Πανεπιστήμιο Πατρών

Τμήμα Μηχανικών Η/Υ και Πληροφορικής

2ο Σύνολο Θεωρητικών Ασκήσεων

Θεόφραστος Παξιμάδης 1093460

Κωνσταντίνος Αναστασόπουλος 1093320

Άσκηση 1

Το αρχικό population protocol που δημιουργήθηκε που υπολογίζει ευσταθώς αν υπάρχει περιττό ή άρτιο πλήθος από 1 στους κόμβους ήταν το παρακάτω:

States Q: {1, 0, odd, even}

Output O: Q{1} = 1, Q{odd} = 1, Q{0} = 0, Q{even} = 0

Initial States I: {0, 1}

Transitions T: (1) T(1,0) → (1, odd)

(2) T(1,1) → (even, even)

(3) T(0,0) → (even, even)

(4) T(1, even) → (1, odd)

(5) T(odd, even) → (even, even)

(Δεν αναγράφονται οι συμμετρικοί κανόνες, για παράδειγμα οι T(1,0) και T(0,1) είναι ίδιοι)

Εξήγηση: Εκτός από τις αρχικές καταστάσεις 0 και 1, εισάγουμε δύο ακόμα καταστάσεις odd και even, ομοίως με τις passive καταστάσεις των ninjas. Odd σημαίνει πως ο κόμβος νομίζει ότι υπάρχει περιττός αριθμός από άσσους ενώ even άρτιος. Σε περίπτωση όπου δύο μηδενικά ή δύο άσσοι αλληλοεπιδρούν, τότε και οι δύο γίνονται even.

Η λογική είναι πως εάν υπάρχει άρτιο πλήθος άσσων αρχικά, τότε σε κάποιο σημείο όλοι θα αλληλοεπιδράσουν μεταξύ τους και δεν θα υπάρχουν πλέον άσσοι. Άρα τα odd και even που θα έχουν δημιουργηθεί (even θα υπάρχουν σίγουρα από τους τελευταίους άσσους που θα αλληλοεπιδράσουν), τελικά από τον κανόνα 5 θα καταλήξουν όλα σε even και θα έχει επιτευχθεί το consensus. Επίσης τα μηδενικά δεν επηρεάζουν διότι Q{0} = 0, Q{even} = 0.

Στην περίπτωση των περιττών άσσων, σίγουρα θα φτάσουμε σε ένα σημείο όπου θα έχει απομείνει μόνο ένας άσσος. Τότε, ο άσσος αυτός από τους κανόνες 1 και κυρίως 4, θα προσπαθεί να μετατρέψει τους άλλους agents σε odd ώστε να καταλήξουν σε consensus odd.

Ωστόσο, η συγκεκριμένη υλοποίηση αντιμετωπίζει το ίδιο πρόβλημα που έχει και το δεύτερο πρωτόκολλο των ninjas των διαφανειών. Στην περίπτωση των περιττών άσσων, όσο ο τελευταίος άσσος προσπαθεί να μετατρέψει τους υπόλοιπους agents σε odd, τα odd που δημιουργούνται απαλείφονται από τον κανόνα 5 και γίνονται πάλι even. Άρα εξαιτίας των κανόνων 4 και 5, υπάρχει μια μορφή αναδρομής που καθυστερεί πολύ το τελικό consensus.

Για να απαλειφθεί αυτή η αναδρομή, προσθέσαμε δύο νέες καταστάσεις ισοπαλίας (όπως είναι και στην περίπτωση του τρίτου πρωτόκολλου των ninjas). Τις καταστάσεις αυτές τις ονομάζουμε Tie και tie (active και passive αντίστοιχα) και το ανανεωμένο πρωτόκολλο φαίνεται παρακάτω:

States Q: {1, 0, odd, even, Tie, tie}

Output O: Q{1} = 1, Q{odd} = 1, Q{0} = 0, Q{even} = 0, Q{Tie} = 0, Q{tie} = 0

Initial States I: {0, 1}

Transitions T: (1) T(1,0) → (1, odd)

(2) T(1,1) → (even, even)

(3) T(0,0) → (even, even)

(4) T(1, even) → (1, odd)

(5) T(odd, even) → (Tie, tie)

(6) T(odd, Tie) → (Tie, tie)

(7) T(even, Tie) → (Tie, tie)

(8) T(1, Tie) → (1, odd)

(9) T(1, tie) → (1, odd)

Αυτή η αλλαγή λειτουργεί ακριβώς όπως και στο πρωτόκολλο 3 των ninjas και επιτυγχάνει να αποφύγει τις αναδρομές που συναντήσαμε προηγουμένως.

