

Example 2: Trading In Conjectures for Hypotheses

This example illustrates "good" and "bad" ways to leave a loop. Mango can find these exit points by traversing the [local forward flow](#). Only the "good" ways will ultimately be specified. One of the bad ways can be eliminated by assuming x is defined, avoiding the `NullPointerException`. This can be done automatically with no extra effort. The `ArrayIndexOutOfBoundsException` is more subtle. It requires a certain amount of insight to make the assumption that the array length of x is greater than or equal to 10. For now, it will be up to the user to add such "insightful" hypotheses, but eventually routine assumptions like this one should also be automated. With these assumptions, an automated theorem prover can then prove the conjecture that i^{\wedge} is greater than or equal to 10. The specification for the good case may now soundly replace the conjecture:

i^{\wedge} is greater than or equal to 10

with the much more helpful hypotheses:

x is defined and the length of x is greater than or equal to 10.

Observe that the specification for the good case is not very informative. It just says that the heap is altered by a loop, and the stack frame for the `loop()` method has been popped. This is intentional. We don't know yet what facts about the loop are pertinent, so there is little to say at this point. It is up to dependent modules to introduce such information. In particular, the [specification for `main\(\)`](#) generates interesting conjectures about this loop.

Source code

```
27 package baseline;
28
29 public class ItsAWrap {
30
31     public static boolean main (int[] x) {
32         clear(x);
33         if(x[5]==x[6]){
34             return true;
35         }
36         return false;
37     }
38
39     static void clear(int[] x){
40         for(int i=0;i<10;++i){
41             x[i]=0;
42         }
43     }
44 }
45
```

Specification

Specifying loop at 40: for(int i=0;i<10;++i){

40: for(int i=0;i<10;++i){ [1]

Hypothesis: op0 is less than 10

Hypothesis: x is defined

Hypothesis: i is less than length of the array x

Hypothesis: i is greater than or equal to 0

x[i] = 0

i = i + 1

op0 = i + 1

Specifying method: void baseline.ItsAWrap.clear(int[])

40: for(int i=0;i<10;++i){ [1]

41: x[i]=0; [1.1]

-1: #6: ArrayIndexOutOfBoundsException [1.1.1]

Hypothesis: x is defined

Conjecture: i^ is greater than or equal to length of the array x OR i^ is less than 0

output heap of #12_iloop_i<loop1>

Throws: java.lang.ArrayIndexOutOfBoundsException.

-1: #6: NullPointerException [1.1.2]

Hypothesis: x is undefined

output heap of #12_iloop_i<loop1>

Throws: java.lang.NullPointerException.

43: } [1.2]

Conjecture: i^ is greater than or equal to 10

output heap of #12_iloop_i<loop1>

stack

No return value.

Flow Control

