Assignment 4
Diamonds in the Rough

15-414: Bug Catching: Automated Program Verification

Due 23:59pm, Tuesday, March 30, 2021
85 pts

This assignment is due on the above date and it must be submitted electronically on Gradescope. Please carefully read the policies on collaboration and credit on the course web pages at `http://www.cs.cmu.edu/~15414/assignments.html`.

What To Hand In

You should hand in the following files on Gradescope:

- Submit the file `asst4.zip` to Assignment 4 (Code). You can generate this file by running `make handin`. This will include your solutions `ubarray.mlw`, `ind.mlw`, and the proof sessions in `ubarray/` and `ind/`
- Submit a PDF containing your answers to the written questions to Assignment 4 (Written). You may use the file `asst4-sol.tex` as a template and submit `asst4-sol.pdf`.

  Make sure your session directories and your PDF solution files are up to date before you create the handin file.

Using LaTeX

We prefer the answer to your written questions to be typeset in LaTeX, but as long as you hand in a readable PDF with your solutions it is not a requirement. We package the assignment source `asst4.tex` and a solution template `asst4-sol.tex` in the handout to get you started on this.

1 Box vs. Diamond (25 pts)

In dynamic logic, we define the semantics of negation

$$\omega \models \neg P \quad \text{iff} \quad \omega \not\models P$$

Under this definition it is easy to check, for example, that $\neg\neg P \leftrightarrow P$ is valid. In the tasks below you may use this and the other usual De Morgan laws for (classical) propositional reasoning with negation. Like the $[\alpha]$ and $\langle\alpha\rangle$, we follow the convention that the unary operators bind more tightly than binary ones, so $[\alpha]\neg P \rightarrow \neg Q$ stands for $([\alpha](\neg P)) \rightarrow (\neg Q)$.

For each of the following two implications, either prove its validity or find a counterexample.

Task 1 (5 pts). $\neg[\alpha]P \rightarrow \langle\alpha\rangle\neg P$

Task 2 (5 pts). $\neg\langle\alpha\rangle P \rightarrow [\alpha]\neg P$

Task 3 (5 pts). What can you conclude about the relationship of $[\alpha]$ and $\langle\alpha\rangle$ in dynamic logic in general?

Task 4 (10 pts). In view of what you discovered in Tasks 1–3, can you justify the axioms regarding the following constructs directly from the axioms for $[-]Q$, without explicitly referencing the semantic definitions?

(i) $\langle\alpha\ ;\ \beta\rangle Q$

(ii) $\langle ?P\rangle Q$

(iii) $\langle\alpha \cup \beta\rangle Q$

2 Unbounded Arrays (40 pts)

In this problem we explore the use of verification to certify resource bounds using amortized analysis. We also revisit data structure invariants, ghosts, and illustrate how to handle data that admit a null value.

An *unbounded array* has constant time set and get operations, just like ordinary arrays, but we can also extend their domain by *adding* elements at the end or shrink their domain by *removing* elements from the end. Moreover, we specify that add and remove should have *constant-time amortized cost*. We fix the cost model by specifying

A write operation to an array requires one unit of work; all other operations are free.

You can find a description of unbounded arrays and their amortized analysis at 11-ubarrays.pdf from *15-122 Principles of Imperative Computation*.

In WhyML we represent an unbounded array with

```
type uba 'a = { mutable size : int ;
                mutable limit : int ;
                mutable data : array (option 'a) ;
                mutable ghost potential : int }
```

The `data` array contains elements `Some x` in its domain but may also have some unused elements. The `size` field represents the current domain of the unbounded array. We can apply `get` and `set` to any index $0 \leq i <$ size. `limit` is the actual length of the underlying `data` array that has been allocated, with elements size $\leq i <$ limit being reserved for expansion of the domain.

The ghost field `potential` represents the available potential (or number of "tokens") in the data structure, which must always remain nonnegative. According to our cost model, each token permits one array write operation. Each operation that entails a write, namely `set`, `add`, and `rem` is given a certain amount of potential. Any potential not immediately used is stored in the ghost field for later use. The stored potential is necessary to copy the array content whenever a new underlying data array is allocated, which happens when the domain becomes too large or too small. Further specifics are given with the operations below.

Implement the operations on unbounded arrays according to the following specs.

(i) `new (size : int) (default : 'a) : uba 'a`
Allocate and return a new unbounded array with initial domain size `size` and limit `2*size` (or `1` when `size` is `0`). The array should be initialized with the given default element. Allocation incurs no cost in our model.

(ii) `len (u : uba 'a) : int`
Return the current size of the domain of u.

(iii) `get (u : uba 'a) (i : int) : 'a`
Get the element at index i of u.

(iv) `set (u : uba 'a) (i : int) (x : 'a) (ghost p : int)`
Set the element at index i of u to be x. This requires 1 token which should be passed as p.

(v) `add (u : uba 'a) (x : 'a) (ghost p : int)`
Add a new element at the end of u, expanding it domain. This requires 3 tokens: 1 to perform the write, and 2 to save. If adding an element fills the array completely, double the length of the array and copy the elements in the domain to the new array.

(vi) `rem (u : uba 'a) (ghost p : int) : 'a`
Remove an element from the end of u, shrinking its domain. This costs 2 tokens: 1 to overwrite the element to be `None` and 1 to save. When the domain is only one fourth of the length of the array or smaller, cut the length of the array in half and copy the elements in the domain to the new array. A precondition should require that `rem` cannot be called on an unbounded array with empty domain.

In order to implement the cost model, every array write operation is followed by a decrement of the potential. Also, each function that receives tokens adds them to the potential of the unbounded array. As an example, we show the (incompletely specified) `set` function.

```
let set (u : uba 'a) (i : int) (x : 'a) (ghost p : int) =
requires { 0 <= i < u.size }                   (* i must be in domain *)
requires { p = 1 }                             (* amortized cost of 'set' is 1 *)
...                                            (* more contracts as needed *)
ghost (u.potential <- u.potential + p) ;       (* store received potential *)
u.data[i] <- Some x ;
ghost (u.potential <- u.potential - 1)         (* pay for write *)
```

The data structure invariants are simpler if the array can only be expanded but not shrunk. We therefore recommend the following sequence of tasks, even if you should hand in just one file `ubarray.mlw` at the end.

Task 5 (5 pts). Specify the data structure invariants of unbounded arrays, including the requirement that potential remain nonnegative. For this task, you may restrict attention to domain extension with the `add` operation and ignore `rem`.

Task 6 (25 pts). Implement and verify the `new`, `len`, `get`, `set`, and `add` operations. Verification of contracts should guarantee the intended meaning of each operation and, together with the data structure invariants, the correct amortized cost if each operation.

Task 7 (10 pts). Implement the `rem` operation and update the data structure invariants to guarantee the correctness of the amortized analysis.

3 Induction (20 pts)

Prove the following theorems in Why3, using the `int.SimpleInduction` module. Your proofs should be in a file `ind.mlw`.

Task 8 (5 pts).

$$\sum_{i=0}^{i=n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

Task 9 (5 pts).

$$\sum_{i=0}^{i=n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$$

Task 10 (10 pts). The correctness of the formula for Pascal's triangle (see Pascal's Triangle on Wikipedia): The entry in row n, column k for $0 \leq k \leq n$ is

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$$