ΘΕΩΡΗΤΙΚΗ ΠΛΗΡΟΦΟΡΙΚΗ Ι
Σημειώσεις

Γεώργιος Ραχώνης
Καθηγητής
Τμήμα Μαθηματικών, Α.Π.Θ.

Θεσσαλονίκη, 2024

Περιεχόμενα

Εισαγωγή

Η *Θεωρητική Πληροφορική* είναι ο κλάδος των Μαθηματικών που ασχολείται με προβλήματα που αναφύονται στην επιστήμη της Πληροφορικής. Σχετικά νέος, έχει τις ρίζες του στη δεκαετία του 1930 όταν οι John von Neumann, Alan Turing, Alonzo Church, Emil Post και Claude Shannon προσπάθησαν να θεμελιώσουν με αυστηρά μαθηματικό τρόπο τις έννοιες της πληροφορίας, της υπολογισιμότητας και του ψηφιακού υπολογιστή. Στη δεκαετία του 1940 είχε ήδη κατασκευαστεί ο πρώτος ηλεκτρονικός υπολογιστής, ο ENIAC (1943-1946), του οποίου τα κυκλώματα υλοποιούνταν με (περισσότερες από 18.000) ηλεκτρονικές λυχνίες. Στη δεκαετία του 1950 κατασκευάστηκαν ο TRADIC (1951-1954) και ο CADET (1955) οι πρώτοι ηλεκτρονικοί υπολογιστές με transistors, και αργότερα στη δεκαετία του 1980 έγινε ευρέως γνωστός, με το όνομα PC (Personal Computer), ο προσωπικός υπολογιστής, για να φτάσουμε στη σημερινή τεχνολογία των laptops, tablets, κλπ. Στις μέρες μας όλο και περισσότερα υπολογιστικά συστήματα ενσωματώνουν χαρακτηριστικά της Τεχνητής Νοημοσύνης (AI = Artificial Intelligence). Ειδικότερα, τα αποτελέσματα από την έρευνα στην θεωρία Μηχανικής Μάθησης (Machine Learning) προϊδεάζουν για σημαντικές εφαρμογές στην ιατρική, στην ασφάλεια των δικτύων, στην πρόβλεψη καταναλωτικών συμπεριφορών, στο στρατιωτικό τομέα, κλπ. Παρόλα αυτά, θεμελιώδη ερωτήματα απασχολούσαν τους επιστήμονες ήδη από τη δεκαετία του 1930, ενώ νέα προβλήματα αναφύονται ιδιαίτερα με τους κάθε μορφής σύγχρονους υπολογιστές, το Διαδίκτυο, την Τεχνητή Νοημοσύνη,τα Αυτόνομα Συστήματα κλπ. Για παράδειγμα:

- Τι είδους προβλήματα μπορούν να λύσουν οι υπολογιστές;
- Μπορούν οι αλγόριθμοι για συγκεκριμένα προβλήματα να υλοποιηθούν σε "πραγματικό χρόνο";
- Μπορούμε να παραστήσουμε αλγοριθμικά τις φυσικές γλώσσες και συνεπώς να κατασκευάσουμε αξιόπιστους μεταφραστές;
- Πως μπορούμε να εντοπίσουμε τα λογικά λάθη στον κώδικα των προγραμμάτων;
- Μπορούμε να "αποφασίσουμε" αν δύο προγράμματα είναι ισοδύναμα;

- Μπορούμε από ένα πρόγραμμα να κατασκευάσουμε ένα ισοδύναμο "οικονομικότερο";
- Μπορούμε να απλοποιήσουμε την επικοινωνία ανθρώπου-μηχανής;
- Μπορούμε να περιγράψουμε αλγοριθμικά τις σοβαρές ασθένειες;
- Πόσο ασφαλείς είναι οι συναλλαγές μέσω Διαδικτύου;
- Προστατεύονται πραγματικά τα δεδομένα των υπολογιστών και των κινητών μας τηλεφώνων από υποκλοπές;
- Πως θα απαντήσουμε στα ηθικά διλήμματα που προκύπτουν από τη χρήση της Τεχνητής Νοημοσύνης;
- Πως θα διαχειρισθούμε με ασφάλεια τον τεράστιο όγκο δεδομένων (Big Data) που χρειάζονται σε πολλές εφαρμογές;
- Πόσο αξιόπιστα είναι σήμερα τα Αυτόνομα Συστήματα;
- Καθώς οι ηλεκτρονικοί υπολογιστές έχουν περιορισμένες δυνατότητες ταχύτητας (με "άνω φράγμα" την ταχύτητα του ηλεκτρικού ρεύματος) μπορούμε να κατασκευάσουμε υπολογιστικές μηχανές χρησιμοποιώντας "κάποια διαφορετική τεχνολογία";
- ....

Από τη μελέτη αυτών των προβλημάτων έγινε φανερό ότι για την αντιμετώπισή τους απαιτούνται εργαλεία από διάφορα πεδία των Μαθηματικών, όπως για παράδειγμα *τη Καθολική Άλγεβρα, τη Λογική, τη Θεωρία Παιγνίων, τη Θεωρία Πιθανοτήτων, τη Θεωρία Αριθμών,* κλπ., και σε κάποιες περιπτώσεις και από άλλες επιστήμες όπως *τη Φυσική*, *τη Γλωσσολογία*, *τη Βιολογία* και *την Ιατρική*. Όπως προαναφέρθηκε, οι πρώτες προσπάθειες για την μαθηματική περιγραφή της πληροφορίας, της υπολογισιμότητας και του ψηφιακού υπολογιστή ξεκίνησαν τη δεκαετία του 1930. Εντούτοις αποδείχθηκε, πολύ αργότερα, ότι εργασίες με καθαρά "μαθηματικό προσανατολισμό" ήδη από το 1906, όπως για παράδειγμα του Alex Thue [15] είχαν σημαντική συμβολή στην αυστηρή μαθηματική προσέγγιση της Πληροφορικής. Από τη δεκαετία του 1950 μέχρι και τη δεκαετία του 1970 αξιόλογοι μαθηματικοί θεμελίωσαν τη "Θεωρία Τυπικών Γλωσσών" που αποτελεί τη βάση της Θεωρητικής Πληροφορικής. Ενδεικτικά μόνο, αναφέρουμε τους Stephen Kleene, Marcel-Paul Schützenberger, Arto Salomaa, και Samuel Eilenberg καθώς τον διάσημο γλωσσολόγο Noam Chomsky. Το 1973 κυκλοφόρησε το βιβλίο *Formal Languages* [14] του Arto Salomaa, το πρώτο που αναφερόταν στη Θεωρία Τυπικών Γλωσσών. Το 1974 και 1976 εκδόθηκαν αντίστοιχα, ο πρώτος και δεύτερος τόμος του βιβλίου *Automata, Languages and Machines* [2, 3] του Samulel Eilenberg. Όπως χαρακτηριστικά αναφέρει ο Eilenberg, το δίτομο αυτό έργο αυτό απευθύνεται σε μαθηματικούς και επιστήμονες της Πληροφορικής. Σε μαθηματικούς, γιατί διαπραγματεύεται στην ουσία ένα νέο πεδίο της Άλγεβρας, με τεχνικές και αποτελέσματα βαθιά και κομψά κάτι που οφείλεται στους λόγους για τους οποίους αναπτύχθηκε το πεδίο αυτό. Στους επιστήμονες της Πληροφορικής για να τους εφοδιάσει με τα κατάλληλα μαθηματικά εργαλεία, απαραίτητα για την έρευνά τους. Για να αντιληφθεί κανείς την εξέλιξη της Θεωρητικής Πληροφορικής αναφέρουμε ενδεικτικά ότι οι τρείς τόμοι 889, 528 και 625 σελίδων αντίστοιχα του "*Handbook of Formal Languages*" [10, 11, 12] που κυκλοφόρησε το 1997, περιέχουν τα ως τότε γνωστά αποτελέσματα με συνοπτικές μόνο αποδείξεις. Πρόσφατα κυκλοφόρησε το δίτομο έργο "*Handbook of Automata Theory*" [8, 9], 1493 σελίδων, που παρουσιάζει συνοπτικά τα πιο σημαντικά αποτελέσματα στην θεωρία των αυτομάτων καθώς και τις εφαρμογές τους σε άλλους κλάδους των Μαθηματικών και της Πληροφορικής. Τα αξιολογότερα ερευνητικά περιοδικά της Θεωρητικής Πληροφορικής απαριθμούν πλέον αρκετές χιλιάδες σελίδων κάθε χρόνο!

Ο σκοπός του μαθήματος *Θεωρητική Πληροφορική Ι* είναι η εισαγωγή των φοιτητριών και φοιτητών σε βασικές έννοιες της Θεωρητικής Πληροφορικής και ειδικότερα της θεωρίας των τυπικών γλωσσών και των πεπερασμένων αυτομάτων. Τα πεπερασμένα αυτόματα είναι τα απλούστερα μαθηματικά μοντέλα αλγορίθμων. Με τη βοήθεια των αυτομάτων, οι φοιτήτριες και φοιτητές θα κατανοήσουν την έννοια της μαθηματικής μοντελοποίησης των αλγορίθμων, του ελέγχου της ισοδυναμίας συγκεκριμένης κλάσης αλγορίθμων, καθώς και τα εργαλεία ελαχιστοποίησης αλγορίθμων. Θα πρέπει να σημειώσουμε εδώ ότι οι αποδείξεις στη Θεωρητική Πληροφορική είναι ως επί το πλείστον (*και ενδιαφέρει να είναι*) κατασκευαστικές, δηλαδή δεν ενδιαφέρει απλώς η απόδειξη ύπαρξης ενός αντικειμένου, αλλά και ο αλγόριθμος προσδιορισμού του.
Θα εισάγουμε διάφορα μοντέλα πεπερασμένων αυτομάτων, τα *πλήρη*, τα *deterministic* και τα *non-deterministic* και με τη βοήθεια της *θεωρίας σταθερού σημείου* θα δούμε πως μπορούμε να υπολογίσουμε τη γλώσσα που αναγνωρίζει ένα αυτόματο. Θα δείξουμε ότι και τα τρία μοντέλα, τα πλήρη, τα deterministic και τα non-determinitsic έχουν τη ίδια υπολογιστική ισχύ, δηλαδή αναγνωρίζουν την ίδια κλάση γλωσσών, αυτή *των αναγνωρίσιμων γλωσσών*. Θα μελετήσουμε τις ιδιότητες της κλάσης των αναγνωρίσιμων γλωσσών, θα δείξουμε ότι υπάρχουν γλώσσες που δεν είναι αναγνωρίσιμες και θα αποδείξουμε ένα κριτήριο μη-αναγνωρισιμότητας. Στη συνέχεια θα παρουσιάσουμε αλγόριθμους ελαχιστοποίησης των πεπερασμένων αυτομάτων δηλαδή αλγόριθμους με τους οποίους μπορούμε από ένα συγκεκριμένο αυτόματο να κατασκευάσουμε ένα *οικονομικότερο*, εφόσον αυτό υπάρχει, που όμως αναγνωρίζει την ίδια γλώσσα. Τέλος θα δώσουμε έναν αλγεβρικό χαρακτηρισμό της κλάσης των αναγνωρίσιμων γλωσσών αποδεικύοντας το *θέωρημα του Kleene*.

Η δομή των σημειώσεων αυτών είναι ως ακολούθως. Το Κεφάλαιο 1, περιέχει όλες τις στοιχειώδεις μαθηματικές έννοιες και αποτελέσματα που μας είναι χρήσι-

μα για την ανάπτυξη της θεωρίας μας.
Στο Κεφάλαιο 2 εισάγουμε την έννοια του αλφαβήτου και της τυπικής γλώσσας καθώς και τις πράξεις μεταξύ γλωσσών. Μελετάμε εξισώσεις και συστήματα εξισώσεων με συντελεστές τυπικές γλώσσες και αποδεικνύουμε την ύπαρξη ελαχίστων λύσεων.
Στο Κεφάλαιο 3 ασχολούμαστε με τα πλήρη πεπερασμένα αυτόματα, και δείχνουμε ότι η εύρεση *της γλώσσας* (ή *συμπεριφοράς*) ενός τέτοιου μοντέλου ανάγεται στη λύση ενός συστήματος εξισώσεων.
Το Κεφάλαιο 4 περιέχει τη μελέτη της κλάσης *των αναγνωρίσιμων γλωσσών* δηλαδή των γλωσσών που αναγνωρίζονται από τα πλήρη πεπερασμένα αυτόματα. Δείχνουμε ότι η κλάση αυτή είναι κλειστή με τις πράξεις της τομής, της ένωσης και του συμπληρώματος.
Στο Κεφάλαιο 5 εισάγουμε και μελετάμε τα deterministic και τα non-deterministic πεπερασμένα αυτόματα. Αν και γενικότερα μοντέλα από τα πλήρη, αποδεικνύουμε ότι δεν είναι ισχυρότερα, δηλαδή αναγνωρίζουν τις ίδιες ακριβώς γλώσσες που αναγνωρίζουν και τα πλήρη πεπερασμένα αυτόματα. Με τη βοήθεια των μοντέλων αυτών δείχνουμε περαιτέρω ιδιότητες της κλάσης των αναγνωρίσιμων γλωσσών.
Οι αλγόριθμοι ελαχιστοποίησης των πεπερασμένων αυτομάτων παρουσιάζονται στο Κεφάλαιο 6.
Τέλος, στο Κεφάλαιο 7, εισάγουμε την έννοια *των ρητών γλωσσών* και αποδεικνύουμε το *θεώρημα του Kleene* σύμφωνα με το οποίο αναγνωρίσιμες και ρητές γλώσσες, από το ίδιο αλφάβητο, ταυτίζονται.
Στο τέλος κάθε κεφαλαίου παρατίθενται ασκήσεις. Καλούμε τον αναγνώστη να ασχοληθεί με αυτές *μόνο όταν* έχει κατανοήσει σε βάθος τη προαναφερθείσα θεωρία.
Η Βιβλιογραφία, στο τέλος των σημειώσεων, περιέχει τις αναφορές των βιβλίων από την Εισαγωγή, καθώς και (ενδεικτικά κάποια από τα πιο) αξιόλογα βιβλία στο αντικείμενο της Θεωρίας Τυπικών Γλωσσών και Αυτομάτων.

Ευχαριστώ την κα Ειρήνη-Ελευθερία Mens, διδάκτορα του πανεπιστημίου της Grenoble, για τη σχεδίαση των σχημάτων στη πρώτη έκδοση των σημειώσεων αυτών.

