liberating.

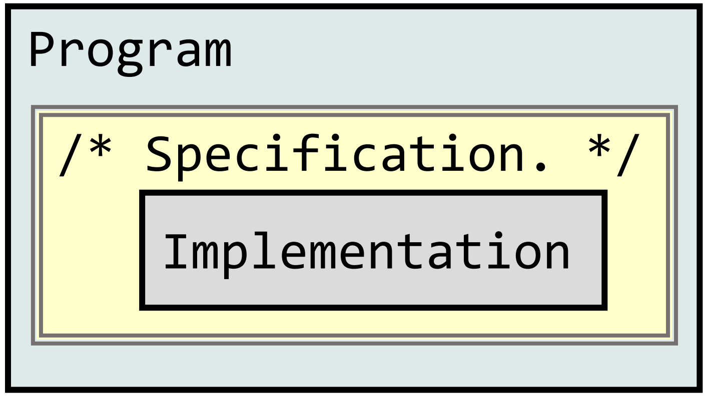


Constraining: (If the proviso is met) then it must do what is required.
Liberating: But its implementation is free to do so in any way it wants.

Statement Specifications

What? Not How?

A specification promotes pliability and comprehensibility.



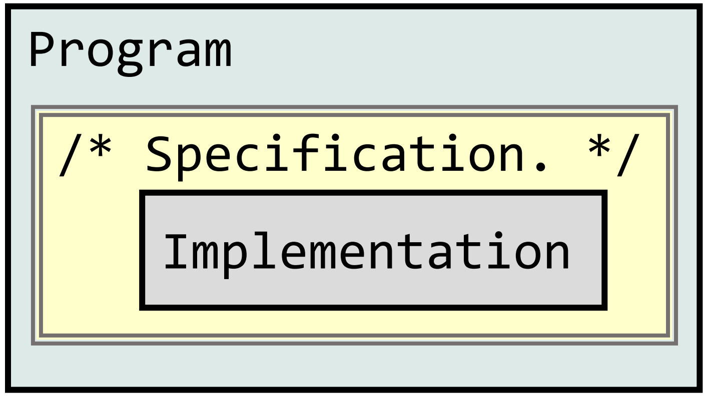
Pliability: The implementation can be changed without affecting the rest of the program.

Comprehensibility: The program can ignore implementation details not mentioned by the specification.

Statement Specifications

What? Not How?

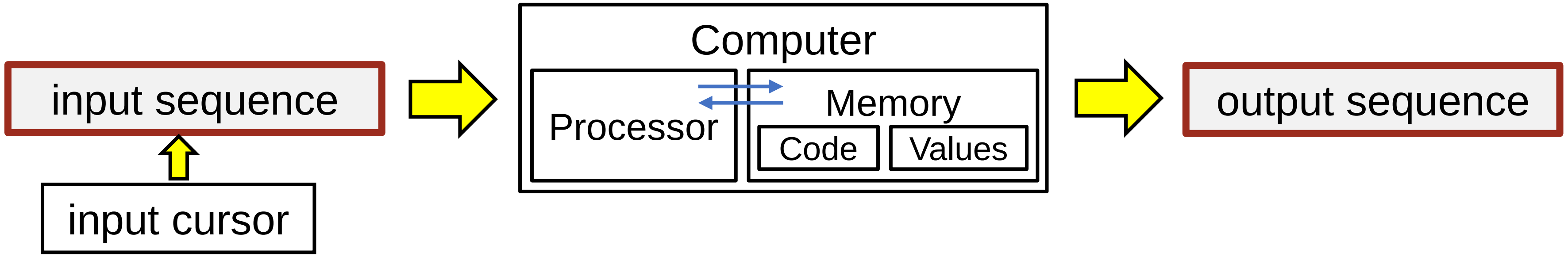
Specifications encapsulate details and hide information behind abstraction barriers.



These notions are central to object-oriented programming (discussed later, but already relevant at the level of statement specifications).

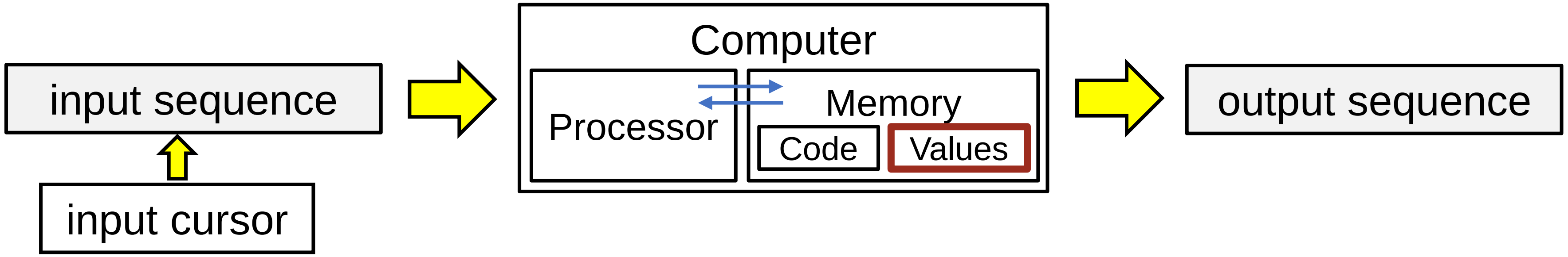
An Input/Output specification ("I/O spec") reads and writes external data

```
/* Input integer n, and output n squared. */
```



