Whiley Comparison

Vivian Stewart

January 20, 2016

Abstract

1 Introduction

2 Benchmarks

2.1 palindrome

Scans through an array from the outer elements in towards the centre searching for a mismatch in characters in which case returning false if there is such a mismatch and returning true if there is no such mismatch.

```
// Status wyc-37:  verified [96203ms]  (-54.73// wyc-36:  verified [43551ms]
function isPalindrome(int[] chars) -> (bool r)
  ensures r <==> all { x in 0..|chars| | chars[x] == chars[|chars| - (x + 1)] }
:
  int i = 0
  int j = |chars|

  while i < j
    where i + j == |chars| && i >= 0
    where all { k in 0..i | chars[k] == chars[|chars| - (k+1)] }
  :
    j = j - 1
    if chars[i] != chars[j]
    :
      return false
    i = i + 1

  return true
```

2.2 firstIndexOf

Finds the first index where the specified element is found in the given array of integers, searching through the array from the zero index in the positive direction.

```
// Status wyc-37:  verifies
//  wyc-36:  verifies
function firstIndexOf(int[] items, int item) -> (int r)
  // If result is positive, element at that position must match item
```

```
  ensures r >= 0 ==> items[r] == item
  // If result is positive, no element at lesser position matches item
  ensures r >= 0 ==> all { k in 0..r | items[k] != item }
  // If result is negative, no element matches item
  ensures r <  0 ==> no  { k in 0..|items| | items[k] == item }
:
  int i = 0
  while i < |items|
    // i is increasing and no element at greater position matches item
    where 0 <= i && i <= |items|
    where no { k in 0..i | items[k] == item }
  :
    if items[i] == item
    :
      return i
    i = i + 1
  // didn't find item in entire list
  return -1
```

2.3 lastIndexOf

Finds the last index where the specified element is found in the given array of integers, searching through the array from the the highest index in the negative direction.

```
// Status wyc-37:  verifies [1048ms]  (-27.77// wyc-36:  verifies [1429ms]

function lastIndexOf(int[] items, int item) -> (int r)
// If result is positive, element at that position must match item
ensures r >= 0 ==> items[r] == item
// If result is positive, no element at greater position matches item
ensures r >= 0 ==> all { x in (r + 1)..|items| | items[x] != item }
// If result is negative, no element matches item
ensures r < 0 ==> no { x in 0..|items| | items[x] == item }
:
  int i = |items|
  while i >= 0
  // i is decreasing and no element at greater position matches item
  where 0 <= i && i <= |items|
  where no { x in i..|items| | items[x] == item }
  :
    i = i - 1
    if items[i] == item
    :
      return i
  // didn't find item in entire list
  return -1
```

2.4 max

Searches the entire list in order to find and return the largest integer found.

```
// Status wyc-37:  verifies.
//  wyc-36:  verifies.
public function maxArray(int[] items) -> (int max)
  requires |items| > 0
  ensures all { k in 0..|items| | max >= items[k] }
:
```

```
  int i = 1
  int r = items[0]

  while i < |items|
    where 0 < i && i <= |items|
    where all { k in 0..i | r >= items[k] }
  :
    if items[i] > r:
      r = items[i]
    i = i + 1

  return r
```

2.5 occurences

Returns the number of duplicate elements that hold a given value in the given array.

```
// Status wyc-37:  loop invariant not restored where count == 0 ==> ...
//  wyc-36:  "
function occurences(int[] items, int item) -> (int r)
  // some number of occurences of item
  ensures r > 0  ==> some { k in 0..|items| | items[k] == item }
  // no occurences of item
  ensures r == 0 ==> all  { k in 0..|items| | items[k] != item }
:
  int i = 0
  int count = 0

  while i < |items|
    // i is increasing and there could be elements that match
    where 0 <= i && i <= |items|
    where count > 0  ==> some { k in 0..i | items[k] == item }
    where count == 0 ==> all  { k in 0..i | items[k] != item }
  :
    if items[i] == item
    :
      count = count + 1
    i = i + 1

  return count
```

