Γιάννης Ρεφανίδης

ΘΕΩΡΙΑ ΥΠΟΛΟΓΙΣΜΟΥ

Απρίλιος 2023

Εργασία #01 – Μηχανές Mealy και Moore

Ένας αιτιοκρατικός μετασχηματιστής πεπερασμένων καταστάσεων (deterministic finite-state transducer, DFST) είναι ένα αιτιοκρατικό πεπερασμένο αυτόματο με τις εξής διαφορές:

- Δεν έχει τελικές καταστάσεις, η λειτουργία του σταματά όταν ολοκληρωθεί η ανάγνωση της λέξης εισόδου.
- Σε κάθε μετάβαση έχει τη δυνατότητα να εξάγει κανένα, ένα ή περισσότερα σύμβολα. Με άλλα λόγια, το DFST μετασχηματίζει τη λέξη εισόδου σε μια λέξη εξόδου.

Σκοπός του DFST δεν είναι λοιπόν η αποδοχή ή η απόρριψη των λέξεων της εισόδου, αλλά ο μετασχηματισμός τους σε νέες λέξεις. Οι δυνατότητες μετασχηματισμού των DFST δεν είναι απεριόριστες, αλλά περιορίζονται από τις δυνατότητες των πεπερασμένων αυτομάτων. Θα μπορούσε κανείς να θεωρήσει τα DFST ως γενίκευση των πεπερασμένων αυτομάτων, μιας και ένα DFST θα μπορούσε, με την ολοκλήρωση ανάγνωσης μιας λέξης, να εξάγει ένα σύμβολο που καθορίζει την αποδοχή ή μη αυτής.

Πάνω στα βελάκια στο διάγραμμα έχουμε δύο ετικέτες: την ετικέτα εισόδου και την ετικέτα εξόδου.

Στο πρόγραμμα JFLAP οι αιτιοκρατικοί μετασχηματιστές πεπερασμένων καταστάσεων αναφέρονται ως μηχανές Mealy (Mealy machines)[1,2]. Εάν μια μηχανή Mealy έχει ένα σύμβολο ως έξοδο σε κάθε βήμα, τότε θεωρείται απλή (simple), αλλιώς θεωρείται πολύπλοκη (complex).

Μια παραλλαγή των μηχανών Mealy (και των DFST) είναι οι μηχανές Moore (Moore machines)[3,4]. Σε αυτές, η έξοδος προκύπτει από τις καταστάσεις και όχι από τις μεταβάσεις. Δηλαδή, κάθε κατάσταση μπορεί να έχει κανένα, ένα ή περισσότερα σύμβολα εξόδου. Κάθε φορά που ο υπολογισμός επισκέπτεται την κατάσταση, τα σύμβολα της κατάστασης εμφανίζονται στην έξοδο.

Το JFLAP υποστηρίζει complex μηχανές Mealy και Moore.

Οι μηχανές Mealy και Moore είναι ισοδύναμες μεταξύ τους, καθώς και με τα απλά πεπερασμένα αυτόματα. Η διαφορά των μηχανών Mealy και Moore έγκειται μόνο σε θέματα συγχρονισμού: Εάν δεν μας ενδιαφέρει μόνο ποια έξοδος θα παραχθεί, αλλά και πότε θα παραχθεί αυτή η έξοδος (υποθέτοντας ότι οι μηχανές λειτουργούν με «σύγχρονο» (synchronous) τρόπο, δηλαδή είναι συγχρονισμένες με κάποιο ρολόι και σε κάθε κτύπο του ρολογιού εκτελούν ένα βήμα υπολογισμού), οι μηχανές Mealy παράγουν γρηγορότερα την έξοδό τους και υπάρχουν περιπτώσεις που δεν μπορεί να κατασκευαστεί εξίσου «γρήγορη» μηχανή Moore.

Τόσο στις μηχανές Mealy, όσο και στις Moore, δεν επιτρέπονται ε-μεταβάσεις ή οποιαδήποτε μορφή μη-αιτιοκρατίας.