Alternatively, an I/O spec sets values of some variables from values of other variables, leaving the external data unchanged.

```
/* Given integer variable n, let variable s be n squared. */
```



Alternatively, an I/O spec sets values of some variables from values of other variables, leaving the external data unchanged.

```
/* Given integer variable n, let variable s be n squared. */
```

	Before			After	
n	4	input variable	n	4	
s	9		s	16	output variable

In general, an I/O spec requires changing a before state into an after state.

```
/* Given before state, establish after state. */
```

In general, an I/O spec requires changing a before state into an after state.

```
/* Given precondition, establish postcondition. */
```

Before

described by precondition

After

described by postcondition

Use pronouns to distinguish the before and after values of a variable that is both input and output

```
/* Swap x and y. */
```

Before			After		
x	4	input variable	x	9	output variable
y	9	input variable	y	4	output variable

Use pronouns to distinguish the before and after values of a variable that is both input and output

```
/* Given x=X and y=Y, establish x=Y and y=X. */
```

Before			After		
x	4	input variable	x	9	output variable
y	9	input variable	y	4	output variable

A specification says what must happen when the precondition holds

```
/* Given x≥0, let y be the square root of x. */
```

Before			After		
x	4	input variable	x	4	
y	9		y	2	output variable

But says nothing about what may happen otherwise.

```
/* Given x≥0, let y be the square root of x. */
```

Before			After		
x	-4	input variable	x	-4	
y	9		y	9	output variable

But says nothing about what may happen otherwise.

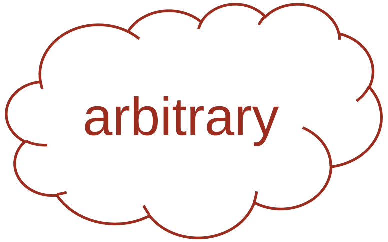
```
/* Given x≥0, let y be the square root of x. */
```

Before

x | -4 | input variable

y | 9

After



Reaching a specification whose precondition doesn't hold is indicative of an error, e.g., we expect x to be nonnegative, so it was incorrectly computed.

```
/* Given x≥0, let y be the square root of x. */
```

Before

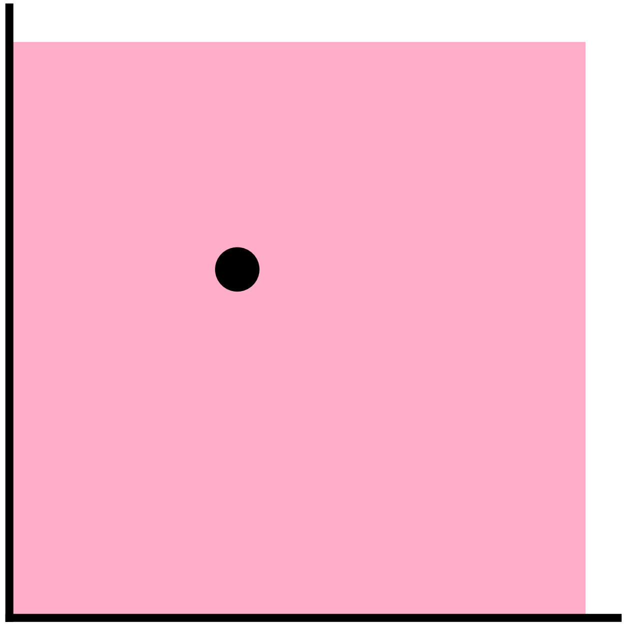
x: -4 (input variable)

y: 9

After

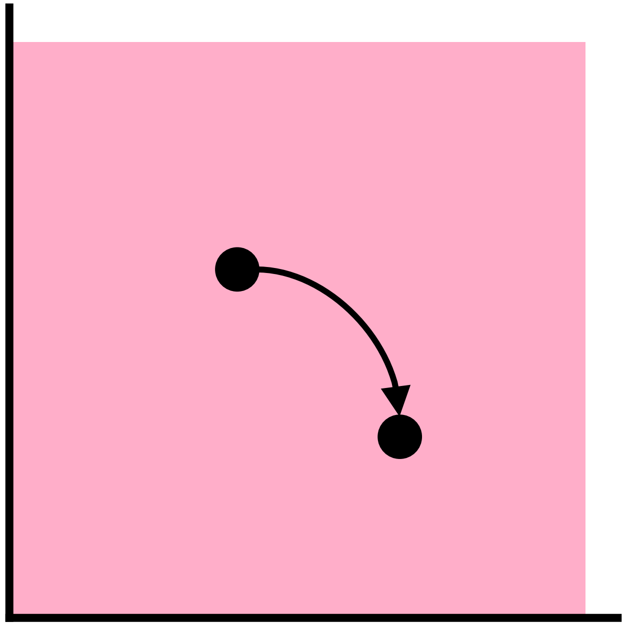
arbitrary

Interrupt a program's execution. Before powering the computer down, save all that you will need to resume later. This is the state.



state and state space

The effect of executing code is to transition from one state to another.