2.6 strlen

Counts the number of characters in a string of characters, having come to the end of the list when encountering a null character.

```
// Status:  wyc-37:  verified and compiled [1197ms]  (-7.76)
//  wyc-36:  verified and compiled [1104ms]
constant NULL is 0

// ASCII character is unsigned 8bit integer
type ASCII_char is (int n) where n >= 0 && n < 256

// C String is array of chars where at least one is NULL
type C_string is (ASCII_char[] chars)
     where some { i in 0..|chars| | chars[i] == NULL }

```

```
// Calculate length of string
function strlen(C_string str) -> (int r)
  ensures r >= 0
:
  int i = 0
  //
  while str[i] != NULL
    where i >= 0
    where all { k in 0..i | str[k] != NULL }
  :
    i = i + 1
  return i
```

2.7 linearSearch

Return the index in the given array where the first occurrence of an element matching the given value would be inserted. Previously the find function was to find an insertion point into the sorted part of array where the value would be inserted into the part of the array and would still be sorted.

```
// Status wyc-37:  verifies [49640ms]
//  wyc-36:  verifies [76839ms]
type nat is (int n) where n >= 0

function linearSearch(int[] arr, int val, nat len) -> (nat r)
  requires len < |arr|
  // arr is an ordered array
  requires all { k in 0..len - 1 | j < k ==> arr[j] <= arr[k] }
  // return value should not exceed len
  ensures r <= len
  // index of place of insertion is returned
  ensures all { k in 0..r | arr[k] <  val }
  ensures all { k in r..len | arr[k] >=  val }
:
  nat i = 0

  while i < len
    where i <= len
    where all { k in 0..i | arr[k] < val }
    where i < (len - 1) ==> arr[i] <= arr[i + 1]
  :
    if arr[i] >= val
    :
      return i
    i = i + 1

  return i
```

2.8 binarySearch

Using the divide and conquer method to find the index of an element in the given array matching the given value.

```
// Status:  verifies and compiles?...no
//  ( if items[mid] < key:, index out of bounds (negative) )
type nat is (int n) where n >= 0
```

```
4
5  method binarySearch( int[] items, int key ) -> (int r)
6    requires |items| > 0
7    requires all { j in 0..|items|, k in 0..|items|
8                 | j < k ==> items[j] <= items[k] }
9    ensures r >= 0 ==> r < |items| && items[r] == key
10   ensures r < 0  ==> all { k in 0..|items| | items[k] != key }
11 :
12   nat low = 0
13   nat high = |items|
14   nat mid = 0
15
16   while low < high
17     where low <= mid
18     where mid < high
19     where high <= |items|
20     // elements outside the search range do not equal key
21     where no { i in 0..low, j in high..|items|
22               | items[i] != key && items[j] == key }
23   :
24     mid = (low + high) / 2
25
26     if items[mid] < key
27     :
28       low = mid + 1
29     else if key < items[mid]
30     :
31       high = mid
32     else
33     :
34       return mid
35
36   return -1
```

2.9 append

Adds a single element to the end of the array by making a new array that is one element larger than the original and copies the original array in order to the lower elements and inserting the given value in the last index.

```
1  // Status wyc-37:  verifies [1745ms].   228.48// wyc-36:  verifies [3987ms].
2  public function append(int[] items, int item) -> (int[] rs)
3    ensures |rs| == |items| + 1
4  :
5    int[] result = [ 0; |items| + 1 ]
6    int i = 0
7
8    while i < |items|
9      where all { k in 0..i | result[k] == items[k] }
10     where i >= 0
11     where |result| == |items| + 1
12     where i < |result|
13   :
14       result[i] = items[i]
15       i = i + 1
16
17   result[i] = item
18   return result
```

2.10 remove

The remove function should remove the item at the given index from the given array of integers and return the resulting array otherwise unchanged. The resulting array is of course one element shorter in length. This is done by creating a new array one smaller in size and then copying across the elements before the given index directly, followed by copying across elements above the index to a position one index lower and overwriting the removed element.

```
// Status wyc-37:  infinite loop
//  wyc-36:  verifier "GC overhead limit exceeded"

function remove(int[] items, int index) -> (int[] r)
  requires 0 <= index && index < |items|
  requires |items| > 0
  ensures |r| == |items| - 1
  ensures all { k in 0..index   | r[k] == items[k] }
  ensures all { k in index..|r| | r[k] == items[k + 1] }
:
  int newlen = |items| - 1
  int i = 0
  int[] result = [ 0; newlen ]

  while i < index
    // items before index in result are still the same
    where 0 <= i where i <= index
    where |result| == newlen
    where all { k in 0..i | k < index ==> result[k] == items[k] }
  :
    result[i] = items[i]
    i = i + 1

  assert i == index

  while i < newlen
    // items after index in result are transposed by one place
    where index <= i where i <= newlen
    where |result| == newlen
    where all { k in 0..index | result[k] == items[k] }
    where all { k in index..i | result[k] == items[k + 1] }
  :
    result[i] = items[i + 1]
    i = i + 1

  return result
```