Κεφάλαιο 1

Προκαταρκτικά

Στο κεφάλαιο αυτό αναφερόμαστε σε έννοιες και αποτελέσματα, χρήσιμα για την ανάπτυξη της θεωρίας μας.

1.1 Σύνολα και απεικονίσεις

Θα χρησιμοποιούμε την έννοια *σύνολο* με το συνήθη διαισθητικό ορισμό της συλλογής αντικειμένων. Για τα σύνολα θα χρησιμοπούμε τα κεφαλαία γράμματα της αγγλικής αλφαβήτου ενώ για τα στοιχεία τους τα πεζά. Έτσι αν A είναι σύνολο θα γράφουμε $a \in A$ (αντίστοιχα $a \notin A$) για να δηλώσουμε ότι το a ανήκει (αντίστοιχα δεν ανήκει) στο A. Αν κάθε στοιχείο του συνόλου A ανήκει και στο B, τότε λέμε ότι το A είναι *υποσύνολο* του B και το δηλώνουμε γράφοντας $A \subseteq B$. Αν συμβαίνει και $B \subseteq A$, τότε τα σύνολα A, B ονομάζονται ίσα και γράφουμε $A = B$. Το κενό σύνολο, δηλαδή το σύνολο που στερείται στοιχείων, θα συμβολίζεται με $\emptyset$, ενώ το σύνολο όλων των υποσυνόλων ενός συνόλου A, δηλαδή το *δυναμοσύνολο* του, με $\mathcal{P}(A)$.

Η *ένωση* $A \cup B$ δύο συνόλων A, B είναι το σύνολο όλων των στοιχείων του A και του B, δηλαδή

$$A \cup B = \{x \mid x \in A \text{ ή } x \in B\}$$

ενώ η *τομή* τους $A \cap B$ είναι το σύνολο των κοινών τους στοιχείων, δηλαδή

$$A \cap B = \{x \mid x \in A \text{ και } x \in B\}.$$

Αν $A \cap B = \emptyset$, τότε τα σύνολα A και B ονομάζονται *ξένα μεταξύ τους*. Είναι φανερό ότι $A \cup \emptyset = A$ και $A \cap \emptyset = \emptyset$ για οποιαδήποτε σύνολο A. Είναι επίσης εύκολο να δείξουμε ότι για οποιαδήποτε σύνολα A, B, C ισχύουν οι παρακάτω ιδιότητες:

- $A \cup (B \cup C) = (A \cup B) \cup C$,
- $A \cap (B \cap C) = (A \cap B) \cap C$,
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, και

- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Η *διαφορά* $A \setminus B$ του συνόλου B από το σύνολο A είναι το σύνολο

$$A \setminus B = \{x \mid x \in A \text{ και } x \notin B\}.$$

Το *συμπλήρωμα* $\overline{A}$ *του συνόλου* $A \subseteq X$ *ως προς το σύνολο* X είναι το σύνολο

$$\overline{A} = X \setminus A.$$

Το *καρτεσιανό γινόμενο* $A \times B$ *του* A *με το* B είναι το σύνολο

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

τα στοιχεία του οποίου ονομάζονται *διατεταγμένα ζεύγη*. Για κάθε $(a, b), (a', b') \in A \times B$ ορίζουμε ότι $(a, b) = (a', b')$ αν $a = a'$ και $b = b'$.
Όμοια το καρτεσιανό γινόμενο n συνόλων $A_1, \ldots, A_n$ είναι το σύνολο των διατεταγμένων n-άδων

$$A_1 \times \ldots \times A_n = \{(a_1, \ldots, a_n) \mid a_1 \in A_1, \ldots, a_n \in A_n\}.$$

Ας είναι I ένα σύνολο δεικτών, π.χ. το σύνολο των φυσικών αριθμών, ή το σύνολο των αρτίων φυσικών κλπ. Σε κάθε στοιχείο $i \in I$ αντιστοιχούμε ένα σύνολο A_i, και έτσι αποκτούμε μια *οικογένεια συνόλων με δείκτες από το* I, που θα τη συμβολίζουμε με $(A_i)_{i \in I}$.

Η οικογένεια $(A_i)_{i \in I}$ θα ονομάζεται *διαμέριση του συνόλου* A αν

- $\bigcup\limits_{i \in I} A_i = A$,
- $A_i \neq \emptyset$ για κάθε $i \in I$, και
- $i \neq j \implies A_i \cap A_j = \emptyset$ για κάθε $i, j \in I$.

Μια *απεικόνιση από το σύνολο* A *στο σύνολο* B

$$f : A \to B$$

είναι ένας κανόνας με τον οποίο σε κάθε στοιχείο $a \in A$ αντιστοιχίζεται ένα μοναδικό στοιχείο του B που συμβολίζεται με $f(a)$. Η απεικόνιση f ονομάζεται *ένεση* (ή *ένα προς ένα*, 1-1 για συντομία) αν για κάθε $a_1, a_2 \in A$ ισχύει $a_1 \neq a_2 \implies f(a_1) \neq f(a_2)$. Ονομάζεται *έφεση* (ή *επί*) αν για κάθε $b \in B$ υπάρχει $a \in A$ τέτοιο ώστε $f(a) = b$. Τέλος η f ονομάζεται *αμφίεση* (ή *αμφιμονοσήμαντη*, ή 1-1 *και επί*) αν είναι ένεση και έφεση. Η *εικόνα* ενός συνόλου $A' \subseteq A$ είναι το υποσύνολο του B

$$f(A') = \{f(a) \mid a \in A'\}$$

και η *αντίστροφη εικόνα* του $B' \subseteq B$ το υποσύνολο του A

$$f^{-1}(B') = \{a \mid a \in A \text{ και } f(a) \in B'\}.$$

Δύο απεικονίσεις $f, g : A \to B$ ονομάζονται *ίσες* και γράφουμε $f = g$ αν $f(a) = g(a)$ για κάθε $a \in A$. Το σύνολο όλων των απεικονίσεων από το A στο B συμβολίζεται με B^A.

Η *ταυτοτική απεικόνιση* $I_A : A \to A$ *του συνόλου* A ορίζεται από τη σχέση $I_A(a) = a$ για κάθε $a \in A$.

Ας είναι $f : A \to B$ και $g : B \to C$. Για κάθε $a \in A$ το $f(a) \in B$ και συνεπώς το $g(f(a)) \in C$. Με τον τρόπο αυτό ορίζεται μια νέα απεικόνιση από το A στο C που ονομάζεται *σύνθεση της* f *με τη* g και συμβολίζεται με $g \circ f$, δηλαδή

$$g \circ f : A \to C$$

με $g \circ f(a) = g(f(a))$ για κάθε $a \in A$. Από τον ορισμό της σύνθεσης απεικονίσεων προκύπτει εύκολα ότι αν $f : A \to B$, $g : B \to C$ και $h : C \to D$ είναι τρεις απεικονίσεις, τότε $h \circ (g \circ f) = (h \circ g) \circ f$, και ακόμη $f \circ I_A = f = I_B \circ f$.

1.2 Μονοειδή και ημιδακτύλιοι

Θεωρούμε ένα μη-κενό σύνολο K. Μια απεικόνιση

$$\triangle : K \times K \to K$$

ονομάζεται *(διμελής) πράξη στο σύνολο* K. Θα γράφουμε απλούστερα $k_1 \triangle k_2$ αντί για $\triangle((k_1, k_2))$ για κάθε $k_1, k_2 \in K$. Η πράξη $\triangle$ ονομάζεται

- *αντιμεταθετική* αν $k_1 \triangle k_2 = k_2 \triangle k_1$ για κάθε $k_1, k_2 \in K$,

- *προσεταιριστική* αν $k_1 \triangle (k_2 \triangle k_3) = (k_1 \triangle k_2) \triangle k_3$ για κάθε $k_1, k_2, k_3 \in K$.

Θα λέμε ότι η πράξη $\triangle$ έχει *ουδέτερο στοιχείο* αν υπάρχει $e \in K$ τέτοιο ώστε $k \triangle e = k = e \triangle k$ για κάθε $k \in K$. Είναι εύκολο να δείξουμε ότι αν μια πράξη έχει ουδέτερο στοιχείο, τότε αυτό είναι μοναδικό.

Σχόλιο 1 *Παρατηρήστε ότι η ίδια πράξη ορισμένη σε διαφορετικά σύνολα δεν έχει πάντα ουδέτερο στοιχείο. Για παράδειγμα ο πολλαπλασιασμός των πραγματικών αριθμών έχει ουδέτερο στοιχείο το* 1 *στο διάστημα* $[0, 1]$, *ενώ δεν έχει ουδέτερο στοιχείο, όπως εύκολα διαπιστώνεται, στο διάστημα* $[0, 1)$.

Τέλος, αν $\triangle, \triangledown : K \times K \to K$ είναι πράξεις στο K, θα λέμε ότι η $\triangledown$ *επιμερίζεται ως προς την* $\triangle$ αν

- $k_1 \triangledown (k_2 \triangle k_3) = (k_1 \triangledown k_2) \triangle (k_1 \triangledown k_3)$, και

- $(k_1 \vartriangle k_2) \triangledown k_3 = (k_1 \triangledown k_3) \vartriangle (k_2 \triangledown k_3)$

για κάθε $k_1, k_2, k_3 \in K$.

Ορισμός 1 *Ένα μονοειδές $(K, \vartriangle, e)$ είναι ένα σύνολο K εφοδιασμένο με μια προσεταιριστική πράξη $\vartriangle$ που έχει ουδέτερο στοιχείο e. Αν η πράξη $\vartriangle$ είναι και αντιμεταθετική τότε το μονοειδές $(K, \vartriangle, e)$ ονομάζεται αντιμεταθετικό.*

Παράδειγμα 1 *Οι παρακάτω τριάδες συνιστούν αντιμεταθετικά μονοειδή:*

- $(\mathbb{N}, +, 0)$ *όπου $\mathbb{N}$ είναι το σύνολο των φυσικών αριθμών,*

- $(\mathbb{N}, \cdot, 1)$ *όπου $\cdot$ παριστάνει τον πολλαπλασιασμό των φυσικών αριθμών,*

- $(\mathbb{Z}, +, 0)$ *όπου $\mathbb{Z}$ είναι το σύνολο των ακέραιων αριθμών,*

- $(\mathbb{Z}, \cdot, 1)$ *όπου $\cdot$ παριστάνει τον πολλαπλασιασμό των ακέραιων αριθμών,*

- $([0, 1], \max, 0)$ *όπου* $\max$, *είναι η πράξη που το αποτέλεσμα της είναι το μέγιστο δύο αριθμών,*

- $([0, 1], \min, 1)$ *όπου* $\min$, *είναι η πράξη που το αποτέλεσμά της είναι το ελάχιστο δύο αριθμών,*

- $(\mathcal{P}(A), \cap, A)$ *για οποιοδήποτε σύνολο A,*

- $(\mathcal{P}(A), \cup, \emptyset)$ *για οποιοδήποτε σύνολο A,*

ενώ η τριάδα $(A^A, \circ, I_A)$ όλων των απεικονίσεων από το σύνολο A στο σύνολο A με πράξη την σύνθεση, είναι μη-αντιμεταθετικό μονοειδές.

Σε ένα μονοειδές $(K, \vartriangle, e)$ μπορούμε να ορίσουμε τη *δύναμη* k^n κάθε στοιχείου $k \in K$ για κάθε φυσικό αριθμό $n \geq 0$, επαγωγικά ως εξής:

- $k^0 = e$,

- $k^{n+1} = k^n \vartriangle k \quad$ για κάθε $n \geq 0$.

Καθώς η πράξη $\vartriangle$ είναι προσεταιριστική, εύκολα αποδεικνύεται ότι $k^n \vartriangle k = k \vartriangle k^n$ για κάθε $n \geq 0$, και συνεπώς η παραπάνω δύναμη είναι καλά ορισμένη.
Ιδιαίτερα, για το μονοειδές $(A^A, \circ, I_A)$ θα συμβολίζουμε με $f^{(n)}$ την δύναμη f^n, για κάθε $n \geq 0$.

Αν $(K, \vartriangle, e)$ και $(K', \diamond, e')$ είναι μονοειδή, ένας *μορφισμός μονοειδών* είναι μια απεικόνιση $h : K \to K'$ τέτοια ώστε

- $h(k_1 \vartriangle k_2) = h(k_1) \diamond h(k_2) \qquad$ για κάθε $k_1, k_2 \in K$,

- $h(e) = e'$.

Στη συνέχεια θα ασχοληθούμε με ημιδακτύλιους. Θα πρέπει να αναφέρουμε εδώ, ότι οι δομές των μονοειδών και ημιδακτυλίων παρουσιάζουν ιδιαίτερο ενδιαφέρον στην Πληροφορική, καθώς τα θεωρητικά μοντέλα των περισσότερων πραγματικών εφαρμογών αναπτύσσονται στα πλαίσια αυτών των δομών.

Ορισμός 2 *Ένας ημιδακτύλιος είναι μία πεντάδα* $(K, \triangle, \triangledown, e, f)$ *όπου*

i) *το* $(K, \triangle, e)$ *είναι αντιμεταθετικό μονοειδές,*

ii) *το* $(K, \triangledown, f)$ *είναι μονοειδές,*

iii) *η πράξη* $\triangledown$ *επιμερίζεται ως προς την* $\triangle$, *και*

iv) $k \triangledown e = e \triangledown k = e$ *για κάθε* $k \in K$.

Ο ημιδακτύλιος $(K, \triangle, \triangledown, e, f)$ θα ονομάζεται *αντιμεταθετικός* αν το μονοειδές $(K, \triangledown, f)$ είναι αντιμεταθετικό.