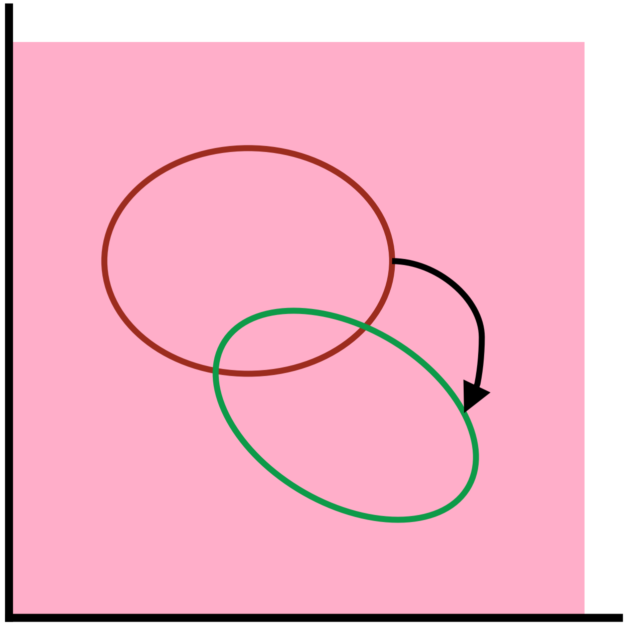


state transition

Statement Specifications

Conditions and Sets of States

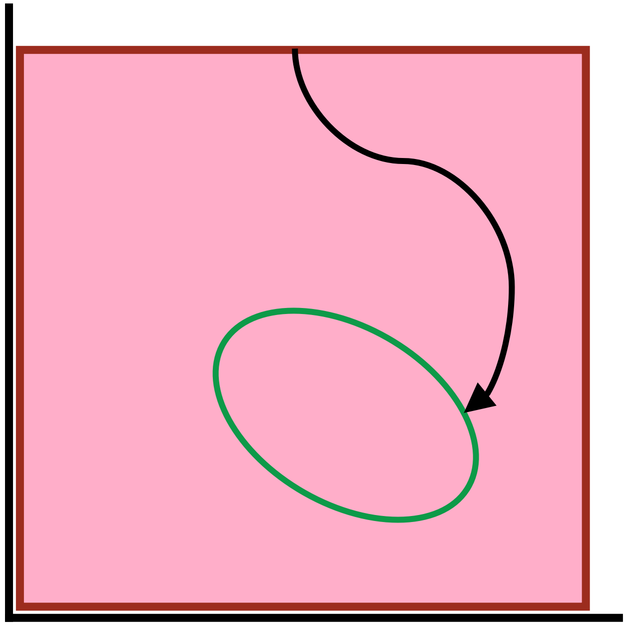
```
/* Given precondition, establish postcondition . */
```



precondition to postcondition

The specification requires transition from any state satisfying the precondition to some state satisfying the postcondition.

```
/* Output “Hello World”. */
```



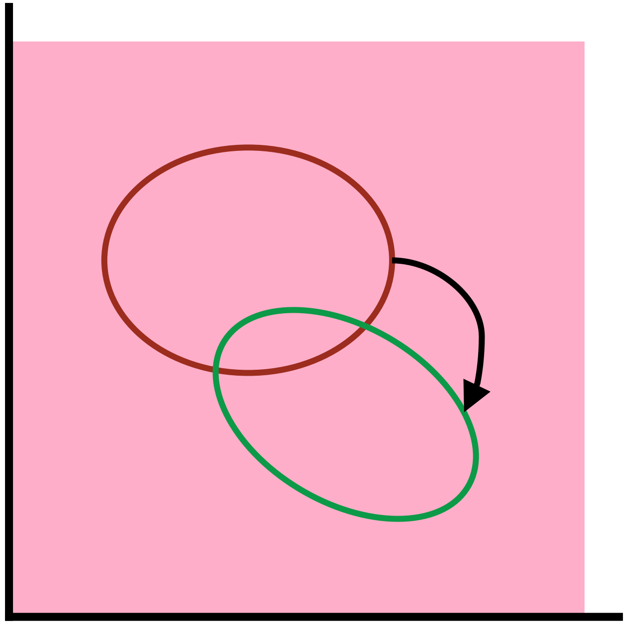
precondition to postcondition

The specification requires transition from any state whatsoever to a state where the output ends with “Hello World”.