2.11 copy

...

```
// Status wyc-37:  null pointer exception.
//  wyc-36:  loop invariant not restored
//  where all  k in 0..dStart | dest[k] == odest[k]
import whiley.lang.System

method main(System.Console console):
    int[] src = [1,2,3,4,5]
    int[] res = copy( src, 2, [3,4,5,6,7], 1, 3 )
    console.out.println(res)

```

```
function copy(int[] src, int sStart, int[] dest, int dStart, int len) -> (int[] r)
  // starting points in both arrays cannot be negative
  requires sStart >= 0 && dStart >= 0 && len > 0
  // Source array must contain enough elements to be copied
  requires |src| >= sStart + len
  // Destination array must have enough space for copied elements
  requires |dest| >= dStart + len
  // Result is same size as dest
  ensures |r| == |dest|
  // All elements before copied region are same
  ensures all { k in 0..dStart | r[k] == dest[k] }
  // All elements in copied region match src
  ensures all { k in 0..len | r[dStart + k] == src[sStart + k] }
  // All elements above copied region are same
  ensures all { k in dStart + len..|dest| | r[k] == dest[k] }
:
  int i = 0
  int[] odest = dest
  assert all { k in 0..|dest| | dest[k] == odest[k] }

  while i < len
    where 0 <= i where i <= len
    where |dest| == |odest| // all items are still the same before dStart index
    where all { k in 0..dStart | dest[k] == odest[k] }
    // all items after dStart index are still the same
    where all { k in (dStart + len)..|dest| | dest[k] == odest[k] }
    // inbetween items are copied from src
    where all { k in sStart..sStart + i, j in dStart..dStart + i
                   | src[k] == dest[j] }
  :
    dest[dStart + i] = src[sStart + i]
    i = i + 1

  return dest
```

2.12 displace

rotates a region of the array by one place forward

```
// Status wyc-37:  null pointer exception
//  wyc-36:  line 37:  loop invariant not restored
type nat is (int n) where n >= 0

function displace( int[] arr, nat start, nat len) -> (int[] r)
  requires len > 0
  requires start + len <= |arr|
  ensures |r| == |arr|
  ensures all { k in             0..start       | r[k] == arr[k] }
  ensures all { k in (start + len)..|arr|       | r[k] == arr[k] }
  ensures all { k in   (start + 1)..start + len | r[k] == arr[k - 1] }
  ensures r[start] == arr[start + len - 1]
:
  nat i = 0
  int[] res = [0 ; |arr|]

  while i < start
    where i <= start
    where |res| == |arr|
    where all { k in  0..i | res[k] == arr[k] }
  :
```

```
    res[i] = arr[i]
    i = i + 1

  assert all { k in 0..start | res[k] == arr[k] }

  res[start] = arr[start + len - 1]

  assert res[start] == arr[start + len - 1]

  i = start + 1
  while i < start + len
    where |res| == |arr|
    where start < i && i <= (start + len)
    where res[start] == arr[start + len - 1]
    where all { k in           0..start | res[k] == arr[k] }
    where all { k in (start + 1)..i     | res[k] == arr[k - 1] }
  :
    res[i] = arr[i - 1]
    i = i + 1

  assert all { k in (start + 1)..start + len | res[k] == arr[k - 1] }

  i = start + len
  while i < |arr|
    where |res| == |arr|
    where (start + len) <= i && i <= |arr|
    where res[start] == arr[start + len - 1]
    where all { k in             0..start       | res[k] == arr[k] }
    where all { k in   (start + 1)..start + len | res[k] == arr[k - 1] }
    where all { k in (start + len)..i           | res[k] == arr[k] }
  :
    res[i] = arr[i]
    i = i + 1

  return res
```