Παράδειγμα 2 *Οι παρακάτω πεντάδες αποτελούν ημιδακτύλιους:*

i) $(\mathbb{N}, +, \cdot, 0, 1)$ *όπου* $\cdot$ *είναι ο πολλαπλασιασμός των φυσικών αριθμών,*

ii) $(\mathbb{Z}, +, \cdot, 0, 1)$ *όπου* $\cdot$ *είναι ο πολλαπλασιασμός των ακέραιων αριθμών,*

iii) $([0, 1], \max, \min, 0, 1)$,

iv) $([0, 1], \min, \max, 1, 0)$,

v) $(\mathcal{P}(A), \cup, \cap, \emptyset, A)$ *για οποιοδήποτε σύνολο* A,

vi) $(\mathcal{P}(A), \cap, \cup, A, \emptyset)$ *για οποιοδήποτε σύνολο* A,

vii) $\mathbb{R}_{\max} = (\mathbb{R}_+ \cup \{-\infty\}, \max, +, -\infty, 0)$ *όπου* $\mathbb{R}_+$ *είναι το σύνολο των μη-αρνητικών πραγματικών αριθμών,*

viii) $\mathbb{R}_{\min} = (\mathbb{R}_+ \cup \{\infty\}, \min, +, \infty, 0)$,

ix) $(\mathbb{N}^{n\times n}, +, \cdot, \mathbf{0}, I_n)$ *όπου* $\mathbb{N}^{n\times n}$ *είναι το σύνολο των* $n \times n$ *πινάκων με στοιχεία φυσικούς αριθμούς,* $+$ *και* $\cdot$ *είναι η πρόσθεση και ο πολλαπλασιασμός πινάκων αντίστοιχα,* $\mathbf{0}$ *είναι ο μηδενικός* $n \times n$ *πίνακας, και* I_n *είναι ο μοναδιαίος* $n \times n$ *πίνακας.*

Οι ημιδακτύλιοι των περιπτώσεων (i) έως (viii) είναι αντιμεταθετικοί, ενώ αυτός της περίπτωσης (ix) είναι μη-αντιμεταθετικός. Ο ημιδακτύλιος της περίπτωσης (iii) ονομάζεται fuzzy semiring (ασαφής ημιδακτύλιος) ενώ οι ημιδακτύλιοι των περιπτώσεων (vii) και (viii) ονομάζονται αντίστοιχα max-plus και min-plus. Και οι τρείς έχουν αξιοσημείωτες εφαρμογές.

Αν $(K, \triangle, \triangledown, e, f)$ και $(K', \diamond, \circ, e', f')$ είναι ημιδακτύλιοι, ένας *μορφισμός ημιδακτυλίων* είναι μια απεικόνιση

$$h : K \to K'$$

τέτοια ώστε

- $h(k_1 \triangle k_2) = h(k_1) \diamond h(k_2)$ για κάθε $k_1, k_2 \in K$,
- $h(k_1 \triangledown k_2) = h(k_1) \circ h(k_2)$ για κάθε $k_1, k_2 \in K$,
- $h(e) = e'$,
- $h(f) = f'$.

Η πρώτη και η τρίτη σχέση παραπάνω, σημαίνουν ότι ο h είναι μορφισμός των μονοειδών $(K, \triangle, e)$ και $(K', \diamond, e')$, ενώ η δεύτερη και η τέταρτη ότι ο h είναι και μορφισμός των μονοειδών $(K, \triangledown, f)$ και $(K', \circ, f')$.

Χάριν απλότητας, μερικές φορές, συμβολίζουμε την πρώτη πράξη ενός ημιδακτυκλίου με το $+$, την δεύτερη με το $\cdot$ και τα ουδέτερα στοιχεία αντίστοιχα με 0 και 1, δηλαδή γράφουμε $(K, +, \cdot, 0, 1)$.

1.3 Σχέσεις

Ας είναι A και B σύνολα. Κάθε υποσύνολο $R \subseteq A \times B$ ονομάζεται *σχέση από το A στο B*, ενώ αν $R \subseteq A \times A$ τότε η R ονομάζεται απλούστερα *σχέση στο A*. Αν $(a, b) \in R$, τότε θα γράφουμε και aRb.

Αν R είναι μία σχέση από το A στο B και S μία σχέση από το B στο C, τότε η *σύνθεσή τους* $R \circ S$ είναι μία σχέση από A στο C και ορίζεται ώς εξής

$$R \circ S = \{(a, c) \in A \times C \mid \text{ υπάρχει } b \in B \text{ τέτοιο ώστε } (a, b) \in R \text{ και } (b, c) \in S\}.$$

Για κάθε σύνολο A, η *διαγώνιος του A* είναι η σχέση $\Delta_A = \{(a, a) \mid a \in A\}$.

Μια σχέση R στο σύνολο A θα ονομάζεται

- *ανακλαστική* αν aRa για κάθε $a \in A$,
- *συμμετρική* αν $aRb \implies bRa$ για κάθε $a, b \in A$,
- *αντισυμμετρική* αν aRb και $bRA \implies a = b$ για κάθε $a, b \in A$,
- *μεταβατική* αν aRb και $bRc \implies aRc$ για κάθε $a, b, c \in A$.

Μια σχέση R στο σύνολο A ονομάζεται *σχέση ισοδυναμίας* αν είναι ανακλαστική, συμμετρική και μεταβατική. Συνήθως αντί για $(a, b) \in R$ γράφουμε $a \equiv b(R)$. Για κάθε $a \in A$ θα ονομάζουμε *κλάση ισοδυναμίας του a στην R* το σύνολο

$$[a]_R = \{b \mid b \in A \text{ και } a \equiv b(R)\}.$$

Το στοιχείο a ονομάζεται *αντιπρόσωπος της κλάσης* $[a]_R$. Το σύνολο των κλάσεων ισοδυναμίας της R ονομάζεται *σύνολο πηλίκο* και συμβολίζεται με A/R, δηλαδή

$$A/R = \{[a]_R \mid a \in A\}\,.$$

Η κλάση ισοδυναμίας $[a]_R$ θα συμβολίζεται απλούστερα και με $[a]$, όταν η R υπονοείται.

Λήμμα 1 *Θεωρούμε το σύνολο A και μια σχέση ισοδυναμίας R στο A. Για κάθε $a, b \in A$ ισχύει*

$$a \equiv b(R) \quad \text{αν-ν} \quad [a] = [b].$$

Απόδειξη Υποθέτουμε ότι $a \equiv b(R)$, και έστω $c \in [a]$. Τότε $a \equiv c(R)$, οπότε και $c \equiv b(R)$ που σημαίνει ότι $c \in [b]$. Έτσι $[a] \subseteq [b]$. Ο εγκλεισμός $[b] \subseteq [a]$ αποδεικνύεται ανάλογα, και συνεπώς $[a] = [b]$.
Αντίστροφα ας είναι $[a] = [b]$. Καθώς $a \in [a]$, θα είναι και $a \in [b]$, και συνεπώς $a \equiv b(R)$. □

Το παραπάνω λήμμα σημαίνει ότι οποιοδήποτε στοιχείο μιας κλάσης ισοδυναμίας αποτελεί έναν αντιπρόσωπό της.

Παράδειγμα 3 *Θεωρούμε το σύνολο $\mathbb{Z}$ των ακέραιων αριθμών, το θετικό ακέραιο m και τη σχέση R στο $\mathbb{Z}$, που ορίζεται ως εξής:*

$$aRb \quad \text{αν-ν} \quad m/a-b.$$

Είναι εύκολο να δείξουμε ότι η R είναι μια σχέση ισοδυναμίας, η οποία συμβολίζεται με $\mathrm{mod}\, m$. Έτσι θα γράφουμε

$$a \equiv b \bmod m \quad \text{αν-ν} \quad m/a-b$$

για κάθε $a, b \in \mathbb{Z}$. Θα υπολογίσουμε τώρα τη κλάση ισοδυναμίας $[a]$ οποιουδήποτε ακέραιου αριθμού a. Έχουμε

$$\begin{aligned}
[a] &= \{b \mid b \in \mathbb{Z} \ \text{ και } \ b \equiv a \bmod m\} \\
&= \{b \mid b \in \mathbb{Z} \ \text{ και } \ m/b-a\} \\
&= \{b \mid b \in \mathbb{Z} \ \text{ και } \ b-a = km \ \text{ με } \ k \in \mathbb{Z}\} \\
&= \{b \mid b \in \mathbb{Z} \ \text{ και } \ b = a+km \ \text{ με } \ k \in \mathbb{Z}\} \\
&= \{a+km \mid k \in \mathbb{Z}\}
\end{aligned}$$

δηλαδή η κλάση $[a]$ αποτελείται από όλους τους ακέραιους αριθμούς που προκύπτουν από τον a προσθέτοντας σε αυτόν οποιοδήποτε πολλαπλάσιο του m. Θα δείξουμε ότι το σύνολο πηλίκο $\mathbb{Z}/\bmod m$ περιέχει ακριβώς m στοιχεία. Συγκεκριμένα θα δείξουμε ότι

$$\mathbb{Z}/\bmod m = \{[0], \ldots, [m-1]\}.$$

Πράγματι, εύκολα αποδεικνύεται ότι οι κλάσεις του παραπάνω συνόλου είναι σύνολα ξένα ανά δύο μεταξύ τους (Άσκηση). Περαιτέρω, θεωρούμε οποιοδήποτε ακέραιο αριθμό $a \in \mathbb{Z}$*. Τότε υπάρχουν ακέραιοι* π *και* υ *με* $0 \leq \upsilon < m$*, έτσι ώστε* $a = \pi m + \upsilon$ *δηλαδή* $a - \upsilon = \pi m$*, και συνεπώς* $m/a - \upsilon$*. Άρα* $a \equiv \upsilon \bmod m$*, και σύμφωνα με το Λήμμα 1* $[a] = [\upsilon]$ *που σημαίνει ότι* $[a] \in \{[0], \ldots, [m-1]\}$*.*

Θα δείξουμε τώρα ότι οι διαμερίσεις ενός συνόλου συνδέονται άμεσα με τις σχέσεις ισοδυναμίας στο σύνολο αυτό. Συγκεκριμένα, θα αποδείξουμε την επόμενη πρόταση.

Πρόταση 1 *Αν* R *είναι μια σχέση ισοδυναμίας στο σύνολο* A*, τότε οι κλάσεις ισοδυναμίας των στοιχείων του* A *συνιστούν μια διαμέριση του* A*. Αντίστροφα, κάθε διαμέριση του* A *προέρχεται από μια σχέση ισοδυναμίας στο* A*.*

Απόδειξη Από τον ορισμό του A/R είναι φανερό ότι η ένωση των στοιχείων του είναι υποσύνολο του συνόλου A. Περαιτέρω, κάθε στοχείο a του A ανήκει στην κλάση ισοδυναμίας $[a]_R$ και συνεπώς $\bigcup_{a \in A} [a]_R = A$. Στη συνέχεια θα δείξουμε ότι για κάθε $[a]_R, [b]_R \in A/R$ ισχύει

$$[a]_R = [b]_R \quad \text{ή} \quad [a]_R \cap [b]_R = \emptyset.$$

Πράγματι ας υποθέσουμε ότι

$$[a]_R \cap [b]_R \neq \emptyset$$

και έστω $c \in [a]_R \cap [b]_R$. Αυτό σημαίνει ότι $c \in [a]_R$ και $c \in [b]_R$, δηλαδή $a \equiv c(R)$ και $b \equiv c(R)$ και συνεπώς $a \equiv b(R)$, καθώς η R είναι σχέση ισοδυναμίας στο A. Έτσι από το Λήμμα 1 συνάγουμε ότι $[a]_R = [b]_R$. Τέλος είναι φανερό ότι κάθε στοιχείο $[a]_R$ του A/R δεν είναι το κενό σύνολο καθώς περιέχει το a. Άρα τα στοιχεία του A/R συνιστούν μια διαμέριση του A.

Ας είναι τώρα $(A_i)_{i \in I}$ μια διαμέριση του συνόλου A. Ορίζουμε στο A τη σχέση R ως εξής:

$$(a, b) \in R \quad \text{αν-ν} \quad a, b \in A_i \ \text{ για κάποιο } \ i \in I.$$

Θα δείξουμε ότι η R είναι σχέση ισοδυναμίας. Πράγματι από τον τρόπο ορισμού της είναι προφανώς ανακλαστική και συμμετρική. Έστω τώρα ότι $(a, b) \in R$ και $(b, c) \in R$. Τότε υπάρχουν $i, j \in I$ έτσι ώστε $a, b \in A_i$ και $b, c \in A_j$. Έτσι το $b \in A_i \cap A_j$ που σημαίνει ότι $A_i \cap A_j \neq \emptyset$. Καθώς $(A_i)_{i \in I}$ είναι διαμέριση του A συνάγουμε ότι $A_i = A_j$. Άρα $a, c \in A_i$ και συνεπώς $(a, c) \in R$, δηλαδή η R είναι και μεταβατική, άρα σχέση ισοδυναμίας.
Θα δείξουμε τώρα ότι οι κλάσεις ισοδυναμίας της R ταυτίζονται με τα σύνολα της διαμέρισης $(A_i)_{i \in I}$. Πράγματι, ας είναι a στοιχείο του συνόλου A και $i \in I$ έτσι ώστε $a \in A_i$. Θεωρούμε ένα στοιχείο $b \in [a]_R$. Τότε $a \equiv b(R)$ και συνεπώς $b \in A_i$ που σημαίνει ότι $[a]_R \subseteq A_i$. Αντίστροφα αν $b \in A_i$ θα έχουμε $a \equiv b(R)$, δηλαδή $b \in [a]_R$, και συνεπώς $A_i \subseteq [a]_R$. Άρα $[a]_R = A_i$, και η απόδειξή μας τελείωσε. □

Πρόταση 2 *Η τομή δύο σχέσεων ισοδυναμίας στο σύνολο A είναι σχέση ισοδυναμίας στο σύνολο A.*

Απόδειξη Ας είναι R, S σχέσεις ισοδυναμίας στο A. Θα δείξουμε ότι και η $R \cap S$ είναι επίσης σχέση ισοδυναμίας στο A. Πράγματι για κάθε $a \in A$ έχουμε $a \equiv a(R)$ και $a \equiv a(S)$ δηλαδή $(a, a) \in R$ και $(a, a) \in S$ και συνεπώς $(a, a) \in R \cap S$. Άρα η $R \cap S$ είναι ανακλαστική. Έστω τώρα ότι $(a, b) \in R \cap S$. Τότε $(a, b) \in R$ και $(a, b) \in S$ και καθώς οι R και S είναι σχέσεις ισοδυναμίας, θα έχουμε $(b, a) \in R$ και $(b, a) \in S$ που σημαίνει ότι $(b, a) \in R \cap S$. Άρα η $R \cap S$ είναι και συμμετρική. Τέλος, έστω ότι $(a, b), (b, c) \in R \cap S$. Τότε $(a, b), (b, c) \in R$ και $(a, b), (b, c) \in S$, δηλαδή $(a, c) \in R$ και $(a, c) \in S$. Έτσι $(a, c) \in R \cap S$ που σημαίνει ότι η $R \cap S$ είναι και μεταβατική, και συνεπώς είναι σχέση ισοδυναμίας στο A. □

