Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών
Τομέας Τεχνολογίας Πληροφορικής & Υπολογιστών
http://courses.softlab.ntua.gr/pl2/

Γλώσσες Προγραμματισμού II

Οι ασκήσεις πρέπει να παραδοθούν στους διδάσκοντες σε ηλεκτρονική μορφή μέσω του συνεργατικού συστήματος ηλεκτρονικής μάθησης moodle.softlab.ntua.gr. Η προθεσμία παράδοσης θα τηρείται αυστηρά. Έχετε δικαίωμα να καθυστερήσετε το πολύ μία άσκηση.

Άσκηση 9 Αξιωματική σημασιολογία

Προθεσμία παράδοσης: 25/3/2018

Σε πρόσφατη γραπτή εξέταση του μαθήματος των πρωτοετών δόθηκε το ακόλουθο πρόβλημα:

> Έστω a ένας μονοδιάστατος πίνακας που περιέχει N ακέραιους αριθμούς ($1 \leq N \leq 1.000.000$) με τιμές μεταξύ 1 και 1.000.000. Να γράψετε μία κομψή και αποδοτική συνάρτηση η οποία να βρίσκει αν υπάρχει αριθμός που εμφανίζεται δύο (ή περισσότερες) φορές μέσα στον πίνακα. Αν υπάρχει τέτοιος αριθμός, η συνάρτησή σας πρέπει να τον επιστρέφει. Αν υπάρχουν περισσότεροι τέτοιοι αριθμοί, μπορείτε να επιστρέφετε όποιον από αυτούς θέλετε. Διαφορετικά, αν όλοι οι αριθμοί εμφανίζονται το πολύ μία φορά, η συνάρτησή σας πρέπει να επιστρέφει 0.
>
> Παράδειγμα 1: ($N = 6$)
> $a = [1, 2, 3, 2, 4, 5]$ findDouble$(N, a) = 2$
>
> Παράδειγμα 2: ($N = 8$)
> $a = [9, 3, 5, 7, 2, 4, 1, 6]$ findDouble$(N, a) = 0$

Ένας σπουδαστής έδωσε την εξής λύση για το παραπάνω πρόβλημα:

```
#include <stdbool.h>

#define MAXV 1000000

int findDouble(int N, int a[]) {
  bool f[MAXV];
  for (int i = 1; i <= MAXV; ++i) f[i-1] = false;
  for (int i = 0; i < N; ++i)
    if (f[a[i]-1]) return a[i]; else f[a[i]-1] = true;
  return 0;
}
```

Αποδείξτε την ορθότητα της συνάρτησης χρησιμοποιώντας αξιωματική σημασιολογία. Συγκεκριμένα, αποδείξτε ότι το αποτέλεσμα της συνάρτησης είναι $r \neq 0$ αν και μόνο αν υπάρχουν δύο στοιχεία του πίνακα $a[i]$ και $a[j]$ με $i \neq j$ και $a[i] = a[j] = r$.

Μπορείτε να λύσετε αυτή την άσκηση με δύο (εναλλακτικούς) τρόπους:

1. Να γράψετε το σώμα της συνάρτησης στην απλή προστακτική γλώσσα των διαφανειών. Υποθέστε ότι η γλώσσα υποστηρίζει όλες τις αριθμητικές πράξεις και πίνακες. Υποθέστε επίσης ότι όλες οι πράξεις υπολογίζουν πάντα το ιδεατό αποτέλεσμα, χωρίς το ενδεχόμενο υπερχείλισης ή αριθμητικού σφάλματος. Αν χρησιμοποιήσετε αυτόν τον τρόπο, παραδώστε ένα αρχείο κειμένου ή PDF που να περιέχει αναλυτικά την απόδειξή σας.

2. Να χρησιμοποιήσετε το εργαλείο επαλήθευσης προγραμμάτων Frama-C, που είναι διαθέσιμο από την ιστοσελίδα http://frama-c.com/. Αν το επιχειρήσετε, ίσως χρειαστεί να εγκαταστήσετε και κάποιο εργαλείο αυτόματης απόδειξης θεωρημάτων, όπως το Alt-Ergo, ή κάποιο σύστημα υποστήριξης αποδείξεων, όπως το Coq. Υπάρχουν σύνδεσμοι προς τέτοια εργαλεία από την ιστοσελίδα του Frama-C. Με μία από τις τελευταίες εκδόσεις του Frama-C (από Neon μέχρι και την τρέχουσα Sulfur) προτείνεται η χρήση του plugin WP (αντί του παλιότερου Jessie). Αν χρησιμοποιήσετε αυτόν τον τρόπο, παραδώστε ένα πρόγραμμα C με σχόλια-annotations για το Frama-C. Στην αρχή του προγράμματος, γράψτε σε ένα σχόλιο την έκδοση του Frama-C και των solvers που χρησιμοποιήσατε, καθώς και την ακριβή γραμμή εντολών που επαληθεύει αυτόματα την ορθότητα του προγράμματος.

```
$ frama-c -wp -wp-prover alt-ergo -wp-rte -wp-timeout 300 -wp-verbose 0 find-double.c
    -then -report
[kernel] Parsing FRAMAC_SHARE/libc/__fc_builtin_for_normalization.i (no preprocessing)
[kernel] Parsing find-double.c (with preprocessing)
[rte] annotating function findDouble
[report] Computing properties status...

------------------------------------------------------------------------------
--- Properties of Function 'findDouble'
------------------------------------------------------------------------------

[  Valid  ] Post-condition (file find-double.c, line 8)
            by Wp.typed.
[  Valid  ] Loop assigns (file find-double.c, line 15)
            by Wp.typed.
[  Valid  ] Loop assigns (file find-double.c, line 22)
            by Wp.typed.
[  Valid  ] Loop variant at loop (file find-double.c, line 18)
            by Wp.typed.
[  Valid  ] Loop variant at loop (file find-double.c, line 25)
            by Wp.typed.
[  Valid  ] Invariant (file find-double.c, line 13)
            by Wp.typed.

... snip ...

[  Valid  ] Default behavior
            by Frama-C kernel.

------------------------------------------------------------------------------
--- Status Report Summary
------------------------------------------------------------------------------
    24 Completely validated
    24 Total
------------------------------------------------------------------------------
```

Εναλλακτικά, μπορείτε να χρησιμοποιήσετε την παρακάτω εντολή που σας φέρνει στο GUI, και να ελέγξετε ότι όλα τα proof obligations είναι πράσινα.

```
$ frama-c-gui -wp -wp-prover alt-ergo -wp-rte -wp-timeout 300 find-double.c
```