2.13 insert

This function should insert the item at the given index from the items array. The resulting array is of course one element longer in length.

```
// Status wyc-37:  null pointer exception.
//  wyc-36:  loop invariant does not hold on entry
//  where all  k in 0..index | result[k] == items[k]
type nat is (int n) where n >= 0

function insert(int[] items, int item, nat index) -> (int[] r)
  requires index < |items|
  requires |items| > 0
  ensures |r| == |items| + 1
  ensures all { k in 0..index | r[k] == items[k] }
  ensures r[index] == item
  ensures all { k in index..|r| | r[k] == items[k - 1] }
:
  // length of the new array
  nat newlen = |items| + 1
  int[] result = [ 0; newlen ]
  nat i = 0

```

```
  while i < index
    // items before index in result are still the same
    where i <= index
    where |result| == newlen
    where all { k in 0..i | result[k] == items[k] }
  :
    result[i] = items[i]
    i = i + 1

  result[i] = item
  i = i + 1
  assert i == index + 1
  assume all { k in 0..index | result[k] == items[k] }

  while i < newlen
    // items after index in result are transposed by one place
    where index < i where i <= newlen
    where |result| == newlen
    where all { k in 0..index | result[k] == items[k] }
    where result[index] == item
    where all { k in (index + 1)..i | result[k] == items[k - 1] }
  :
    result[i] = items[i - 1]
    i = i + 1

  return result
```

2.14 insertionSort

...

3 Results & Discussion

Env.	Palin.	FIO	LIO	Max	Occ	Slen	LSrch
Whiley	✓	✓	✓	✓	✘	✓	✓
Dafny	✓	✓	✓	✓	✓	✓	✓

Env.	BSrch	Appd	Remv	Copy	Dplc	Inst	InSrt
Whiley	✘	✓	✘	✘	✘	✘	✘
Dafny	✓	✓	✓	✓	✓	✓	✓

Whiley allows you to do more with less, minimal syntax but more expressive. (IMPORTANT!! flexible language constructs)... Dafny has more complicated syntax to deal with memory management i.e pointers/references, lots to remember and coordinate. The tools Dafny provides are for the development of proofs in a "top-down" manner, and which allow us to concentrate on the "architecture" of the proof. Unlike Frama-C. Deduction of bounds of different variables seems to not work in Whiley (not array bounds.) TODO: insert(), merge(), binarySearch(), qsort() The semantics of logic expressions in ACSL (Frama-C), Whiley and Dafny are based on mathematical first-order logic. With Frama-C in particular, it is a 2-valued logic with only total functions. Consequently, expressions are never "undefined". Having only total functions implies that one can write terms such as 1/0, or *p when p is null. Specifications in Frama-C can have implicit casts between C-types and Mathematical types (something to watch out for.) Weird:

- 5/3 is 1 and 5 % 3 is 2;

- (-5)/3 is -1 and (-5) % 3 is -2;
- 5/(-3) is -1 and 5 % (-3) is 2;
- (-5)/(-3) is 1 and (-5) % (-3) is -2.

Frama-C Degree of Completeness The previous section has taught us that writing a fairly complete specification (in fact we could still add some clauses to the specification above, as we will see in the next chapters) is not immediate, and thus that it is easy to come up with only a partial specification. Hence, it raises two frequently asked questions: how can we be sure that our specification is complete, and how complete must a specification be. The answers however do not lie in ACSL itself. For the first one, one must reason on some model of the specified application. For the second one, there is no definite answer. It depends on the context in which the specification is written and the kind of properties that must be established: the amount of specification required for a given function is very different when verifying a given property for a given application in which calls to the function always occur in a well-defined context and when specifying it as a library function which should be callable in as many contexts as possible.

Frama-C When no 'assigns' clauses are specified, the function is allowed to modify every visible variable.

Termintes It is possible to relax a particular function's specification by providing a formula that describes the conditions in which the function is guaranteed to terminate.

Assertions when the analyzer is not able to determine that an assertion always holds, it may be able to produce a pre-condition for the function that would, if it was added to the function's contract, ensure that the assertion was verified.