Σχόλιο 2 *Το αποτέλεσμα της Πρότασης 2 δεν ισχύει πάντοτε για τη πράξη της ένωσης, δηλαδή η ένωση δύο σχέσεων ισοδυναμίας δεν είναι πάντοτε σχέση ισοδυναμίας. Για παράδειγμα, στο σύνολο $\mathbb{Z}$ έχουμε $2 \equiv 4 \bmod 2$ και $4 \equiv 7 \bmod 3$. Αν η $\bmod 2 \cup \bmod 3$ ήταν σχέση ισοδυναμίας θα είχαμε, λόγω της μεταβατικής ιδιότητας, $2 \equiv 7 (\bmod 2 \cup \bmod 3)$, δηλαδή $2 \equiv 7 \bmod 2$ ή $2 \equiv 7 \bmod 3$, σχέσεις που προφανώς δεν ισχύουν.*

Στη συνέχεια ασχολούμαστε με σχέσεις μερικής διάταξης. Συγκεκριμένα, μια σχέση R στο σύνολο A ονομάζεται *σχέση μερικής διάταξης* (ή απλούστερα *μερική διάταξη*) αν είναι ανακλαστική, αντισυμμετρική και μεταβατική. Θα συμβολίζουμε στο εξής μια σχέση μερικής διάταξης R με το σύμβολο $\leq$, δηλαδή θα γράφουμε $a \leq b$ αν-ν aRb. Η διάταξη $\leq$ θα καλείται *ολική* αν $a \leq b$ ή $b \leq a$ για κάθε $a, b \in A$. Θα ονομάζουμε το ζεύγος $(A, \leq)$ *μερικά διατεγμένο σύνολο* (μ.δ.σ. για συντομία). Αν η $\leq$ είναι ολική διάταξη, τότε το $(A, \leq)$ ονομάζεται *ολικά διατεγμένο σύνολο*. Είναι φανερό πως κάθε ολικά διατεταγμένο σύνολο είναι και μερικά διατεταγμένο, αλλά το αντίθετο δεν ισχύει πάντα. Αν σε ένα μ.δ.σ. $(A, \leq)$ υπάρχει στοιχείο $\perp \in A$ τέτοιο ώστε $\perp \leq a$ για κάθε $a \in A$, τότε αυτό θα ονομάζεται *ελάχιστο στοιχείο του* $(A, \leq)$.

Παράδειγμα 4 *Τα παρακάτω ζεύγη είναι ολικά διατεταγμένα σύνολα.*

i) $(\mathbb{N}, \leq)$ *όπου $\leq$ είναι η διάταξη των φυσικών αριθμών. Το $(\mathbb{N}, \leq)$ έχει ελάχιστο στοιχείο το* 0.

ii) $(\mathbb{Z}, \leq)$ *όπου $\leq$ είναι η διάταξη των ακέραιων αριθμών. Το $(\mathbb{Z}, \leq)$ δεν έχει ελάχιστο στοιχείο.*

iii) $([0, 1], \leq)$ *όπου $\leq$ είναι η διάταξη των πραγματικών αριθμών. Το $([0, 1], \leq)$ έχει ελάχιστο στοιχείο το 0.*

iv) $((0, 1], \leq)$ *το οποίο δεν έχει ελάχιστο στοιχείο.*

Τα παρακάτω ζεύγη είναι μερικά διατεταγμένα σύνολα (αλλά όχι ολικά).

v) $(\mathbb{R}_+^{\mathbb{N}}, \leq)$ *το σύνολο όλων των ακολουθιών μη-αρνητικών πραγματικών αριθμών, όπου η* $\leq$ *ορίζεται ως ακολούθως. Για κάθε* $f_1, f_2 \in \mathbb{R}_+^{\mathbb{N}}$ *θα έχουμε* $f_1 \leq f_2$ *αν-ν* $f_1(n) \leq f_2(n)$ *για κάθε* $n \in \mathbb{N}$. *Το* $(\mathbb{R}_+^{\mathbb{N}}, \leq)$ *έχει ελάχιστο στοιχείο τη μηδενική ακολουθία.*

vi) $(\mathcal{P}(A), \subseteq)$ *όπου* A *είναι οποιοδήποτε μη-κενό σύνολο και* $\subseteq$ *είναι η σχέση υποσυνόλου. Το ελάχιστο στοιχείο του είναι το* $\emptyset$.

Αν $(A, \leq)$ είναι μ.δ.σ. και $B \subseteq A$, τότε ονομάζουμε *supremum* του B και συμβολίζουμε με $\sup B$ το στοιχείο του A με τις εξής ιδιότητες:

- $b \leq \sup B$ για κάθε $b \in B$,

- αν $b' \in A$ και $b \leq b'$ για κάθε $b \in B$, τότε $\sup B \leq b'$.

Το $\sup B$ δεν υπάρχει πάντα για οποιοδήποτε υποσύνολο B ενός μ.δ.σ. $(A, \leq)$. Για παράδειγμα το *supremum* οποιασδήποτε γνήσια αύξουσας ακολουθίας του μ.δ.σ. $([0, 1), \leq)$ *δεν υπάρχει* στο διάστημα $[0, 1)$.

Αν $(a_n)_{n\geq 0}$ είναι ακολουθία στοιχείων του μ.δ.σ. $(A, \leq)$, τότε θα συμβολίζουμε το *supremum* του συνόλου $\{a_n \mid n \geq 0\}$ (αν υπάρχει) με $\sup_{n\geq 0} a_n$.

Ορισμός 3 *Ένα μ.δ.σ.* $(A, \leq)$ *ονομάζεται ω-πλήρες αν έχει ελάχιστο στοιχείο* $\perp$, *και για κάθε αύξουσα ακολουθία* $a_0 \leq a_1 \leq a_2 \ldots$ *στοιχείων του* A *το* $\sup_{n\geq 0} a_n$ *υπάρχει και ανήκει στο* A.

Παράδειγμα 5 *Τα παρακάτω μ.δ.σ. είναι ω-πλήρη:*

- $([0, 1], \leq)$,

- $(\mathbb{N} \cup \{\infty\}, \leq)$,

- $(\mathcal{P}(A), \subseteq)$ *με ελάχιστο στοιχείο το* $\emptyset$ *για οποιοδήποτε σύνολο* A.

Ας είναι $(A, \leq)$ ένα μ.δ.σ. και $f : A \to A$ μια απεικόνιση. Ένα στοιχείο $a \in A$ ονομάζεται *σταθερό σημείο της* f αν $f(a) = a$. Το $a \in A$ ονομάζεται *ελάχιστο σταθερό σημείο της* f, και συμβολίζεται με $\text{fix}f$, αν $a \leq a'$ για κάθε σταθερό σημείο a' της f.

Αν το μ.δ.σ. $(A, \leq)$ είναι ω-πλήρες και για κάθε αύξουσα ακολουθία $a_0 \leq a_1 \leq a_2 \ldots$ στοιχείων του A ισχύει $f\left(\sup_{n\geq 0} a_n\right) = \sup_{n\geq 0} f(a_n)$, τότε η f ονομάζεται *ω-συνεχής*.

Λήμμα 2 *Αν η* $f : A \to A$ *είναι ω-συνεχής, τότε είναι μονότονη δηλαδή* $a \leq a' \implies f(a) \leq f(a')$ *για κάθε* $a, a' \in A$.

Απόδειξη Για κάθε $a, a' \in A$, αν $a \leq a'$, τότε $a' = \sup\{a, a'\}$ και καθώς η f είναι ω-συνεχής θα έχουμε $f(a') = f(\sup\{a, a'\}) = \sup\{f(a), f(a')\}$ που σημαίνει ότι $f(a) \leq f(a')$ και συνεπώς η f είναι μονότονη. □

Το ακόλουθο σημαντικό αποτέλεσμα της καθολικής άλγεβρας είναι γνωστό σαν *Θεώρημα σταθερού σημείου του Tarski*.

Θεώρημα 1 *(Tarski) Ας είναι $(A, \leq)$ ω-πλήρες μ.δ.σ. και $f : A \to A$ ω-συνεχής απεικόνιση. Τότε το ελάχιστο σταθερό σημείο της f υπάρχει και* $\mathrm{fix} f = \sup_{n\geq 0} f^{(n)}(\bot)$.

Απόδειξη Καταρχήν θα δείξουμε ότι η ακολουθία $\left(f^{(n)}(\bot)\right)_{n\geq 0}$ είναι αύξουσα, δηλαδή $f^{(n)}(\bot) \leq f^{(n+1)}(\bot)$ για κάθε $n \geq 0$. Χρησιμοποιούμε επαγωγή στο n. Καθώς το $\bot$ είναι το ελάχιστο στοιχείο του μ.δ.σ. $(A, \leq)$, θα έχουμε $f^{(0)}(\bot) = \bot \leq f(\bot) = f^{(1)}(\bot)$. Υποθέτουμε ότι $f^{(n)}(\bot) \leq f^{(n+1)}(\bot)$ και επειδή η f είναι μονότονη, λόγω του Λήμματος 2, θα έχουμε $f(f^{(n)}(\bot)) \leq f(f^{(n+1)}(\bot))$ δηλαδή $f^{(n+1)}(\bot) \leq f^{(n+2)}(\bot)$, όπως το θέλαμε. Έτσι, καθώς το μ.δ.σ. $(A, \leq)$ είναι ω-πλήρες, το $\sup_{n\geq 0} f^{(n)}(\bot)$ υπάρχει. Θα δείξουμε ότι είναι σταθερό σημείο της f. Πράγματι έχουμε

$$\begin{aligned} f\left(\sup_{n\geq 0} f^{(n)}(\bot)\right) &= \sup_{n\geq 0} f\left(f^{(n)}(\bot)\right) \\ &= \sup_{n\geq 0} f^{(n+1)}(\bot) \\ &= \sup_{n\geq 0} f^{(n)}(\bot) \end{aligned}$$

όπου η πρώτη ισότητα ισχύει διότι η f είναι ω-συνεχής, και η τρίτη καθώς οι ακολουθίες στοιχείων $(f^n(\bot))_{n\geq 0}$ και $(f^n(\bot))_{n\geq 1}$ του A είναι αύξουσες και διαφέρουν μόνο ως προς τον πρώτο τους όρο.

Απομένει λοιπόν να δείξουμε ότι το $\sup_{n\geq 0} f^{(n)}(\bot)$ είναι το ελάχιστο από όλα τα σταθερά σημεία της f. Ας είναι λοιπόν $a \in A$ σταθερό σημείο της f. Τότε από την $\bot \leq a$ παίρνουμε $f(\bot) \leq f(a) = a$, και επαγωγικά $f^{(n)}(\bot) \leq a$ για κάθε $n \geq 0$, οπότε $\sup_{n\geq 0} f^{(n)}(\bot) \leq a$, και η απόδειξή μας τελείωσε. □

Ασκήσεις

1) Δίνονται τα σύνολα $A, B \subseteq X$. Να δείξετε ότι ισχύουν οι σχέσεις:

   - $\overline{\overline{A}} = A$,
   - $\overline{A \cup B} = \overline{A} \cap \overline{B}$,
   - $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

2) Δίνονται τα σύνολα A, B, C. Να δείξετε ότι ισχύουν οι σχέσεις:

- $A \times \emptyset = \emptyset \times A = \emptyset$,
- $A \times (B \cup C) = (A \times B) \cup (A \times C)$,
- $A \times (B \cap C) = (A \times B) \cap (A \times C)$,
- $B \subseteq C \implies (A \times B) \subseteq (A \times C)$.

3) Να δείξετε ότι αν μια πράξη έχει ουδέτερο στοιχείο, τότε αυτό είναι μοναδικό.

4) Δίνονται οι απεικονίσεις $f : A \to B$ και $g : B \to C$. Να αποδείξετε ότι αν

i) οι f, g είναι 1-1, τότε και η $g \circ f$ είναι 1-1,

ii) οι f, g είναι επί, τότε και η $g \circ f$ είναι επί,

iii) οι f, g είναι αμφιμονοσήμαντες, τότε και η $g \circ f$ είναι αμφιμονοσήμαντη.

5) Δίνονται οι απεικονίσεις $f : A \to B$ και $g : B \to C$. Να αποδείξετε ότι αν

i) η $g \circ f$ είναι 1-1, τότε η f είναι 1-1,

ii) η $g \circ f$ είναι επί, τότε η g είναι επί,

iii) η $g \circ f$ είναι αμφιμονοσήμαντη, τότε η f είναι 1-1 και η g είναι επί.

6) Δίνεται η απεικόνιση $f : A \to B$. Για οποιαδήποτε σύνολα $A_1, A_2 \subseteq A$ και $B_1, B_2 \subseteq B$ να αποδείξετε τις παρακάτω προτάσεις:

i) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$,

ii) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$,

iii) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$, και

iv) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$.

Να αποδείξετε επίσης ότι δεν ισχύει πάντα ο αντίστροφος εγκλεισμός της πρότασης (*iv*).

(7) Να εξετάσετε αν

i) το σύνολο $\mathbb{N}$ των φυσικών αριθμών με την πράξη max μπορεί να δομηθεί σε μονοειδές,

ii) το σύνολο $\mathbb{N}$ των φυσικών αριθμών με την πράξη min μπορεί να δομηθεί σε μονοειδές, *iii*) το σύνολο $\mathbb{Z}$ των ακεραίων αριθμών με την πράξη max μπορεί να δομηθεί σε μονοειδές,

iv) το σύνολο $\mathbb{Z}$ των ακεραίων αριθμών με την πράξη min μπορεί να δομηθεί σε μονοειδές.

8) Να αποδείξετε τις προτάσεις (*iii*)-(*viii*) του Παραδείγματος 2.

9) Δίνεται μη-κενό σύνολο A. Να αποδείξετε ότι η πεντάδα $(\mathcal{P}(A\times A), \cup, \circ, \emptyset, \Delta_A)$ είναι ημιδακτύλιος.

10) Να εξετάσετε αν ο ημιδακτύλιος της προηγούμενης άσκησης είναι αντιμεταθετικός.

11) Στο σύνολο $\mathbb{Z} \setminus \{0\}$ ορίζουμε τη σχέση

$$R = \{(a, b) \mid a, b \in \mathbb{Z} \setminus \{0\} \text{ και } ab > 0\}.$$

Να δείξετε ότι η R είναι σχέση ισοδυναμίας και να βρείτε τις κλάσεις της.