Statement Specifications

Conditions and Sets of States

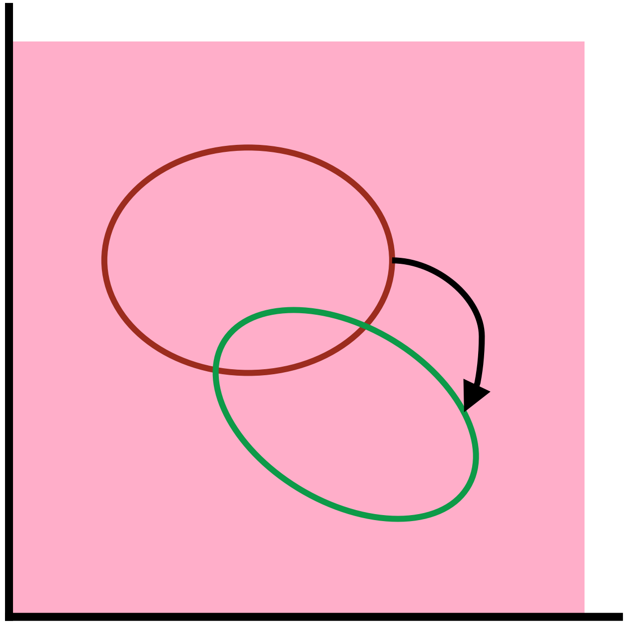
```
/* Swap x and y. */
```



precondition to postcondition

The specification requires transition from any state containing variables x and y to a state where the contents of x and y have been exchanged.

Define sets of states either in English, or using Boolean expressions.



precondition to postcondition

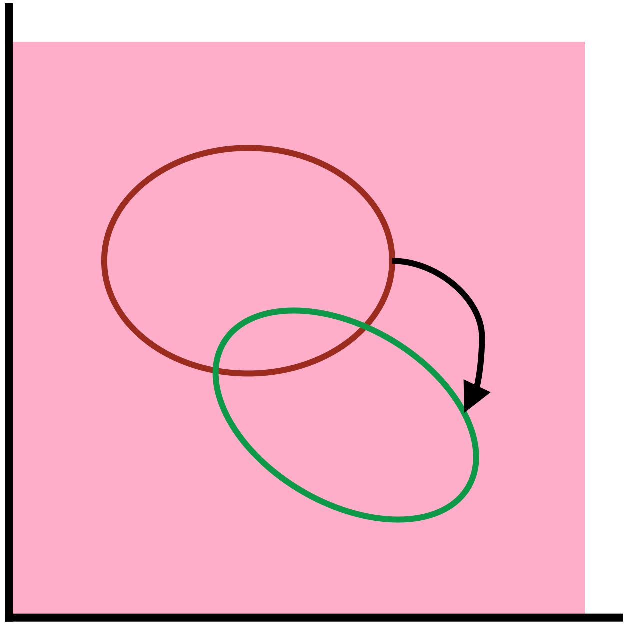
In code, Boolean expressions control execution flow:

```
/* Set y to the square root of x if x is
   not negative, and 0 otherwise. */
   if ( x>=0 ) y = Math.sqrt(x); else y = 0;
```

Statement Specifications

Conditions and Sets of States

Define sets of states either in English, or using Boolean expressions.



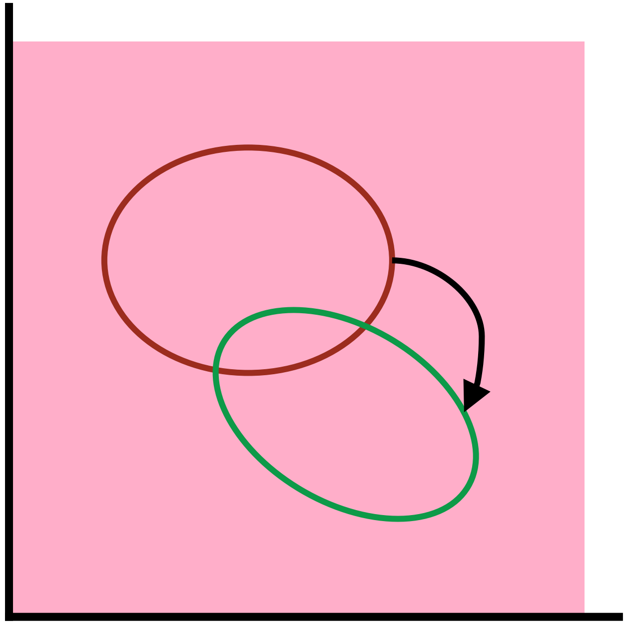
precondition to postcondition

In specifications, Boolean expressions define state sets:

```
/* Given x≥0, let y be the square root of x. */
```

Specifically, the set of all states in which the given Boolean expression is **true**.

Transition to *any* state satisfying the postcondition is allowed.



precondition to postcondition

For example,

```
/* Given x≥0, let y be the square root of x. */
   y = Math.sqrt(x);
```