Βασικό χαρακτηριστικό των μηχανών Mealy και Moore είναι ότι η έξοδος μπορεί να επηρεάζεται από πεπερασμένο πλήθος προηγουμένων εισόδων. Πολλές φορές χρειάζεται, με την ολοκλήρωση της λέξης εισόδου, να εισαχθεί ένα ακόμη σύμβολο που υποδηλώνει ακριβώς την ολοκλήρωση της λέξης εισόδου, με το οποίο οι μηχανές θα παράγουν την τελευταία τους έξοδο.

Μια από τις εφαρμογές των μηχανών Mealy και Moore είναι και η κρυπτογραφία.

Έστω ο παρακάτω αλγόριθμος κρυπτογράφησης: Έχουμε στην είσοδο μια ακολουθία από μηδενικά και άσσους, π.χ. την:

0 1 0 1 0 0 1 0 0 1

[1] https://en.wikipedia.org/wiki/Mealy_machine
[2] https://jflap.org/tutorial/mealy/mealyMachines.html
[3] https://en.wikipedia.org/wiki/Moore_machine
[4] https://jflap.org/tutorial/mealy/mooreMachines.html

Διαβάζουμε ένα-ένα τα ψηφία της ακολουθίας και αρχίζουμε να εξάγουμε κρυπτογραφημένα ψηφία από την ανάγνωση του τρίτου ψηφίου και μετά. Έστω ο εξής κανόνας: Η έξοδος ισούται με το τελευταίο ψηφίο του αθροίσματος των τριών τελευταίων ψηφίων. Για το λόγο αυτό, θα χρειαστεί να θεωρήσουμε ότι υπάρχουν δύο επιπλέον μηδενικά στο τέλος της εισόδου. Για την παραπάνω είσοδο, η έξοδος είναι ως εξής:

0	1	0	1	0	0	1	0	0	1	0	0
		1	0	1	1	1	1	1	1	1	1

Στο παραπάνω σχήμα, η τιμή του x προκύπτει από τις τιμές των a, b, και c:

a	b	c
		x

Ειδικότερα, αν το άθροισμα των a, b, και c είναι (στο δυαδικό σύστημα αρίθμησης) 01 ή 11, το x ισούται με 1. Αλλιώς, αν το άθροισμα των a, b και c είναι (στο δυαδικό σύστημα αρίθμησης) 00 ή 10, το x ισούται με 0.

Για την αποκωδικοποίηση, προχωράμε από το τέλος προς την αρχή, λαμβάνοντας υπόψη τα δύο τελευταία ψηφία που προστέθηκαν. Η διαδικασία της αποκωδικοποίησης φαίνεται παρακάτω:

1	0	1	1	1	1	1	1	1	1		
0	1	0	1	0	0	1	0	0	1	0	0

Ομοίως, στο παραπάνω σχήμα, η τιμή του x προκύπτει από τις τιμές των a, b, και c:

a		
x	b	c

Ειδικότερα, αν το άθροισμα των a, b, και c είναι (στο δυαδικό σύστημα αρίθμησης) 01 ή 11, το x ισούται με 1. Αλλιώς, αν το άθροισμα των a, b και c είναι (στο δυαδικό σύστημα αρίθμησης) 00 ή 10, το x ισούται με 0.

Με βάση τα παραπάνω:

Α) Κατασκευάστε στο JFLAP δύο μηχανές Mealy, ένα για την κωδικοποίηση και ένα για την αποκωδικοποίηση σύμφωνα με την παραπάνω διαδικασία.

Β) Κατασκευάστε στο JFLAP δύο μηχανές Moore, ένα για την κωδικοποίηση και ένα για την αποκωδικοποίηση σύμφωνα με την παραπάνω διαδικασία.

Θα πρέπει να υποβάλλετε τις τέσσερις μηχανές, μαζί με ένα έγγραφο κειμένου (docx, open office κλπ), στο οποίο θα έχετε σύντομη περιγραφή της λειτουργίας των αυτομάτων σας, μαζί με ένα παραδείγματα κρυπτογράφησης/αποκρυπτογράφησης για κάθε ζευγάρι αυτομάτων.