12) Δίνονται σύνολα A και B και μια απεικόνιση $f : A \to B$. Στο σύνολο A θεωρούμε τη σχέση R ως εξής:

$$aRb \quad \text{αν-ν} \quad f(a) = f(b)$$

για κάθε $a, b \in A$.
Να εξετάσετε αν η σχέση R είναι σχέση ισοδυναμίας, και στην περίπτωση που είναι, να βρείτε το πλήθος των κλάσεων ισοδυναμίας.

13) Να βρείτε το πλήθος των σχέσεων ισοδυναμίας που μπορούν να ορισθούν στο σύνολο $A = \{1, 2, 3\}$. (Υπόδειξη: Βρείτε όλες τις διαμερίσεις του συνόλου A και χρησιμοποιείστε την Πρόταση 1).

14) Να βρείτε το πλήθος των σχέσεων ισοδυναμίας που μπορούν να ορισθούν στο σύνολο $A = \{1, 2, 3, 4\}$.

15) Δίνεται σύνολο A και σχέσεις ισοδυναμίας $R_1, \ldots, R_n$ στο A. Να εξετάσετε αν η τομή $R_1 \cap \ldots \cap R_n$ είναι σχέση ισοδυναμίας στο A.

16) Να εξετάσετε αν το συμπλήρωμα μιας σχέσης ισοδυναμίας σε ένα σύνολο A, είναι σχέση ισοδυναμίας στο A.

17) Δίνεται σύνολο A και σχέσεις ισοδυναμίας R, S στο A. Να βρείτε την ελάχιστη σχέση ισοδυναμίας στο A που περιέχει τη σχέση $R \cup S$.

18) Να αποδείξετε την πρόταση του Παραδείγματος 5.

19) Δίνονται τα μερικά διατεταγμένα σύνολα $(A, \leq_A)$ και $(B, \leq_B)$. Στο καρτεσιανό γινόμενο $A \times B$ ορίζουμε τη σχέση $\leq$ ως εξής:

$$(a, b) \leq (a', b') \qquad \text{αν-ν} \qquad ((a \leq_A a' \text{ και } a \neq a') \text{ ή } (a = a' \text{ και } b \leq_B b'))$$

για κάθε $(a, b), (a', b') \in A \times B$.

Να εξετάσετε αν το ζεύγος $(A \times B, \leq)$ είναι μερικά διατεταγμένο σύνολο.

20) Δίνονται τα ολικά διατεταγμένα σύνολα $(A, \leq_A)$ και $(B, \leq_B)$. Στο καρτεσιανό γινόμενο $A \times B$ ορίζουμε τη σχέση $\leq$ ως εξής:

$$(a, b) \leq (a', b') \qquad \text{αν-ν} \qquad ((a \leq_A a' \text{ και } a \neq a') \text{ ή } (a = a' \text{ και } b \leq_B b'))$$

για κάθε $(a, b), (a', b') \in A \times B$.

Να εξετάσετε αν το ζεύγος $(A \times B, \leq)$ είναι ολικά διατεταγμένο σύνολο.

21) Δίνονται τα μερικά διατεταγμένα σύνολα $(A, \leq_A)$, $(B, \leq_B)$ και $(C, \leq_C)$. Στο καρτεσιανό γινόμενο $A \times B \times C$ ορίζουμε τη σχέση $\leq$ ως εξής:

$$(a, b, c) \leq (a', b', c) \quad \text{αν-ν} \quad \left(\begin{array}{c} (a \leq_A a' \text{ και } a \neq a') \\ \text{ή} \\ (a = a' \text{ και } b \leq_B b' \text{ και } b \neq b') \\ \text{ή} \\ (a = a' \text{ και } b = b' \text{ και } c \leq_C c') \end{array} \right)$$

για κάθε $(a, b, c), (a', b', c') \in A \times B \times C$.

Να εξετάσετε αν το ζεύγος $(A \times B \times C, \leq)$ είναι μερικά διατεταγμένο σύνολο.

22) Δίνονται τα ολικά διατεταγμένα σύνολα $(A, \leq_A)$, $(B, \leq_B)$ και $(C, \leq_C)$. Στο καρτεσιανό γινόμενο $A \times B \times C$ ορίζουμε τη σχέση $\leq$ ως εξής:

$$(a,b,c) \leq (a',b',c) \quad \text{αν-ν} \quad \left(\begin{array}{c} (a \leq_A a' \text{ και } a \neq a') \\ \text{ή} \\ (a = a' \text{ και } b \leq_B b' \text{ και } b \neq b') \\ \text{ή} \\ (a = a' \text{ και } b = b' \text{ και } c \leq_C c') \end{array} \right)$$

για κάθε $(a,b,c),(a',b',c') \in A \times B \times C$.

Να εξετάσετε αν το ζεύγος $(A \times B \times C, \leq)$ είναι ολικά διατεταγμένο σύνολο.

23) Δίνεται μη-κενό σύνολο A και έστω $\mathcal{D}$ το σύνολο όλων των διαμερίσεων του A. Στο $\mathcal{D}$ ορίζουμε μια σχέση $\mathcal{R}$ ως εξής:

$$\Delta \mathcal{R} \Delta' \quad \text{αν-ν} \quad \text{για κάθε } A_i \in \Delta \text{ υπάρχει } A'_j \in \Delta' \text{ έτσι ώστε } A_i \subseteq A'_j$$

για κάθε $\Delta = (A_i)_{i \in I}, \Delta' = \left(A'_j\right)_{j \in J} \in \mathcal{D}$.

Να δείξετε ότι η $\mathcal{R}$ είναι σχέση μερικής διάταξης στο σύνολο $\mathcal{D}$.

24) Δίνεται μη-κενό σύνολο A και έστω $\mathcal{E}$ το σύνολο όλων των σχέσων ισοδυναμίας στο A. Στο $\mathcal{E}$ ορίζουμε μια σχέση $\mathcal{R}$ ως εξής:

$$S \mathcal{R} S' \quad \text{αν-ν} \quad \text{για κάθε } [a]_S \in A/S \text{ υπάρχει } [b]_{S'} \in A/S' \text{ έτσι ώστε } [a]_S \subseteq [b]_{S'}$$

για κάθε $S, S' \in \mathcal{E}$.

Να δείξετε ότι η $\mathcal{R}$ είναι σχέση μερικής διάταξης στο σύνολο $\mathcal{E}$.

25) Δίνεται μονοειδές $(K, \triangle, e)$ και σχέση ισοδυναμίας R στο K τέτοια ώστε για κάθε $k_1, k_2, k'_1, k'_2 \in K$

$$k_1 \equiv k'_1(R) \text{ και } k_2 \equiv k'_2(R) \implies k_1 \triangle k_2 \equiv k'_1 \triangle k'_2(R).$$

Για κάθε $k, k' \in K$ ορίζουμε

$$[k]_R \tilde{\triangle} [k']_R = [k \triangle k']_R.$$

Να δείξετε ότι

i) η $\tilde{\triangle}$ είναι πράξη στο K/R,

ii) το $(K/R, \tilde{\triangle}, [e])$ είναι μονοειδές,

iii) η απεικόνιση $h : K \to K/R$, που ορίζεται από την $h(k) = [k]_R$ για κάθε $k \in K$, είναι μορφισμός μονοειδών.

Κεφάλαιο 2

Τυπικές γλώσσες

Θα ονομάζουμε *αλφάβητο* ένα πεπερασμένο σύνολο A και τα στοιχεία του *γράμματα*. Κάθε πεπερασμένη ακολουθία $(a_1, \ldots, a_n)$ στοιχείων του A θα ονομάζεται *λέξη* (ή *συμβολοσειρά*) από το αλφάβητο A και θα συμβολίζεται απλούστερα $a_1 \ldots a_n$. Για λόγους πληρότητας της θεωρίας μας θα θεωρήσουμε και μία λέξη που δεν έχει καθόλου γράμματα. Θα τη συμβολίζουμε με ε και θα τη καλούμε *κενή λέξη*.

Παράδειγμα 6 *Θεωρούμε το αλφάβητο της αγγλικής γλώσσας $A_{EN} = \{a, b, \ldots, z\}$. Φανερά κάθε αγγλική λέξη είναι λέξη σύμφωνα με τον ορισμό που δώσαμε προηγουμένως. 'Ομοια οι babb, zzzzzz, cfg είναι λέξεις με την έννοια που ορίσαμε παραπάνω. Εντούτοις δεν αποτελούν λέξεις της αγγλικής γλώσσας. Το ίδιο συμβαίνει με το αλφάβητο οποιασδήποτε φυσικής γλώσσας. Η έννοια της λέξης δηλαδή στη μαθηματική γλωσσολογία είναι γενικότερη από αυτή της λέξης στις φυσικές μας γλώσσες.*

Το σύνολο όλων των λέξεων από το αλφάβητο A θα συμβολίζεται με A^*, δηλαδή

$$A^* = \{\varepsilon\} \cup \{a_1 \ldots a_n \mid n > 0, a_1, \ldots, a_n \in A\}$$

και το σύνολο όλων των λέξεων από το αλφάβητο A χωρίς την κενή λέξη θα συμβολίζεται με A^+, δηλαδή

$$A^+ = A^* \setminus \{\varepsilon\}.$$

Παράδειγμα 7 *Θεωρούμε το αλφάβητο $A = \{0, 1, \ldots, 9\}$. Τότε οι λέξεις του A^* παριστάνουν όλους τους φυσικούς αριθμούς εκφρασμένους στο δεκαδικό σύστημα αρίθμησης. 'Ομοια αν $A = \{0, 1\}$, τότε οι λέξεις του A^* παριστάνουν όλους τους φυσικούς αριθμούς εκφρασμένους στο δυαδικό σύστημα αρίθμησης.*

Δύο λέξεις $w = a_1 \ldots a_n, u = b_1 \ldots b_m$ από το A, με $a_1, \ldots, a_n, b_1, \ldots, b_m \in A$ θα ονομάζονται *ίσες*, και θα γράφουμε $w = u$, αν $n = m$ και $a_i = b_i$ για κάθε $1 \leq i \leq n$.

Στο σύνολο A^* ορίζουμε την πράξη της παράθεσης ως εξής: Αν $w = a_1 \dots a_n$, $u = b_1 \dots b_m \in A^*$ η *παράθεση της* w *με τη* u είναι η λέξη $wu = a_1 \dots a_n b_1 \dots b_m$. Είναι εύκολο να δείξουμε ότι η παράθεση είναι πράξη προσεταιριστική, δηλαδή, για κάθε $w, u, v \in A^*$ ισχύει $w(uv) = (wu)v$ και ότι $w\varepsilon = w = \varepsilon w$ για κάθε $w \in A^*$. Συνεπώς το σύνολο A^* με τη πράξη της παράθεσης και ουδέτερο στοιχείο την κενή λέξη αποτελεί ένα *μονοειδές*.[1] Να σημειώσουμε ότι αν $card(A) > 1$ τότε η παράθεση *δεν* είναι αντιμεταθετική πράξη.

Για κάθε λέξη $w \in A^*$ και $n \geq 0$ ορίζουμε τη *n-οστή δύναμη* w^n της w επαγωγικά ως εξής:

- $w^0 = \varepsilon$,
- $w^{n+1} = w^n w \quad$ για κάθε $n \geq 0$.

Τότε για κάθε $w \in A^*$ και $n, m \geq 0$ έχουμε (μπορείτε να το αποδείξετε με επαγωγή στο m)

$$w^n w^m = w^{n+m} \text{ και } (w^n)^m = w^{nm}.$$

Η *αντίστροφη* (ή *είδωλο*) *μιας λέξης* $w = a_1 \dots a_n \in A^*$ είναι η λέξη $w^\rho = a_n \dots a_1$. Είναι εύκολο να δείξουμε ότι $(wu)^\rho = u^\rho w^\rho$ για κάθε $w, u \in A^*$

Τέλος το *μήκος* $|w|$ μιας λέξης w είναι το πλήθος των γραμμάτων της, δηλαδή αν $w = a_1 \dots a_n \in A^*$ τότε $|w| = n$. Φανερά $|wu| = |w| + |u|$ για κάθε $w, u \in A^*$ ενώ $|\varepsilon| = 0$. Με άλλα λόγια η απεικόνιση που αντιστοιχίζει κάθε λέξη στο μήκος της είναι ένας μορφισμός του μονοειδούς A^* στο μονοειδές των φυσικών αριθμών $(\mathbb{N}, +, 0)$.

Κάθε σύνολο $L \subseteq A^*$ ονομάζεται *τυπική γλώσσα* (ή απλούστερα *γλώσσα*) *από το αλφάβητο* A. Για παράδειγμα αν $A = \{a, b, c\}$, τότε τα σύνολα $\{a, bac^{10}, bca(ac)^{30}b\}$, $\{a^n \mid n \geq 0\}$, $\{a^n b^n \mid n \geq 0\}$, $\{a^n b^m \mid n, m \geq 0\}$ αποτελούν γλώσσες από το αλφάβητο A.

Η πράξη της παράθεσης επεκτείνεται σε γλώσσες ως εξής: αν $L_1, L_2 \subseteq A^*$ τότε η *παράθεση της* L_1 *με την* L_2 είναι η γλώσσα

$$L_1 L_2 = \{w_1 w_2 \mid w_1 \in L_1, w_2 \in L_2\}.$$

Για παράδειγμα αν $A = \{a, b, c\}$, $L_1 = \{ab^2, c^{10}, bca\}$ και $L_2 = \{b^2, ac^3, \varepsilon\}$ τότε

$$L_1 L_2 = \{ab^4, ab^2ac^3, ab^2, c^{10}b^2, c^{10}ac^3, c^{10}, bcab^2, bca^2c^3, bca\}.$$

Η παράθεση γλωσσών είναι προσεταιριστική, έχει ουδέτερο στοιχείο τη γλώσσα $\{\varepsilon\}$ και επιμερίζεται ως προς την ένωση, δηλαδή

- $L_1 (L_2 L_3) = (L_1 L_2) L_3 \quad (1)$
- $L_1\{\varepsilon\} = L_1 = \{\varepsilon\}L_1 \quad (2)$

[1] Ακριβέστερα αποτελεί το *ελεύθερο μονοειδές που παράγεται από το πεπερασμένο σύνολο* A (βλ. Άσκηση 12).