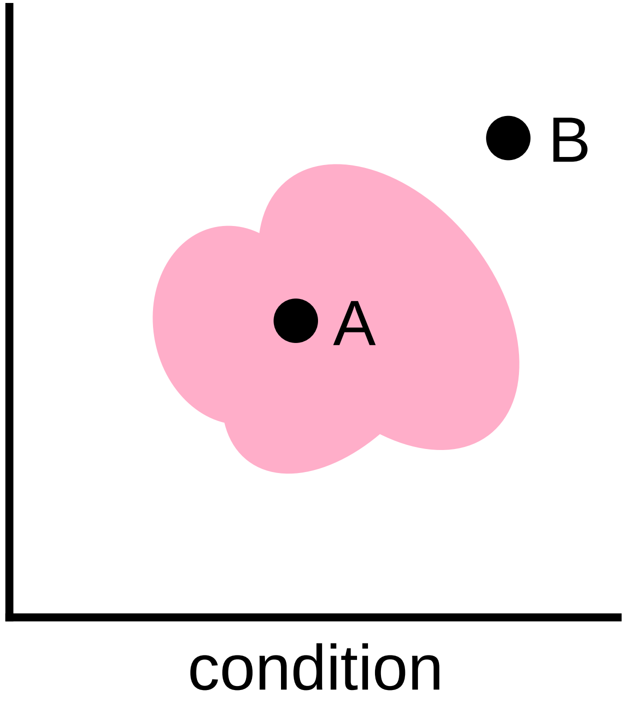
or

```
/* Given x≥0, let y be the square root of x. */
   y = -Math.sqrt(x);
```

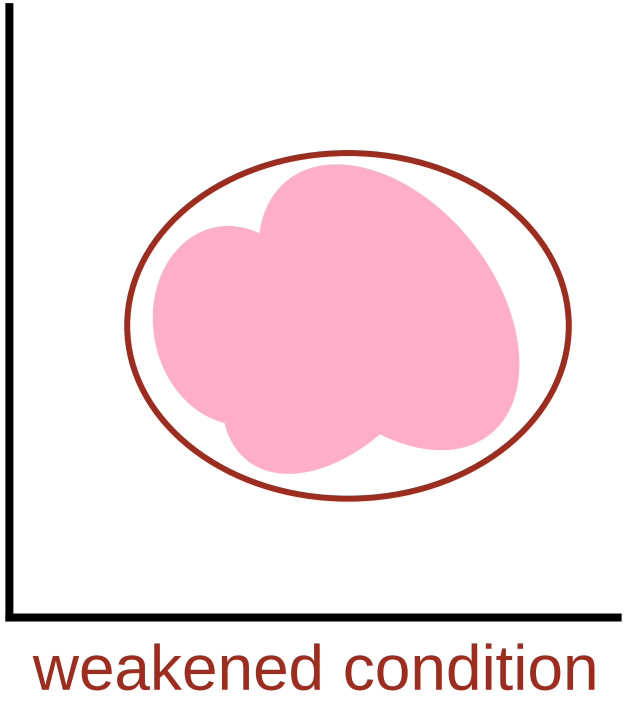
Statement Specifications

Conditions and Sets of States

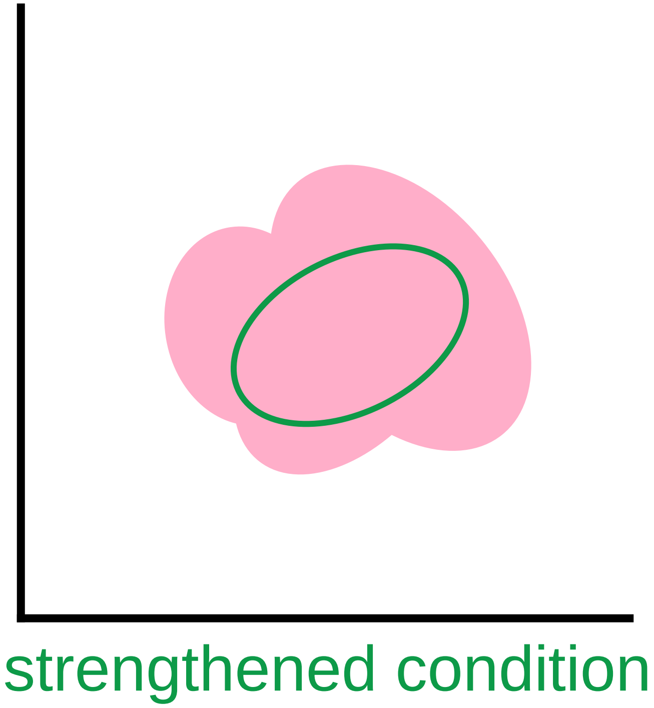
A state either satisfies a condition, or it doesn't.