Overflow overflow is/must be handled.

```
inductive reachable{L} (list* root, list* node) {
  case root_reachable{L}:
    \forall list* root; reachable(root,root);
  case next_reachable{L}: // L indicates a Label -> memory state
    \forall list* root, *node;
      \valid(root) ==> reachable(root -> next, node) ==>
        reachable(root,node);
```

```
requires \valid(p) && \valid(q);
ensures *p <= *q; // pointers
behavior p_minimum:
    assumes *p < *q;
    ensures *p == \old(*p) && *q == \old(*q);
behavior q_minimum:
    assumes *p >= *q;
    ensures *p == \old(*q) && *q == \old(*p);
complete behaviors p_minimum, q_minimum;
disjoint behaviors p_minimum, q_minimum;
```

No verifier can tell you whether your code doesn't work the according to the specification or the specification doesn't describe what the code does, as this depends on the intention of the user/developer. Frama-C ACSL specification language lacks flexible language constructs, very cumbersome/specialised syntax.

All languages need different forms of verification and to different degrees. Sensitivity to approach to the problem.

3.1 Whiley

Whiley is very easy to use and shows promise as a tool to verify programs in such a way that the accompanying specification scales with complexity of the program to be verified. Whiley offers a simplified program and specification definition. However, Whiley's underlying prover needs some work to bring Whiley up to the level attained by other tools. Arrays in Whiley are not reference or pointer types, there is no possibility of the array being null, also copying of an array is just a matter of assigning that array to a different variable, bypassing the issue of specifying array copying loops. Some basic arithmetic and region ranges seem to be difficult for the whiley constraint solver (WyCS.)

3.2 Dafny

Dafny is a sophisticated tool/language for verification based on Microsofts' Z3 prover and Boogie with Monodevelop/Visual Studio. Though tests were performed on the command line to gain feedback from Dafny. Dafny can use pure functional code to help prove the correctness of imperative code for instance, only functions can used in specification unless qualified as 'function method'. These pure function definitions require very minimal specification in order to provide lemmas, axioms and other mathematical constructs to prove correct execution. One thing that struck me as odd was the use of short circuit logic in the specifications which implies a certain order to the specifications statements. Dafny doesn't require return statements in the usual way and defines a return variable(s) that is assigned to, and if necessary a 'return' can be called for early return from the call. Explicit and obvious reference to the returned variable was very convenient. All function/method parameters are immutable unless specified otherwise. Inside the specifications arrays are treated differently from other containers but are implicitly convertible to the built in sequence type if needed. Which allows for the very convenient syntax: arr1[m..n] == arr2[m..n] for an adjacent element comparison avoiding the need for long winded predicates. But not so convenient in that a sequence cannot be easily converted back to an array. Arrays are always possibly null in Dafny and the there are attempts in the specification language to mitigate the issue of reference aliasing and other such memory management quirks (modifies clause.) Unlike Whiley arrays are of reference type and need to be null checked.

3.3 Frama-C

When it comes to verifying C code Frama-C seems to be a current industry favourite. But I found the user gtk interface to be cumbersome and confusing. The ACSL language would appear to appeal more to an expert C programmer which I am not. Much expertise is needed to master Frama-C and every aspect and plugin have large manuals and tutorials available, all very heavy in detail. What I really wanted was a more general tool that would help point out where errors in my reasoning were evident. Frama-C offers only the vaguest of clues and errors in my reasoning are not always obvious. The issues of bounded types are dealt with up front and checked with the WP plugin through an RTE (runtime error) option that injects (over/ under)flow checks. Specifications are meant to be written in a style that complements C and is analogous to C, even mirroring C conventions and C arithmetic. The lack of consolidation makes the various plugins difficult to integrate into a workflow. The ACSL specification language is littered with predefined predicates and detailed set of proof tools such as user defined predicates, behaviours, inductive(recursive) functions and axioms etc. Arrays were a very sticky issue in Frama-C and involve proof of non-null and the validation of the range of indices and elements. For loop invariants, proof of termination is provided by the loop 'variant' key word, which is hard to see in amongst loop 'invariant' clauses in the same comment code block. Also there are

assigns clauses that define the frame of modification for both the function and loop invariants (loop assigns.) since unlike other tools Frama-C has no knowledge of what has been modified in the function or inside the loop (side effects). Since the C language does not have formal semantics one should take the verification of C code with a grain of salt, horribly coded nonsense with undefined results can still be verified.

3.4 Spec#

Spec# having the same underlying workings as Dafny (a.k.a Boogie and Z3) if there are many differences between the two.