- $L_1(L_2 \cup L_3) = L_1L_2 \cup L_1L_3$ και $(L_1 \cup L_2)L_3 = L_1L_3 \cup L_2L_3$ (3)

για κάθε $L_1, L_2, L_3 \subseteq A^*$.
Ας αποδείξουμε τη δεύτερη από τις σχέσεις (3). Για κάθε $w \in A^*$ ισχύει

$$
\begin{aligned}
w \in (L_1 \cup L_2)L_3 &\implies w = uv \text{ με } u \in L_1 \cup L_2 \text{ και } v \in L_3 \\
&\implies w = uv \text{ με } (u \in L_1 \text{ ή } u \in L_2) \text{ και } v \in L_3 \\
&\implies w = uv \text{ με } uv \in L_1L_3 \text{ ή } uv \in L_2L_3 \\
&\implies w \in L_1L_3 \text{ ή } w \in L_2L_3 \\
&\implies w \in L_1L_3 \cup L_2L_3.
\end{aligned}
$$

Άρα $(L_1 \cup L_2)L_3 \subseteq L_1L_3 \cup L_2L_3$. Αντίστροφα, αν $w \in L_1L_3$, τότε $w = uv$ με $u \in L_1$ και $v \in L_3$. Καθώς όμως $L_1 \subseteq L_1 \cup L_2$ παίρνουμε ότι $w = uv \in (L_1 \cup L_2)L_3$ και συνεπώς $L_1L_3 \subseteq (L_1 \cup L_2)L_3$. Όμοια δείχνουμε ότι $L_2L_3 \subseteq (L_1 \cup L_2)L_3$ οπότε και $L_1L_3 \cup L_2L_3 \subseteq (L_1 \cup L_2)L_3$.

Από τον ορισμό της παράθεσης γλωσσών προκύπτει ότι

- $L\emptyset = \emptyset = \emptyset L$ (4).

για κάθε $L \subseteq A^*$.

Το $(\mathcal{P}(A^*), \cup, \emptyset)$ είναι αντιμεταθετικό μονοειδές και λόγω των (1) και (2) το $\mathcal{P}(A^*)$ είναι μονοειδές με τη πράξη της παράθεσης και ουδέτερο στοιχείο τη γλώσσα $\{\varepsilon\}$. Λαμβάνοντας υπόψη και τις (3), (4) συνάγουμε ότι το $\mathcal{P}(A^*)$ είναι *ημιδακτύλιος με τις πράξεις της ένωσης και της παράθεσης*.

Καθώς η παράθεση γλωσσών είναι προσεταιριστική, μπορούμε να ορίσουμε για κάθε γλώσσα $L \subseteq A^*$ και κάθε $n \geq 0$ τη *n-δύναμη* ή (*n-επανάληψη*) L^n της γλώσσας L ως εξής:

- $L^0 = \{\varepsilon\}$,

- $L^{n+1} = L^nL$ για κάθε $n \geq 0$.

Περαιτέρω η *θήκη L^* της γλώσσας L* ορίζεται ως εξής:

$$
\begin{aligned}
L^* &= \bigcup_{n \geq 0} L^n \\
&= \{\varepsilon\} \cup L \cup L^2 \cup L^3 \cup \ldots.
\end{aligned}
$$

Για παράδειγμα αν $L = \{a\}$ με $a \in A$, τότε $\{a\}^* = \{a^n \mid n \geq 0\}$.

Στη συνέχεια για κάθε γράμμα $a \in A$ θα συμβολίζουμε το μονοσύνολο $\{a\}$ απλούστερα με a. Με αυτή τη σύμβαση, το μονοσύνολο $\{w\}$ με $w = a_1 \ldots a_n$ όπου $a_1, \ldots, a_n \in A$ θα συμβολίζεται με w αφού $\{w\} = \{a_1\} \ldots \{a_n\}$. Όμοια θα γράφουμε $w \cup u$ για το σύνολο $\{w, u\}$, και $(w^3u^{10}c \cup bac^9b^3)^*$ για το σύνολο $\{w^3u^{10}c, bac^9b^3\}^*$, κλπ.

Επόμενο καθήκον μας είναι η επίλυση γραμμικών εξισώσεων (και συστημάτων γραμμικών εξισώσεων) στο σύνολο $\mathcal{P}(A^*)$. Συγκεκριμένα θα αναζητήσουμε τις λύσεις εξισώσεων (ως προς X) της μορφής $X = LX \cup M$ όπου $L, M \subseteq A^*$. Μία γλώσσα F ονομάζεται *λύση* της εν λόγω εξίσωσης αν $F = LF \cup M$. Η λύση F θα ονομάζεται *ελάχιστη* αν ισχύει $F \subseteq F'$ για οποιαδήποτε λύση της εξίσωσης. Θα αποδείξουμε ότι η εν λόγω εξίσωση έχει ελάχιστη λύση. Για αυτό θα μας χρειαστεί το επόμενο αποτέλεσμα.

Λήμμα 3 *Ας είναι $L_1, L_2, M_1, M_2 \subseteq A^*$ γλώσσες. Αν $L_1 \subseteq M_1$ και $L_2 \subseteq M_2$, τότε $L_1L_2 \subseteq M_1M_2$.*

Απόδειξη Έστω $w \in L_1L_2$. Τότε $w = w_1w_2$ με $w_1 \in L_1 \subseteq M_1$ και $w_2 \in L_2 \subseteq M_2$, και συνεπώς $w \in M_1M_2$. Άρα $L_1L_2 \subseteq M_1M_2$. □

Πρόταση 3 *Ας είναι $L, M \subseteq A^*$. Η ελάχιστη λύση της εξίσωσης*

$$\text{(E)} \qquad X = LX \cup M$$

είναι η γλώσσα L^*M. Αν η γλώσσα L δεν περιέχει την κενή λέξη, δηλαδή $\varepsilon \notin L$, τότε η L^*M είναι μοναδική λύση.

Απόδειξη Θεωρούμε την απεικόνιση

$$f_{(\mathrm{E})} : \mathcal{P}(A^*) \to \mathcal{P}(A^*)$$

που ορίζεται από τη σχέση

$$f_{(\mathrm{E})}(F) = LF \cup M$$

για κάθε $F \in \mathcal{P}(A^*)$. Είναι φανερό πως κάθε λύση της εξίσωσης (E) είναι σταθερό σημείο της $f_{(\mathrm{E})}$ και αντίστροφα. Έτσι το ελάχιστο σταθερό σημείο της $f_{(\mathrm{E})}$ (αν υπάρχει) θα ταυτίζεται με την ελάχιστη λύση της (E). Θα δείξουμε ότι το $\mathrm{fix} f_{(\mathrm{E})}$ υπάρχει. Από το Παράδειγμα 5, το μ.δ.σ. $(\mathcal{P}(A^*), \subseteq)$ είναι ω-πλήρες, άρα αρκεί να δείξουμε ότι η απεικόνιση $f_{(\mathrm{E})}$ είναι ω-συνεχής. Πράγματι, ας είναι $F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots$ μια αύξουσα ακολουθία στοιχείων του $\mathcal{P}(A^*)$. Τότε $\sup_{n\geq 0} F_n = \bigcup_{n\geq 0} F_n$.

Συνεπώς

$$\begin{aligned}
f_{(\mathrm{E})}\left(\sup_{n\geq 0} F_n\right) &= f_{(\mathrm{E})}\left(\bigcup_{n\geq 0} F_n\right) \\
&= L\bigcup_{n\geq 0} F_n \cup M \\
&= \bigcup_{n\geq 0} LF_n \cup M \\
&= \bigcup_{n\geq 0} (LF_n \cup M) \\
&= \sup_{n\geq 0} (LF_n \cup M) \\
&= \sup_{n\geq 0} f_{(\mathrm{E})}(F_n)
\end{aligned}$$

όπου η προτελευταία ισότητα ισχύει καθώς η ακολουθία $(LF_n \cup M)_{n\geq 0}$ είναι λόγω του Λήμματος 3 αύξουσα.

Έτσι, από το Θεώρημα 1, το $\mathrm{fix} f_{(\mathrm{E})}$ υπάρχει και

$$\begin{aligned}
\mathrm{fix} f_{(\mathrm{E})} &= \sup_{n\geq 0} f_{(\mathrm{E})}^{(n)}(\emptyset) \\
&= \sup_{n\geq 0}(L^{n-1}M \cup L^{n-2}M \cup \ldots \cup M) \\
&= \bigcup_{n\geq 0} L^n M \\
&= \left(\bigcup_{n\geq 0} L^n\right) M \\
&= L^* M
\end{aligned}$$

όπου η δεύτερη ισότητα ισχύει καθώς $f_{(\mathrm{E})}^{(0)}(\emptyset) = \emptyset$, $f_{(\mathrm{E})}^{(1)}(\emptyset) = L\emptyset \cup M = M$, $f_{(\mathrm{E})}^{(2)}(\emptyset) = f_{(\mathrm{E})}(M) = LM \cup M$, $f_{(\mathrm{E})}^{(3)}(\emptyset) = f_{(\mathrm{E})}(LM \cup M) = L(LM \cup M) \cup M = L^2 M \cup LM \cup M$, και γενικότερα μπορούμε με επαγωγή να δείξουμε ότι $f_{(\mathrm{E})}^{(n)}(\emptyset) = L^{n-1}M \cup \ldots \cup M$ για κάθε $n \geq 1$.

Άρα η ελάχιστη λύση της εξίσωσης (Ε) είναι η γλώσσα $L^* M$.

Υποθέτουμε τώρα ότι $\varepsilon \notin L$ και θεωρούμε μια οποιαδήποτε λύση Y της εξίσωσης. Θα δείξουμε ότι $Y = L^* M$. Καθώς η $L^* M$ είναι η ελάχιστη λύση της (Ε) θα έχουμε $L^* M \subseteq Y$. Απομένει λοιπόν να δείξουμε τον αντίστροφο εγκλεισμό. Ας είναι $w \in Y$ και έστω $|w| = n$. Τότε

$$\begin{aligned} Y &= LY \cup M \\ &= L(LY \cup M) \cup M \\ &= L^2Y \cup LM \cup M \\ &= L^2(LY \cup M) \cup LM \cup M \\ &= L^3Y \cup L^2M \cup LM \cup M \\ &= \ldots \\ &= L^{n+1}Y \cup L^nM \cup \ldots \cup M. \end{aligned}$$

Αρκεί λοιπόν να δείξουμε ότι $w \in L^nM \cup \ldots \cup M \subseteq L^*M$. Αντίθετα ας υποθέσουμε ότι αυτό δεν ισχύει. Τότε $w \in L^{n+1}Y$. Αυτό σημαίνει ότι $w = w_1 \ldots w_{n+1}u$ όπου $w_1, \ldots, w_{n+1} \in L$ και $u \in Y$. Έτσι

$$\begin{aligned} |w| &= |w_1 \ldots w_{n+1}u| \\ &= |w_1| + \ldots + |w_{n+1}| + |u| \\ &\geq n + 1 + |u| \quad \text{καθώς } \varepsilon \notin L, \end{aligned}$$

άτοπο. □

Παράδειγμα 8 *Δίνεται το αλφάβητο* $A = \{a, b\}$ *και η εξίσωση* $X = (ab^3 \cup b)X \cup a^{10}$. *Σύμφωνα με τη Πρόταση 3 η ελάχιστη λύση της εξίσωσης είναι η γλώσσα* $X = (ab^3 \cup b)^* a^{10}$. *Καθώς η κενή λέξη* ε *δεν ανήκει στη γλώσσα* $(ab^3 \cup b)$, *η λύση είναι μοναδική.*

Στη συνέχεια θα ασχοληθούμε με τη λύση συστημάτων εξισώσεων της μορφής

$$X_1 = L_{11}X_1 \cup L_{12}X_2 \cup \ldots \cup L_{1n}X_n \cup M_1$$

$$X_2 = L_{21}X_1 \cup L_{22}X_2 \cup \ldots \cup L_{2n}X_n \cup M_2$$

$$\ldots$$

$$X_n = L_{n1}X_1 \cup L_{n2}X_2 \cup \ldots \cup L_{nn}X_n \cup M_n$$

όπου $L_{ij}, M_i \subseteq A^*$ για κάθε $1 \leq i,j \leq n$.
Για τη λύση τέτοιων συστημάτων θα χρησιμοποιήσουμε το αποτέλεσμα της Πρότασης 3 και τη γνωστή, από τα αριθμητικά γραμμικά συστήματα, μέθοδο της αντικατάστασης. Ας το δούμε με ένα παράδειγμα.

Παράδειγμα 9 *Δίνεται το αλφάβητο* $A = \{a, b, c\}$ *και το σύστημα εξισώσεων*

$$\begin{aligned} X_1 &= (a^2b^3 \cup c)X_1 \cup a^{10}X_2 \cup \varepsilon \quad (1) \\ X_2 &= (c^4 \cup acb)X_1 \cup bX_2 \cup c \quad (2). \end{aligned}$$

Ξεκινούμε από την πρώτη εξίσωση. Σύμφωνα με τη Πρόταση 3 έχουμε

$$X_1 = (a^2b^3 \cup c)^*(a^{10}X_2 \cup \varepsilon) \ \ (1').$$

Αντικαθιστούμε τη X_1 από την (1 ') στην εξίσωση (2)

$$\begin{aligned} X_2 &= (c^4 \cup acb)(a^2b^3 \cup c)^*(a^{10}X_2 \cup \varepsilon) \cup bX_2 \cup c \\ &= (c^4 \cup acb)(a^2b^3 \cup c)^*a^{10}X_2 \cup (c^4 \cup acb)(a^2b^3 \cup c)^* \cup bX_2 \cup c \\ &= ((c^4 \cup acb)(a^2b^3 \cup c)^*a^{10} \cup b)X_2 \cup (c^4 \cup acb)(a^2b^3 \cup c)^* \cup c. \end{aligned}$$

Η τελευταία εξίσωση έχει άγνωστο μόνο τη X_2 συνεπώς εφαρμόζοντας και πάλι τη Πρόταση 3 παίρνουμε

$$X_2 = ((c^4 \cup acb)(a^2b^3 \cup c)^*a^{10} \cup b)^*((c^4 \cup acb)(a^2b^3 \cup c)^* \cup c).$$

Αντικαθιστώντας την X_2 στην εξίσωση (1 ') αποκτούμε και την X_1, δηλαδή

$$X_1 = (a^2b^3 \cup c)^*(a^{10}((c^4 \cup acb)(a^2b^3 \cup c)^*a^{10} \cup b)^*((c^4 \cup acb)(a^2b^3 \cup c)^* \cup c) \cup \varepsilon).$$

Για να λύσουμε το παραπάνω σύστημα ξεκινήσαμε από τη πρώτη εξίσωση. Θα βρίσκαμε άραγε την ίδια λύση αν ξεκινούσαμε από τη δεύτερη; Η απάντηση είναι *ναι* διότι η λύση είναι μοναδική και αυτό εξασφαλίζεται από το αποτέλεσμα της Πρότασης 3 καθώς οι συντελεστές του συστήματός μας δεν περιέχουν την κενή λέξη ε. Θα πρέπει να παρατηρήσουμε εδώ ότι οι λύσεις που θα πάρουμε ξεκινώντας από τη δεύτερη εξίσωση θα έχουν ενδεχομένως διαφορετική μορφή. Για να γίνει κατανοητό αυτό παρατηρείστε (και αποδείξτε σαν άσκηση) ότι $a(ba)^* = (ab)^*a$.
Στη πραγματικότητα, για τις εφαρμογές της παραπάνω θεωρίας, θα μας απασχολήσουν συστήματα εξισώσεων στα οποία οι συντελεστές των αγνώστων θα είναι γράμματα ή το κενό σύνολο, και η σταθερή γλώσσα θα είναι η κενή λέξη ε ή το κενό σύνολο.