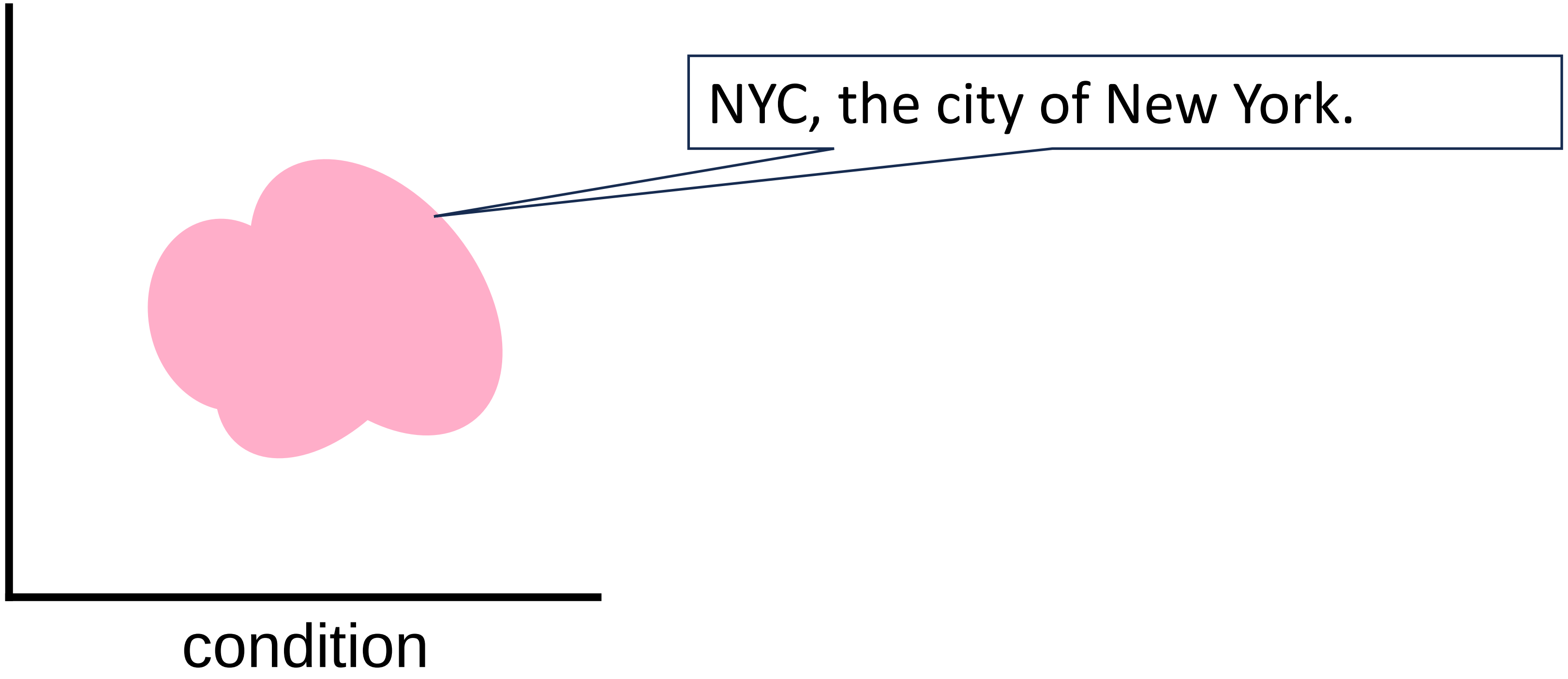
A weakened condition satisfies more states than the original condition.



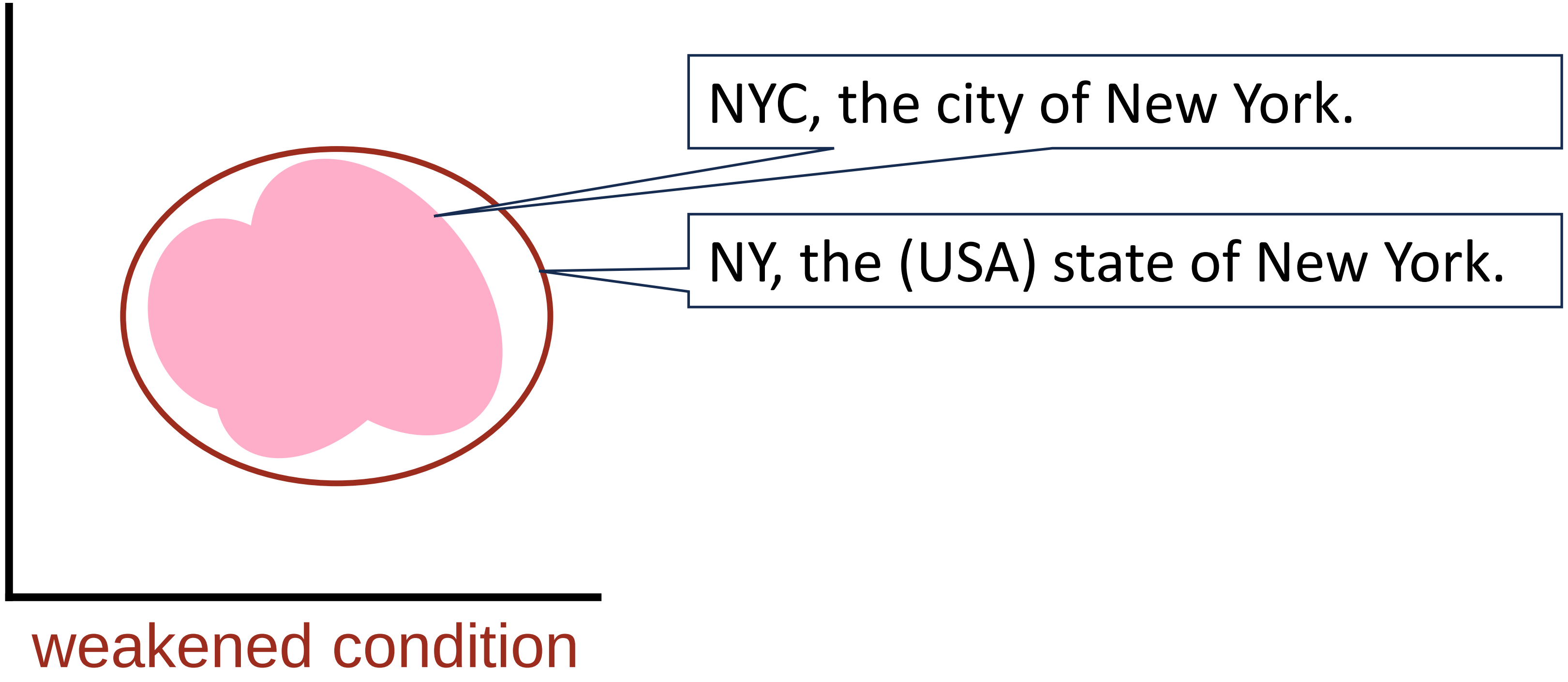
A strengthened condition satisfies fewer states than the original condition.



