2ο σύνολο Προγραμματιστικών/Θεωρητικών Ασκήσεων

Καταληκτική Ημερομηνία Παράδοσης: 24/05/2025

Συνολικό Βάρος Βαθμολογίας: >35%[1]

Η εργασία είναι **ομαδική (μέχρι 2 φοιτητές ανά ομάδα)**. Την εργασία την καταθέτετε στο eclass, στο μενού εργασίες. Θα πρέπει να καταθέσετε ένα συμπιεσμένο αρχείο (.zip) το οποίο θα περιλαμβάνει τα εξής: α) σε ένα .pdf τις λύσεις των θεωρητικών ασκήσεων – θα εκτιμηθεί θετικά αν έχουν γραφεί ηλεκτρονικά και δεν είναι χειρόγραφες σαρωμένες και β) τα αρχεία με τον πηγαίο κώδικα NETLOGO για τις προγραμματιστικές ασκήσεις μαζί με μία αναφορά (.pdf) σχετικά με τα πειράματά σας και τις παρατηρήσεις σας σε αυτά τα μοντέλα.

Θεωρητικές Ασκήσεις

Άσκηση 1 (20%)

Να δώσετε ένα πρωτόκολλο πληθυσμού (population protocol) που να υπολογίζει ευσταθώς (stably compute) αν υπάρχει άρτιο αρχικά πλήθος από 1 στους κόμβους. Θεωρείστε ότι αρχικά κάθε κόμβος (η είσοδος) περιέχει 0 ή 1. Όλες οι σχεδιαστικές επιλογές αφήνονται σε εσάς. Σε κάθε περίπτωση θα πρέπει να επιχειρηματολογήσετε για την ορθότητα του αλγορίθμου σας και τη χρονική του πολυπλοκότητα.

Άσκηση 2 (20%)

Αυτή η άσκηση αφορά την επιλογή του κόμβου που θα προτείνει το επόμενο μπλοκ σε ένα σύστημα blockchain που χρησιμοποιεί Proof-of-Stake (PoS). Υποθέτουμε ότι χρησιμοποιείται η στρατηγική της επιλογής της μακρύτερης αλυσίδας. Υποθέστε ότι έχουμε πρόσβαση σε ένα τυχαίο αριθμό $r \in [0,1]$, και ο στόχος είναι να επιλέξουμε έναν από τους n πράκτορες που έχουν στοιχηματίσει για το επόμενο μπλοκ όπου το στοίχημα για τον καθένα από αυτούς είναι $s_1, s_2, \dots, s_n$. Επομένως, ο *i*-οστός πράκτορας θα πρέπει να επιλεχθεί με πιθανότητα $\frac{s_i}{\sum_{k=1}^{n} s_k}$.

Στον παρακάτω αλγόριθμο, ο αριθμός r χρησιμοποιείται για να επιλέξει ομοιόμορφα τυχαία ένα νόμισμα c (νόμισμα ελάχιστης αξίας, π.χ., για το bitcoin ένα satoshi ή για το Ethereum ένα wei). Το νόμισμα c επιλέγεται από αυτά που δημιουργούνται από μία coinbase συναλλαγή, δηλαδή μία συναλλαγή που κόβει νέα νομίσματα για την αμοιβή του νέου προτεινόμενου μπλοκ (δεν μας ενδιαφέρουν οι λεπτομέρειες επιλογής του c από τον r, απλά υποθέστε ότι το c έχει επιλεγεί).

1. Βρες τον τρέχοντα ιδιοκτήτη p_k του νομίσματος c.

[1] Δεν θέλω να καθορίσω ακριβώς το βάρος ώστε να υπάρχει μία σχετική ευελιξία στη βαθμολόγηση μιας και δεν υπάρχει προηγούμενη εμπειρία σε αυτό το μάθημα (θα είναι φιλική προς τους φοιτητές 😊).

2. Αν ο p_k είναι ένας από τους n πράκτορες που έχουν στοιχηματίσει και το c είναι ένα από τα νομίσματα που έχει στοιχηματίσει, θέσε τον p_k ως αυτόν που θα προτείνει το επόμενο μπλοκ.
3. Αν δεν ισχύει κάτι από τα προηγούμενα, επαναεπέλεξε άλλο νόμισμα και επανέλαβε.

Αποδείξτε ότι ο παραπάνω αλγόριθμος θα επιλέξει αυτόν που θα προτείνει το επόμενο μπλοκ με την επιθυμητή πιθανότητα.

Προγραμματιστικές Ασκήσεις

Στις παρακάτω προγραμματιστικές ασκήσεις θα κληθείτε να χρησιμοποιήσετε το περιβάλλον NETLOGO για την υλοποίηση. Σας ζητείται να υλοποιήσετε τους αλγορίθμους και να ελέγξετε πειραματικά ότι τα αποτελέσματα είναι τα αναμενόμενα. Για όλες τις ασκήσεις θα δώσετε μία αναφορά με τις παρατηρήσεις σας.

Άσκηση 1 (30%)

Να υλοποιήσετε μία προσομοίωση του πρωτοκόλλου πληθυσμού που δώσατε στην Άσκηση 1 των θεωρητικών ασκήσεων. Οι αρχικές τιμές των 0 και 1 μπορεί να είναι τυχαία κατανεμημένες ή να ακολουθούν άλλες κατανομές σύμφωνα με δικές σας επιλογές. Η οπτικοποίηση των αποτελεσμάτων είναι δικιά σας επιλογή (π.χ., ένα σύνολο από σταθερούς κόμβους που οι αλληλεπιδράσεις φαίνονται με την οπτικοποίηση των γραμμών σε κάθε γύρο ή κινούμενους κόμβους που όταν συγκρουστούν έχουν μία αλληλεπίδραση). Δεν χρειάζεται να έχετε μία αλληλεπίδραση σε κάθε γύρο αλλά μπορείτε να επιτρέψετε και παραλληλισμό. Δώστε αποτελέσματα για το χρόνο που χρειάζεται ο υπολογισμός ανάλογα με το μέγεθος του πληθυσμού. Συμφωνούν τα πειραματικά αποτελέσματά με τα θεωρητικά αποτελέσματα της Άσκησης 1;

Άσκηση 2 (30%)

Ο θείος Κώστας εξηγεί στον ανιψιό του Ελισαίο τη χρήση του ScroogeCoin αλλά ο Ελισαίος δεν την καταλαβαίνει. Σκέφτεται λοιπόν ο θείος ότι μία προσομοίωση σε Netlogo θα μπορούσε να του δείξει οπτικά πως δουλεύει το συγκεκριμένο νόμισμα καθώς και να του δείξει και τις αδυναμίες του (π.χ., ότι μπορεί να αποκλείει κάποιους από το δικαίωμα που έχουν να κάνουν συναλλαγές).

Ο Διδάσκων έχει το δικαίωμα κλήσης σε προφορική εξέταση όταν υπάρχει βάσιμη υποψία ότι έχουν αντιγράψει.