Παράδειγμα 10 *Δίνεται το αλφάβητο $A = \{a, b, c\}$ και το σύστημα εξισώσεων*

$$\begin{aligned} X_1 &= aX_1 \cup bX_2 \cup cX_3 \cup \varepsilon \quad (1) \\ X_2 &= cX_1 \cup bX_2 \quad (2) \\ X_3 &= bX_1 \cup aX_3 \cup \varepsilon \quad (3). \end{aligned}$$

Από την εξίσωση (2) παίρνουμε

$$X_2 = b^*cX_1 \ \ (2')$$

ενώ απο την εξίσωση (3)

$$X_3 = a^*(bX_1 \cup \varepsilon) \ \ (3').$$

Αντικαθιστώντας τις X_2, X_3 από τις (2'),(3') αντίστοιχα, στην (1) έχουμε

$$\begin{aligned} X_1 &= aX_1 \cup bb^*cX_1 \cup ca^*(bX_1 \cup \varepsilon) \cup \varepsilon \\ &= aX_1 \cup bb^*cX_1 \cup ca^*bX_1 \cup ca^* \cup \varepsilon \\ &= (a \cup bb^*c \cup ca^*b)X_1 \cup (ca^* \cup \varepsilon) \end{aligned}$$

και συνεπώς

$$X_1 = (a \cup bb^*c \cup ca^*b)^*(ca^* \cup \varepsilon).$$

Αντικαθιστώντας την X_1 στις (2') και (3') βρίσκουμε τις X_2 και X_3, αντίστοιχα

$$\begin{aligned} X_2 &= b^*c(a \cup bb^*c \cup ca^*b)^*(ca^* \cup \varepsilon) \\ X_3 &= a^*b(a \cup bb^*c \cup ca^*b)^*(ca^* \cup \varepsilon) \cup a^*. \end{aligned}$$

Η λύση και πάλι είναι μοναδική.

Ασκήσεις

1) Να δείξετε ότι η παράθεση λέξεων είναι προσεταιριστική πράξη.

2) Να εξετάσετε αν η πράξη της παράθεσης γλωσσών επιμερίζεται ως προς την πράξη της τομής.

3) Έστω αλφάβητο A. Η *αντίστροφη γλώσσα* (ή *είδωλο*) *μιας γλώσσας* $L \subseteq A^*$ είναι η γλώσσα
$$L^\rho = \{w^\rho \mid w \in L\}.$$
Να δείξετε ότι για $L, M \subseteq A^*$ ισχύει
$$(LM)^\rho = M^\rho L^\rho.$$

4) Έστω αλφάβητο A. Μια γλώσσα $L \subseteq A^*$ είναι *κλειστή με τη πράξη της παράθεσης* αν $L^2 \subseteq L$. Να δείξετε ότι για οποιαδήποτε γλώσσα $L \subseteq A^*$, η θήκη L^* της L είναι η μικρότερη (με τη διάταξη του υποσυνόλου) κλειστή με την πράξη της παράθεσης γλώσσα που περιέχει την κενή λέξη ε και την L.

5) Να λύσετε το σύστημα του Παραδείγματος 9 ξεκινώντας από την δεύτερη εξίσωση.

6) Να λύσετε το σύστημα

$$\begin{aligned} X_1 &= aX_1 \cup cX_2 \cup bX_3 \\ X_2 &= bX_1 \cup cX_2 \cup aX_3 \cup \varepsilon \\ X_3 &= cX_1 \cup bX_2. \end{aligned}$$

7) Να λύσετε το σύστημα

$$\begin{aligned} X_1 &= aX_1 \cup bX_2 \cup cX_3 \cup \varepsilon \\ X_2 &= bX_1 \cup cX_2 \cup aX_3 \\ X_3 &= cX_1 \cup aX_2 \cup bX_3 \cup \varepsilon. \end{aligned}$$

8) Δίνεται αλφάβητο A. Στο $\mathcal{P}(A^*)$ ορίζουμε την πράξη alt ως εξής: $alt(L, M) = \{a_1b_1a_2b_2 \ldots a_nb_n \mid a_1a_2 \ldots a_n \in L, b_1b_2 \ldots b_n \in M, a_1, \ldots, a_n, b_1, \ldots, b_n \in A\}$. Αν $A = \{a, b, c, d\}$, να βρείτε την γλώσσα $alt(L, M)$ στις παρακάτω περιπτώσεις.
(α) $L = \{a^3, bcab, cda^3\}$, $M = \{a^4, cbc, d^6\}$.
(β) $L = \{ca^3, c^{10}a\}$, $M = \{a^4, cbc, d^6\}$.
(γ) $L = \{a^3, bcab, cda^3\}$, $M = \{a^8, c^7, dacbabd\}$.

9) Έστω αλφάβητο A και $w, u \in A^*$. Το *μικτό γινόμενο* $w \sqcup\!\sqcup u$ *των* w, u είναι η γλώσσα

$$w \sqcup\!\sqcup u = \{w_1u_1 \ldots w_nu_n \mid w = w_1w_2 \ldots w_n, u = u_1u_2, \ldots u_n, \\ w_1, w_2, \ldots, w_n, u_1, u_2, \ldots, u_n \in A^*\}.$$

Το μικτό γινόμενο δύο γλωσσών $L, M \subseteq A^*$ ορίζεται από τη σχέση

$$L \sqcup\!\sqcup M = \bigcup_{w \in L, u \in M} w \sqcup\!\sqcup u.$$

Να βρείτε το μικτό γινόμενο των γλωσσών $L \sqcup\!\sqcup M$ για τις γλώσσες L και M της προηγούμενης άσκησης.

10) Δίνεται αλφάβητο A. Για κάθε λέξη $w \in A^*$ και γλώσσα $L \subseteq A^*$ ορίζουμε τη γλώσσα

$$w^{-1}L = \{u \in A^* \mid wu \in L\}.$$

Να βρείτε την γλώσσα $w^{-1}L$ όταν $A = \{a, b, c\}$ και *i*) $w = a$ και $L = a^*$,

ii) $w = a$ και $L = b^*$,

iii) $w = a^3$ και $L = a^5 b^*$,

iv) $w = a^3$ και $L = ca^* b$,

v) $w = b^2 ac$ και $L = (b^3 ac)^*$,

vi) $w = c^2 a$ και $L = c^b a^*$,

vii) $w = abcabc$ και $L = abcabcc^*$,

viii) $w = ab$ και $L = \{a^n b^n \mid n \geq 0\}$,

ix) $w = cb$ και $L = a^* cb^*$,

x) $w = a^4 c^3 b^2$ και $L = a^8 b^* c^8$.

11) Δίνεται αλφάβητο A το οποίο θεωρούμε ολικά διατεταγμένο με μια σχέση $\leq$. Στο A^* θεωρούμε τη σχέση $\leq_{lex}$ που ορίζεται ως εξής:

$$w \leq_{lex} w' \ \text{αν-ν} \ \left(\begin{array}{c} w' = wv, \quad v \in A^* \\ \text{ή} \\ w = uav \text{ και } w' = ua'v', \quad u, v, v' \in A^*, a, a' \in A \text{ με } a \leq a' \end{array} \right)$$

για κάθε $w, w' \in A^*$.

Να δείξετε ότι η σχέση $\leq_{lex}$ είναι ολική διάταξη στο A^* .

12) Δίνεται αλφάβητο A, μονοειδές $(K, \triangle, e)$ και απεικόνιση $h : A \to K$. Να δείξετε ότι η h επεκτείνεται με μοναδικό τρόπο σε ένα μορφισμό από το μονοειδές $(A^*, \cdot, \varepsilon)$ (όπου $\cdot$ συμβολίζει τη πράξη παράθεσης λέξεων) στο μονοειδές $(K, \triangle, e)$.

(Αυτή ακριβώς η ιδότητα του $(A^*, \cdot, \varepsilon)$ είναι που το χαρακτηρίζει ως *το ελεύθερο μονοειδές που παράγεται από το πεπερασμένο σύνολο A*).

Κεφάλαιο 3

Πλήρη πεπερασμένα αυτόματα

Στο κεφάλαιο αυτό θα εισάγουμε τα πλήρη πεπερασμένα αυτόματα και θα ασχοληθούμε με την εύρεση της συμπεριφοράς τους.

Ορισμός 4 *Ένα πλήρες πεπερασμένο αυτόματο (complete finite automaton, σύντομα* CFA[1]*) είναι μια πεντάδα της μορφής* $\mathcal{A} = (Q, A, q_0, \delta, F)$ *όπου*

- Q *είναι το πεπερασμένο σύνολο των καταστάσεων,*
- A *είναι το αλφάβητο εισόδου,*
- $q_0 \in Q$ *είναι η αρχική κατάσταση,*
- $\delta : Q \times A \to Q$ *είναι μια απεικόνιση που περιγράφει τη λειτουργία το αυτομάτου, και*
- $F \subseteq Q$ *είναι το σύνολο των τελικών καταστάσεων.*

Η δ επεκτείνεται σε μία απεικόνιση $\delta^* : Q \times A^* \to Q$, επαγωγικά στο μήκος των λέξεων, ως εξής:

- $\delta^*(q, \varepsilon) = q$,
- $\delta^*(q, wa) = \delta(\delta^*(q, w), a)$

για κάθε $q \in Q, w \in A^*, a \in A$.

Η λέξη $w \in A^*$ *αναγνωρίζεται* από το CFA $\mathcal{A}$ αν $\delta^*(q_0, w) \in F$. Η γλώσσα όλων των λέξεων που αναγνωρίζονται από το $\mathcal{A}$ ονομάζεται *γλώσσα* (ή *συμπεριφορά*) *του* $\mathcal{A}$ και συμβολίζεται με $L(\mathcal{A})$ (ή με $|\mathcal{A}|$), δηλαδή

$$L(\mathcal{A}) = \{w \in A^* \mid \delta^*(q_0, w) \in F\}.$$

Λήμμα 4 *Ας είναι* $\mathcal{A} = (Q, A, q_0, \delta, F)$ *ένα* CFA. *Για κάθε* $q \in Q, w, u \in A^*$ *ισχύει*

$$\delta^*(q, wu) = \delta^*(\delta^*(q, w), u).$$

[1] Ο όρος θα χρησιμοποιείται για τον ενικό και πληθυντικό αριθμό.

Απόδειξη Θα χρησιμοποιήσουμε επαγωγή στο μήκος της λέξης u. Αν $|u| = 0$, τότε $u = \varepsilon$ και συνεπώς

$$\delta^*(q, w\varepsilon) = \delta^*(q, w) = \delta^*(\delta^*(q, w), \varepsilon).$$

Υποθέτουμε τώρα ότι η σχέση ισχύει για κάθε $u \in A^*$ με $|u| \leq k$ και έστω $|u| = k+1$. Τότε $u = u'a$ όπου $u' \in A^*$, $a \in A$ και $|u'| = k$. Έχουμε

$$\begin{aligned}
\delta^*(q, wu) &= \delta^*(q, wu'a) \\
&= \delta(\delta^*(q, wu'), a) && \text{από τον ορισμό της } \delta^* \\
&= \delta(\delta^*(\delta^*(q, w), u'), a) && \text{από την υπόθεση της επαγωγής} \\
&= \delta^*(\delta^*(q, w), u'a) && \text{από τον ορισμό της } \delta^* \\
&= \delta^*(\delta^*(q, w), u),
\end{aligned}$$

όπως το θέλαμε. □

Ένα CFA $\mathcal{A} = (Q, A, q_0, \delta, F)$ αναπαριστάνεται με ένα γράφημα ως εξής: τοποθετούμε στο επίπεδο τις καταστάσεις του, την κάθε μία μέσα σε ένα κύκλο, και βάζουμε ένα βέλος με το γράμμα a από την κατάσταση q_i στην κατάσταση q_j αν και μόνο αν $\delta(q_i, a) = q_j$. Την αρχική κατάσταση την επισημαίνουμε με ένα βέλος που δείχνει σε αυτή ενώ τις τελικές καταστάσεις διαγράφοντας τον κύκλο τους με διπλή γραμμή. Ας υποθέσουμε τώρα ότι η λέξη $w = a_1 a_2 \dots a_n$ αναγνωρίζεται από το CFA. Αυτό σημαίνει ότι $\delta^*(q_0, w) \in F$ και από τον ορισμό της δ υπάρχουν καταστάσεις $q_1, \dots, q_n$ με $q_n \in F$ έτσι ώστε $\delta(q_0, a_1) = q_1, \delta(q_1, a_2) = q_2, \dots, \delta(q_{n-1}, a_n) = q_n$. Συνεπώς στο γράφημα του CFA θα υπάρχει μια *διαδρομή*

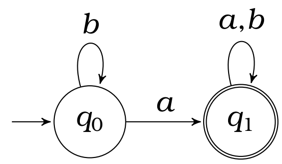
$$\rightarrow q_0 \overset{a_1}{\rightarrow} q_1 \overset{a_2}{\rightarrow} q_2 \dots q_{n-1} \overset{a_n}{\rightarrow} q_n.$$

Μιά τέτοια διαδρομή που ξεκινά από την αρχική κατάσταση και καταλήγει σε τελική ονομάζεται *επιτυχής*. Αντίστροφα, αν για τη λέξη $w = a_1 \dots a_n$ υπάρχει μια επιτυχής διαδρομή της παραπάνω μορφής, τότε η λέξη αναγνωρίζεται από το CFA αφού $\delta^*(q_0, w) = q_n \in F$. Έτσι λοιπόν μια λέξη $w \in A^*$ αναγνωρίζεται απο το CFA $\mathcal{A}$ αν και μόνο αν υπάρχει μια επιτυχής διαδρομή του $\mathcal{A}$ στη w. Συνεπώς για να βρούμε τη γλώσσα $L(\mathcal{A})$ του CFA $\mathcal{A}$ δεν έχουμε παρά να βρούμε όλες τις επιτυχείς διαδρομές του. Είναι όμως αυτό εφικτό; Ας δούμε κάποια παραδείγματα.