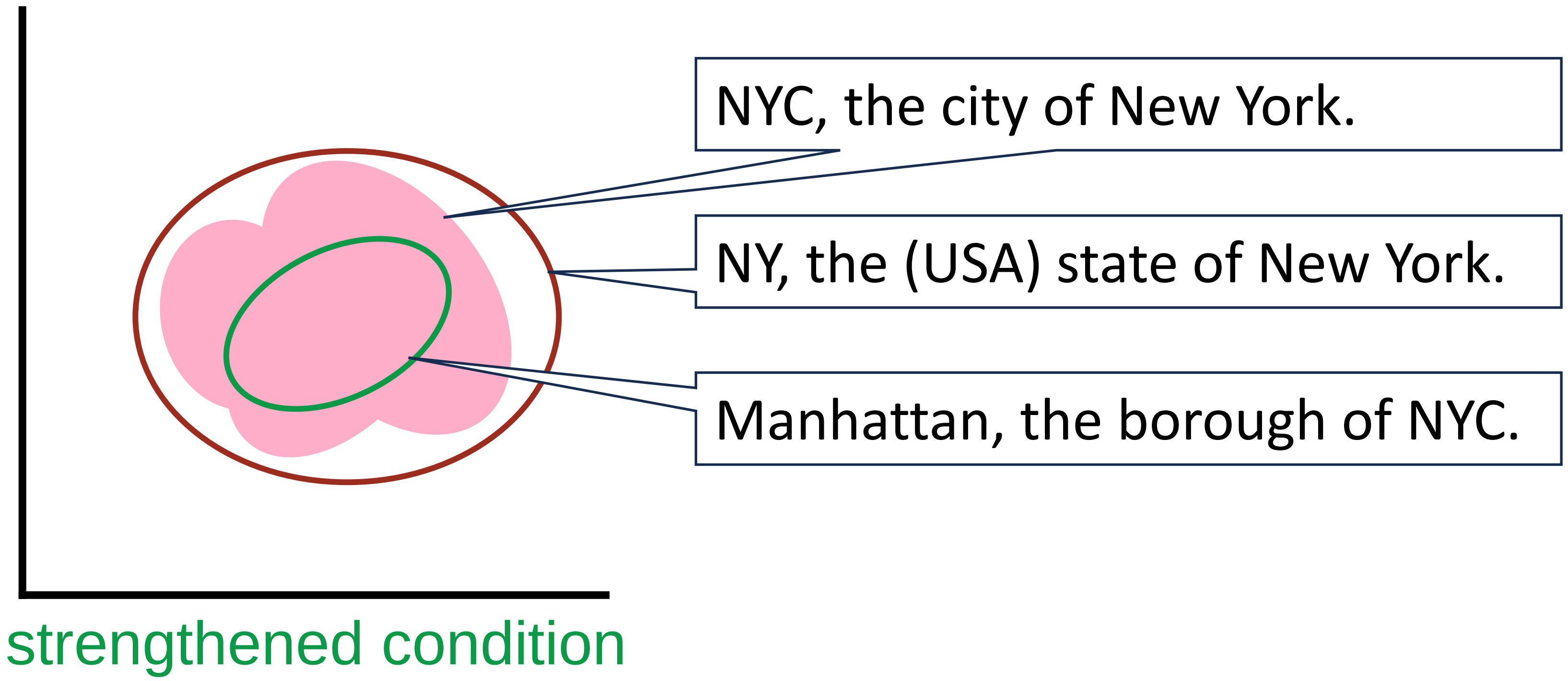
A geographical example:



A geographical example:



A geographical example:



Methods can protect themselves from misuse by their clients by explicitly checking the validity of their arguments, and aborting execution if any are invalid.

Such a protection may derive from a built-in check, e.g., integer division by 0 aborts execution:

```
/* Given n!=0, return x/n. */
static int nth(int x, int n) { return x/n; }
```

Consider this computation. If n turns out to be 0 by mistake, `nth` will abort execution:

```
/* Compute n!=0 such that blah blah. */
   ...
```

```
/* Given n!=0, let y be the nth part of x. */
   y = nth(x, n);
```

```
/* Whatever. */
   ...
```

Aborting execution early is far better than having `Whatever` crash (possibly) much later due to a crazy value of n.

