



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 11 Αξιωματική σημασιολογία

Προθεσμία παράδοσης: 27/2/2009
(τέλος μαθημάτων)

Η παρακάτω συνάρτηση σε C99 υπολογίζει την ύψωση σε δύναμη ενός αριθμού, χρησιμοποιώντας την τεχνική των διαδοχικών τετραγωνισμών.

```
unsigned long pow (unsigned long x, unsigned int n)
{
    for (unsigned long r = 1; n > 0; n /= 2, x = x*x)
        if (n % 2 == 1)
            r *= x;
    return r;
}
```

1. Γράψτε το αντίστοιχο τμήμα προγράμματος στην απλή προστακτική γλώσσα των σημειώσεων. Δεν πρέπει να αλλάξετε τη δομή του προγράμματος (π.χ. προσθέτοντας νέες μεταβλητές ή εντολές). Υποθέστε ότι όλες οι αριθμητικές πράξεις ορίζονται για απροσήμαστους (unsigned) ακέραιους συνηθισμένου και μεγάλου μεγέθους (int και long). Υποθέστε επίσης ότι όλες οι αριθμητικές πράξεις—εκτός της διαίρεσης με το μηδέν—υπολογίζουν το ιδεατό αποτέλεσμα, χωρίς το ενδεχόμενο υπερχείλισης ή αριθμητικού σφάλματος.
2. Ορίστε κατάλληλη προσυνθήκη και μετασυνθήκη, που να αποδίδουν την επιθυμητή προδιαγραφή του τμήματος προγράμματος. (Προσέξτε την περίπτωση $x = n = 0$.)
3. Αποδείξτε τη μερική ορθότητα του τμήματος προγράμματος χρησιμοποιώντας αξιωματική σημασιολογία.
4. Εναλλακτικά των παραπάνω, μπορείτε αν θέλετε να αποδείξετε την ορθότητα της παραπάνω συνάρτησης με το εργαλείο επαλήθευσης προγραμμάτων Caduceus, που είναι διαθέσιμο από την ιστοσελίδα <http://caduceus.lri.fr/>. Αν το επιχειρήσετε, θα χρειαστεί να εγκαταστήσετε και κάποιο εργαλείο αυτόματης απόδειξης θεωρημάτων, όπως το Ergo, ή κάποιο σύστημα υποστήριξης αποδείξεων, όπως το Coq. Υπάρχουν σύνδεσμοι προς τέτοια εργαλεία από την ιστοσελίδα του Caduceus.