Ειδικότερα, εάν υπάρχει άρτιος αριθμός άσσων, τότε πάλι σε κάποιο σημείο θα έχουν απαλειφθεί όλοι οι άσσοι. Χωρίς να υπάρχει απομείναντας άσσος, όλοι οι υπόλοιποι agents με τιμές even, odd, Tie ή tie, από τους κανόνες 5,6 και 7 τελικά θα καταλήξουν σε κατάσταση Tie ή tie που δηλώνει ότι αρχικά υπάρχουν άρτιοι άσσοι (Q{Tie} = 0, Q{tie} = 0).

Στην περίπτωση των περιττών άσσων, ο τελευταίος άσσος που θα απομείνει θα προσπαθεί πάλι να μετατρέψει τους υπόλοιπους agents σε odd (κανόνες 4, 8, 9). Αν και υπάρχει πάλι μία ανάδρομή από τους κανόνες 4 και 5, όπως και από τους 4 και 6, αυτή η αναδρομή είναι μικρότερης σημασίας για τον ακόλουθο λόγο. Τα Tie που δημιουργούνται είναι κατά κύριο λόγο αυτά που απαλείφουν τα (κανόνας 6, ο κανόνας 5 πάλι απαλείφει τα odd αλλά καταλήγουν σε Tie, δηλαδή πάλι στον κανόνα 6). Όμως, από τον κανόνα 8, ο τελευταίος άσσος εξαλείφει σιγά σιγά τα Tie, το οποίο σημαίνει ότι έχει μεγαλύτερη προτεραιότητα. Άρα τελικά, ο τελευταίος άσσος θα μπορέσει να μετατρέψει όλα τα Tie, tie και even σε odd, με περιορισμένη αναδρομή από τα Tie.

Η χρονική πολυπλοκότητα του παραπάνω population protocol είναι κάτι που αδυνατώ να αναλύσω, αλλά είμαι σχεδόν βέβαιος ότι είναι ίδια με αυτήν του τρίτου πρωτόκολλου των ninjas από τις διαφάνειες.

Άσκηση 2

Ο αλγόριθμος Proof-of-Stake που χρησιμοποιείται στο υπό μελέτη σύστημα είναι ο εξής:

Αρχικά επιλέγεται ομοιόμορφα ένα νόμισμα c που προέκυψε από μια coinbase συναλλαγή. Αφού όλα τα νομίσματα στο δίκτυο δημιουργούνται από coinbase συναλλαγές, το c είναι ένα οποιοδήποτε νόμισμα του δικτύου. Η πιθανότητα επιλογής του είναι:

$$\frac{1}{αριθμός\ νομισμάτων}$$

Εφόσον χρησιμοποιείται η τεχνική της μακρύτερης αλυσίδας τελικά το σύστημα θα κάνει επιλογή ακόμα και αν προκύψει διακλάδωση στην αλυσίδα. Αφού επιλεγεί το νόμισμα, ο αλγόριθμος ακολουθεί τρία βήματα.

1. Βρες τον τρέχοντα ιδιοκτήτη p_k του νομίσματος c.
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.

Το δίκτυο περιέχει δύο είδη χρηστών. Αυτούς που στοιχημάτισαν και αυτούς που δε στοιχημάτισαν. Προφανώς, από το βήμα 2, αν κάποιος χρήστης δε στοιχημάτισε, η πιθανότητα επιλογής του είναι:

$$P[επιλογή\ p_k] = 0$$

Επίσης τα νομίσματα που δεν έχουν στοιχηματιστεί δεν επηρεάζουν την επιλογή. Αν ένα νόμισμα επηρεάζει την επιλογή, τότε είναι ένα από τα στοιχηματισμένα.

Ο κάθε χρήστης που στοιχηματίζει, έχει ένα stake. Π.χ. αν ο χρήστης p_k στοιχηματίσει x από τα νομίσματά του, τότε έχει s_k = x. Προφανώς, αν στοιχηματίσουν n χρήστες, τα συνολικά στοιχηματισμένα νομίσματα είναι ίσα με το άθροισμα όλων των stakes.

$$S = \sum_{k=1}^{n} s_k$$

Αν επιλεγεί ένα νόμισμα, έστω c από τα στοιχηματισμένα, εφόσον επιλέγεται ομοιόμορφα, η πιθανότητα επιλογής του είναι:

$$P[επιλογή\ c] = \frac{1}{S}$$

Η πιθανότητα να επιλεγεί ένας χρήστης που έχει στοιχηματίσει ισούται με την πιθανότητα να επιλεγεί ένα από τα νομίσματά του. Αυτό ισούται με το άθροισμα των πιθανοτήτων να επιλεγεί κάθε συγκεκριμένο νόμισμά του.

$$P[\text{επιλογή } p_k] =$$

$$P[\text{επιλογή } 1ου \text{ νομίσματος του } p_k] + \cdots$$

$$+ P[\text{επιλογή } x - \text{οστού νομίσματος του } p_k] =$$

$$\frac{1}{S} + \frac{1}{S} + \cdots + \frac{1}{S} =$$

$$\frac{s_k}{S}$$

Που είναι το ζητούμενο.