This similar code is just as vulnerable to the error in the computation of n, but without the protection of `nth`, will likely crash in `Whatever`.

```
/* Compute n!=0 such that blah blah. */
   ...
```

```
/* Given n!=0, do Whatever. */
   ...
```

It can protect itself by doing the same check as `nth` using an **assert**:

```
/* Compute n!=0 such that blah blah. */
   ...
/* Given n!=0, do Whatever. */
   assert n!=0: "blah blah computed a zero n";
   ...
```

⚠ Abort execution early if the precondition of `Whatever` doesn’t hold

It can protect itself by doing the same check as `nth` using an **assert**:

```
/* Compute n!=0 such that blah blah. */
   ...
   assert n!=0: "blah blah computed a zero n";
```

```
/* Given n!=0, do Whatever. */
   ...
```

⚠ or if the postcondition of blah blah doesn’t hold.

It can protect itself by doing the same check as `nth` using an **assert**:

```
/* Compute n!=0 such that blah blah. */
   ...
   assert n!=0: "blah blah computed a zero n";
```

```
/* Given n!=0, do Whatever. */
   ...
```

Use of **assert** is preferable to debugging.

Declaration Specifications take a data-centric perspective.

```
Declaration-of-one-variable // Specification
```

or

```
/* Specification. */
   Declarations-of-related-variables
```

A declaration specification provides a representation invariant for the variable(s) that characterizes the value(s) contained therein, and is a global precondition for every statement (except for brief moments before the variable(s) have been updated).

It is akin to a glossary entry, and can be used as such.

Example: Suppose input values are to be read and "processed".

```
int count;  // # of input values read so far.
```

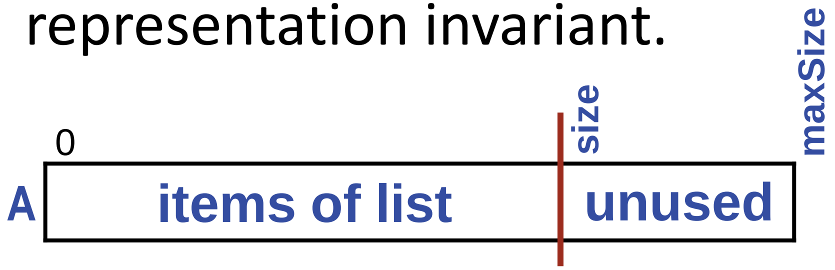
vs

```
int count;  // # of input values processed so far.
```

The two specifications provide different representation invariants for the variable `count`.

In the first case, `count` should be incremented immediately upon reading a value. In the second case, `count` is only incremented when the program gets around to processing the value it has already read.

Example: A group of related variables, called a *data structure*, may share a representation invariant.




```
/* A[0..size-1] are the current items in A[0..maxSize-1], 0≤size≤maxSize. */
    int A[];     // receptacle for items in a list.
    int size;    // current # of elements in list, 0≤size≤maxSize.
    int maxSize; // maximum # of elements storable in the list.
```

An item is inserted into the list (if there is room) at `A[size]`, and then `size` is incremented. The representation invariant characterizes how `A`, `size`, and `maxSize` relate to one another.

A method specification describes the effects (if any) and the return value (if any) of the method in terms of its parameters. This is its postcondition.

```
/* Specification. */
Method definition
```

A method specification describes the effects (if any) and the return value (if any) of the method in terms of its parameters. This is its postcondition.

```
/* Specification. */
Method definition
```

Examples

```
/* Rearrange array A[0..n-1] to be in non-decreasing order. */
void sort( int A[], int n) { ⟨body of sort⟩ }

/* Return the larger of the values x and y. */
int max(int x, int y) { if ( x<y ) return y; else return x; }
```

A method specification may restrict its parameters. This is its precondition.

```
/* Specification. */
Method definition
```

Example

```
/* Given int array A[0..n-1] sorted in non-decreasing order, and int v,
   return an index where A[k]==v, or return n if v does not occur in A. */
int find( int A[], int n, int v) { ⟨body of find⟩ }
```

A method specification may restrict its parameters. This is its precondition.

```
/* Specification. */
Method definition
```

Example

```
/* Given int array A[0..n-1] sorted in non-decreasing order, and int v,
   return an index where A[k]==v, or return n if v does not occur in A. */
int find( int A[], int n, int v) { ⟨body of find⟩ }
```

A class specification summarizes the class's purpose and functionality. The specifications of the class's public declarations and methods are implicitly part of the class specification.

```
/* Specification. */
Class definition
```

Class specifications are often more descriptive and historical than the other forms of specification.

```
/* Rational. A module for the manipulation of rationals, including operations
   for +, -, *, /, conversion to String, and equality.
   Author: Joe Blow.
   Created: 12/25/2022.
   Revision History: Converted to use unbounded integers, 12/25/2023. */
class Rational {
   ...
   } /* Rational */
```