

3ο PROJECT ΑΠΟΚΕΝΤΡΩΜΕΝΟΣ ΥΠΟΛΟΓΙΣΜΟΣ & ΜΟΝΤΕΛΟΠΟΙΗΣΗ

ΛΕΚΚΑΣ ΓΕΩΡΓΙΟΣ ΑΜ:1067430 Έτος 5ο

ΠΑΠΑΝΙΚΟΛΑΟΥ ΠΑΝΑΓΙΩΤΗΣ ΑΜ:1067431 Έτος 5ο

Περιεχόμενα

- A. Θεωρητική Άσκηση 1
- B. Θεωρητική Άσκηση 2
- Γ. Θεωρητική Άσκηση 3
- Δ. Προγραμματιστική Άσκηση 1
- Ε. Προγραμματιστική Άσκηση 2

Α.Θεωρητική Άσκηση 1

Οι μεταβλητές του συστήματος είναι οι x_1 , x_2 και οι οποίες σε μορφή διανύσματος γράφονται ως εξής:

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}.$$

1. Οπότε το μητρώο A είναι το εξής : $A = \begin{bmatrix} 1 & 0 \\ a & (1-a) \end{bmatrix}.$

Ένα μητρώο είναι στοχαστικό ως προς τις γραμμές όταν το άθροισμα των στοιχείων της κάθε γραμμής είναι ίσο με 1. Πράγματι στο μητρώο A παρατηρούμε πως $1+0=1$ και $a+(1-a)=1$. **Επομένως το μητρώο A είναι στοχαστικό ως προς τις γραμμές.**

2. Για να υπολογίσουμε τις ιδιοτιμές και τα ιδιοδιανύσματα του μητρώου A θα χρησιμοποιήσουμε τους τύπους: $\det(A - \lambda * I) = 0$ όπου λ οι ιδιοτιμές και I το ταυτοτικό μητρώο , $(A - \lambda * I) * x = 0$.

Συνεπώς έχουμε: $(A - \lambda * I) = \begin{bmatrix} 1 & 0 \\ a & (1-a) \end{bmatrix} - \lambda * \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1-\lambda & 0 \\ a & (1-a-\lambda) \end{bmatrix}.$

Η ορίζουσα του A είναι : $\det(A - \lambda * I) = (1-\lambda) * (1-a-\lambda)$, οπότε λύνοντας το $\det(A - \lambda * I) = 0$ οι ιδιοτιμές είναι οι : $\lambda = 1$ και $\lambda = 1-a$.

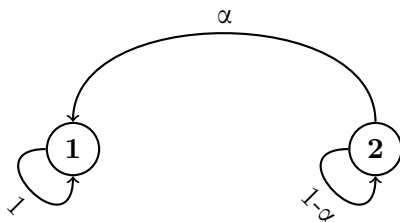
Στη συνέχεια για να υπολογίσουμε τα ιδιοδιανύσματα , θα χρησιμοποιήσουμε τον τύπο $(A - \lambda * I) * \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$

Για $\lambda = 1$ έχουμε : $\begin{bmatrix} 0 & 0 \\ a & -a \end{bmatrix} * \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \Rightarrow \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ (1ο ιδιοδιάνυσμα) ,

Για $\lambda = 1-a$ έχουμε : $\begin{bmatrix} a & 0 \\ a & 0 \end{bmatrix} * \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \Rightarrow \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ (2ο ιδιοδιάνυσμα)

3. Το κατευθυνόμενο διάνυσμα G προκύπτει από το μητρώο A και συγκεκριμένα από τη μελέτη των στοιχείων του και τη ταύτιση τους ως μεταβάσεις από τον ένα κόμβο στον άλλο.

Συνεπώς το κατευθυνόμενο γράφημα G είναι το εξής:



Όσον αφορά τη συνεκτικότητα του γραφήματος, το γράφημα είναι **ασθενώς συνεκτικό** καθώς δεν υπάρχει διαδρομή από τη κορυφή 1 στη κορυφή 2. Για να ήταν ισχυρά συνεκτικό θα έπρεπε να υπήρχε διαδρομή από και προς όλες τις κορυφές του γραφήματος.

4. Ο αλγόριθμος ως συνάρτηση των αρχικών τιμών των παικτών συγκλίνει κάθε φορά στο x_1 .

Β.Θεωρητική Άσκηση 2

1. Για να απαντηθεί σωστά το ερώτημα θα πρέπει αρχικά να γίνει κατανοητό τι συμβαίνει στο blockchain τη στιγμή που υποβληθεί μία διπλοξοδευμένη συναλλαγή στο δίκτυο.

Εκείνη τη στιγμή δημιουργείται στο δίκτυο ένα fork. Ένα fork δημιουργείται όταν δυο miners τυχαίνει να εγκρίνουν ταυτόχρονα ένα block συναλλαγών και έτσι η αλυσίδα ενημερώνεται προς 2 κατευθύνσεις δημιουργώντας πολλαπλά προβλήματα στο δίκτυο. Έτσι για να αφαιρεθεί το fork οι miners δουλεύουν για να επεκτείνουν αυτό που είναι μεγαλύτερο στο δικό τους αντίγραφο του blockchain, ως ότου εγκριθεί η συναλλαγή.

Στη περίπτωση της άσκησης παρατηρούμε πως τη μεγαλύτερη υπολογιστική δύναμη την έχουν οι miners που δουλεύουν την υλοποίηση A (80% έναντι 20% της B). Συνεπώς συνεχίζουν να δουλεύουν στην υλοποίηση A επεκτείνοντας την αλυσίδα του, κάνοντάς τη μεγαλύτερη από τη αλυσίδα του blockchain της υλοποίησης B. Αυτό έχει ως αποτέλεσμα να μετακινηθούν οι miners της B στην A και κατά συνέπεια να οριστικοποιηθεί το double-spending.

2. Σε αντίθεση με το υποερώτημα 1, τώρα 20% της υπολογιστικής ισχύος τρέχει την υλοποίηση A και 80% την B. Συνεπώς η υλοποίηση B θα έχει μεγαλύτερη αλυσίδα και έτσι οι miners καταλαβαίνουν πως η συγκεκριμένη συναλλαγή αφορά double-spending και προχωρούν στην αναγνώριση της ως άκυρη.

Γ.Θεωρητική Άσκηση 3

Ο Μπομπ **δεν πρέπει** να δεχτεί το πρωτόκολλο της υπόθεσης.

Καταλήγουμε στο συγκεκριμένο συμπέρασμα καθώς παρατηρούμε πως η Αλίκη μπορεί να στείλει το s στο CM μετά από χρόνο 2Δ και να πάρει το επιτυχώς το πράσινο νόμισμα, και ταυτόχρονα ο Μπομπ να μην μπορεί να στείλει το s στο CA καθώς ο χρόνος 2Δ θα έχει ήδη τελείωσει.