Παράδειγμα 11 *Δίνεται το* CFA $\mathcal{A} = (Q, A, q_0, \delta, F)$ *με* $A = \{a, b\}$, $Q = \{q_0, q_1\}$, $F = \{q_1\}$ *και την απεικόνιση* δ *που ορίζεται από τον πίνακα*

δ	a	b
q_0	q_1	q_0
q_1	q_1	q_1

Το γράφημα του CFA *είναι το εξής*



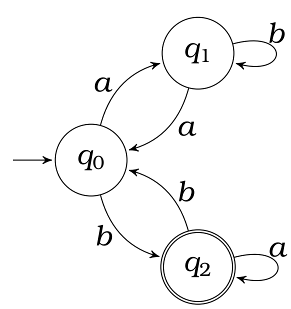
Θεωρούμε τις λέξεις $b^{10}a^3b$, $ab^{1000}a^{40}b^{23}$, b^{10000}. *Τότε* $\delta^*(q_0, b^{10}a^3b) = q_1$, $\delta^*(q_0, ab^{1000}a^{40}b^{23}) = q_1$ *και* $\delta^*(q_0, b^{10000}) = q_0$. *Έτσι* $b^{10}a^3b, ab^{1000}a^{40}b^{23} \in L(\mathcal{A})$, *ενώ* $b^{10000} \notin L(\mathcal{A})$. *Παρατηρούμε ότι με οποιαδήποτε λέξη και αν τροφοδοτήσουμε το* CFA *μας στην αρχική κατάσταση* q_0, *για να φτάσει στην μοναδική τελική κατάσταση* q_1 *θα πρέπει η λέξη να περιέχει μία τουλάχιστο εμφάνιση του γράμματος* a. *Έτσι "είναι εύκολο" να συμπεράνουμε ότι*

$$L(\mathcal{A}) = b^*a(a \cup b)^*.$$

Παράδειγμα 12 *Δίνεται το* CFA $\mathcal{A} = (Q, A, q_0, \delta, F)$ *με* $A = \{a, b\}$, $Q = \{q_0, q_1, q_2\}$, $F = \{q_2\}$ *και την απεικόνιση* δ *που ορίζεται από τον πίνακα*

δ	a	b
q_0	q_1	q_2
q_1	q_0	q_1
q_2	q_2	q_0

Το γράφημα του CFA $\mathcal{A}$ *είναι*



Παρατηρούμε ότι $\delta^*(q_0, a^5b^{30}ab^9a^2) = q_2$, $\delta^*(q_0, a^{2013}b^{3000}ab^{19}a^{2000}) = q_2$, *ενώ* $\delta^*(q_0, a^5b^{30}ab^8) = q_0$ *και συνεπώς* $a^5b^{30}ab^9a^2, a^{2013}b^{3000}ab^{19}a^{2000} \in L(\mathcal{A})$, *ενώ* $a^5b^{30}ab^8 \notin L(\mathcal{A})$.

Είναι φανερό ότι η γλώσσα του CFA του προηγούμενου παραδείγματος δεν μπορεί να υπολογισθεί με κάποιον "εμπειρικό" τρόπο. Και αν το πρόβλημα της αναζήτησης της γλώσσας $L(\mathcal{A})$ στο προηγούμενο παράδειγμα φαίνεται σύνθετο ας αναλογισθεί ο αναγνώστης πόσο αυξάνει η πολυπλοκότητα του προβλήματος αυτού σε ένα CFA με 300 καταστάσεις (μικρός αριθμός για πραγματικές εφαρμογές!) και αλφάβητο εισόδου με 26 γράμματα (π.χ. της Αγγλικής γλώσσας)... Χρειαζόμαστε συνεπώς έναν αλγόριθμο με τον οποίο θα μπορούμε να υπολογίζουμε την γλώσσα οποιουδήποτε αυτομάτου. Πράγματι ο αλγόριθμος αυτός υπάρχει και βασίζεται στη λύση συστημάτων εξισώσεων που μελετήσαμε στο προηγούμενο κεφάλαιο. Χάριν ευκολίας, θα περιγράψουμε παρακάτω τον αλγόριθμο αυτό για το CFA του Παραδείγματος 12.

Θεωρούμε τα τρία CFA (όσα και το πλήθος των καταστάσεων του $\mathcal{A}$) $\mathcal{A}_0 = (Q, A, q_0, \delta, F)$, $\mathcal{A}_1 = (Q, A, q_1, \delta, F)$ και $\mathcal{A}_2 = (Q, A, q_2, \delta, F)$. Παρατηρείστε ότι τα νέα αυτόματα έχουν τα ίδια στοιχεία με το αρχικό εκτός από την αρχική κατάσταση και ότι $\mathcal{A}_0 = \mathcal{A}$. Ονομάζουμε τις γλώσσες τους $X_0 = L(\mathcal{A}_0)$, $X_1 = L(\mathcal{A}_1)$ και $X_2 = L(\mathcal{A}_2)$. Φανερά η ζητούμενη γλώσσα του $\mathcal{A}$ είναι η X_0. Ας υποθέσουμε τώρα ότι η λέξη $w \in A^*$ αναγνωρίζεται από το αυτόματο $\mathcal{A}_0$ δηλαδή $\delta^*(q_0, w) = q_2$. Διακρίνουμε 2 περιπτώσεις:

(α) Η w αρχίζει με a συνεπώς $w = au$ για κάποια λέξη $u \in A^*$ και $\delta^*(q_0, w) = \delta^*(q_0, au) = \delta^*(\delta^*(q_0, a), u) = \delta^*(q_1, u) = q_2$. Η τελευταία ισότητα σημαίνει ότι η λέξη u αναγνωρίζεται από το CFA $\mathcal{A}_1$. Αντίστροφα, ας υποθέσουμε ότι μια λέξη $u' \in A^*$ αναγνωρίζεται από το CFA $\mathcal{A}_1$. Τότε $\delta^*(q_1, u') = q_2$ οπότε $\delta^*(q_0, au') = \delta^*(\delta^*(q_0, a), u') = \delta^*(q_1, u') = q_2$ δηλαδή η $au' \in L(\mathcal{A}_0)$.

(β) Η w αρχίζει με b συνεπώς $w = bv$ για κάποια λέξη $v \in A^*$ και $\delta^*(q_0, w) = \delta^*(q_0, bv) = \delta^*(\delta^*(q_0, b), v) = \delta^*(q_2, v) = q_2$. Η τελευταία σχέση σημαίνει ότι η λέξη v αναγνωρίζεται από το CFA $\mathcal{A}_2$. Αντίστροφα, ας υποθέσουμε ότι μια λέξη $v' \in A^*$ αναγνωρίζεται από το CFA $\mathcal{A}_2$. Τότε $\delta^*(q_2, v') = q_2$ οπότε $\delta^*(q_0, bv') = \delta^*(\delta^*(q_0, b), v') = \delta^*(q_2, v') = q_2$ δηλαδή η $bv' \in L(\mathcal{A}_0)$.

Τα παραπάνω σημαίνουν πως $X_0 = aX_1 \cup bX_2$.

Θεωρούμε τώρα το CFA $\mathcal{A}_1$ και έστω μια λέξη $w \in A^*$ που αναγνωρίζεται από αυτό, δηλαδή $\delta^*(q_1, w) = q_2$. Πάλι διακρίνουμε 2 περιπτώσεις:

(α′) Η w αρχίζει με a συνεπώς $w = au$ για κάποια λέξη $u \in A^*$ και $\delta^*(q_1, w) = \delta^*(q_1, au) = \delta^*(\delta^*(q_1, a), u) = \delta^*(q_0, u) = q_2$. Η τελευταία ισότητα σημαίνει ότι η λέξη u αναγνωρίζεται από το αυτόματο $\mathcal{A}_0$. Αντίστροφα, ας υποθέσουμε ότι μια λέξη $u' \in A^*$ αναγνωρίζεται από το CFA $\mathcal{A}_0$. Τότε $\delta^*(q_0, u') = q_2$ οπότε $\delta^*(q_1, au') = \delta^*(\delta^*(q_1, a), u') = \delta^*(q_0, u') = q_2$ δηλαδή η $au' \in L(\mathcal{A}_1)$.

(β′) Η w αρχίζει με b συνεπώς $w = bv$ για κάποια λέξη $v \in A^*$ και $\delta^*(q_1, w) = \delta^*(q_1, bv) = \delta^*(\delta^*(q_1, b), v) = \delta^*(q_1, v) = q_2$. Η τελευταία ισότητα σημαίνει ότι και η λέξη v αναγνωρίζεται από το αυτόματο $\mathcal{A}_1$. Αντίστροφα, ας υποθέσουμε ότι μια λέξη $v' \in A^*$ αναγνωρίζεται από το CFA $\mathcal{A}_1$. Τότε $\delta^*(q_1, v') = q_1$ οπότε $\delta^*(q_1, bv') = \delta^*(\delta^*(q_1, b), v') = \delta^*(q_1, v') = q_2$ δηλαδή η $bv' \in L(\mathcal{A}_1)$.

Τα παραπάνω σημαίνουν πως $X_1 = aX_0 \cup bX_1$.

Τέλος θα επαναλάβουμε τη διαδικασία για το CFA $\mathcal{A}_2$. Ας είναι λοιπόν $w \in A^*$ μια λέξη που αναγνωρίζεται από το CFA $\mathcal{A}_2$ δηλαδή $\delta^*(q_2, w) = q_2$. Διακρίνουμε 2 περιπτώσεις:

(α) Η w αρχίζει με a συνεπώς $w = au$ για κάποια λέξη $u \in A^*$ και $\delta^*(q_2, w) = \delta^*(q_2, au) = \delta^*(\delta^*(q_2, a), u) = \delta^*(q_2, u) = q_2$. Η τελευταία ισότητα σημαίνει ότι και η λέξη u αναγνωρίζεται από το CFA $\mathcal{A}_2$. Αντίστροφα, ας υποθέσουμε ότι μια λέξη $u' \in A^*$ αναγνωρίζεται από το CFA $\mathcal{A}_2$. Τότε $\delta^*(q_2, u') = q_2$ οπότε $\delta^*(q_2, au') = \delta^*(\delta^*(q_2, a), u') = \delta^*(q_2, u') = q_2$ δηλαδή η $au' \in L(\mathcal{A}_2)$.

(β) Η w αρχίζει με b συνεπώς $w = bv$ για κάποια λέξη $v \in A^*$ και $\delta^*(q_2, w) = \delta^*(q_2, bv) = \delta^*(\delta^*(q_2, b), v) = \delta^*(q_0, v) = q_2$. Η τελευταία ισότητα σημαίνει ότι η λέξη v αναγνωρίζεται από το CFA $\mathcal{A}_0$. Αντίστροφα, ας υποθέσουμε ότι μια λέξη $v' \in A^*$ αναγνωρίζεται από το CFA $\mathcal{A}_0$. Τότε $\delta^*(q_0, v') = q_2$ οπότε $\delta^*(q_2, bv') = \delta^*(\delta^*(q_2, b), v') = \delta^*(q_0, v') = q_2$ δηλαδή η $bv' \in L(\mathcal{A}_2)$.

Θα πρέπει να παρατηρήσουμε εδώ πως $\delta^*(q_2, \varepsilon) = q_2$ και συνεπώς και η κενή λέξη αναγνωρίζεται από το CFA $\mathcal{A}_2$. Από το γεγονός αυτό και την προηγούμενη ανάλυση συνάγουμε ότι $X_2 = aX_2 \cup bX_0 \cup \varepsilon$.

Συνοψίζοντας έχουμε

$$\begin{aligned} X_0 &= aX_1 \cup bX_2 \\ X_1 &= aX_0 \cup bX_1 \\ X_2 &= aX_2 \cup bX_0 \cup \varepsilon. \end{aligned}$$

Συνεπώς για να βρούμε την X_0, δηλαδή τη συμπεριφορά του CFA $\mathcal{A}$, δεν έχουμε παρά να λύσουμε το παραπάνω σύστημα. Έχουμε $X_1 = b^*aX_0$ και $X_2 = a^*(bX_0 \cup \varepsilon)$ και αντικαθιστώντας στη πρώτη εξίσωση παίρνουμε

$$\begin{aligned} X_0 &= ab^*aX_0 \cup ba^*(bX_0 \cup \varepsilon) \\ &= ab^*aX_0 \cup ba^*bX_0 \cup ba^* \\ &= (ab^*a \cup ba^*b)X_0 \cup ba^* \end{aligned}$$

και συνεπώς

$$X_0 = (ab^*a \cup ba^*b)^*ba^*.$$

Άρα $L(\mathcal{A}) = (ab^*a \cup ba^*b)^*ba^*$.

Θα περιγράψουμε τώρα τον παραπάνω αλγόριθμο στην γενική περίπτωση. Ας είναι λοιπόν $\mathcal{A} = (Q, A, q_0, \delta, F)$ ένα CFA και έστω $Q = \{q_0, q_1, \ldots, q_n\}$. Θεωρούμε τις γλώσσες (που απαρτίζονται από γράμματα ή είναι το κενό σύνολο) $L_{ij} = \{a \in A \mid \delta(q_i, a) = q_j\}$ για $0 \le i, j \le n$ και τις μεταβλητές X_i για $0 \le i \le n$. [2]

[2]Οι μεταβλητές X_i προκύπτουν από τη θεώρηση των CFA $\mathcal{A}_i = (Q, A, q_i, \delta, F)$ με $X_i = L(\mathcal{A}_i)$ για κάθε $0 \le i \le n$.

Σχηματίζουμε το σύστημα γραμμικών εξισώσεων

$$\begin{aligned} X_0 &= L_{00}X_0 \cup L_{01}X_1 \cup \ldots \cup L_{0n}X_n \cup M_0 \\ X_1 &= L_{10}X_0 \cup L_{11}X_1 \cup \ldots \cup L_{1n}X_n \cup M_1 \\ &\ldots \\ X_n &= L_{n0}X_0 \cup L_{n1}X_1 \cup \ldots \cup L_{nn}X_n \cup M_n \end{aligned}$$

όπου $M_i = \varepsilon$ αν $q_i \in F$ και $M_i = \emptyset$ αν $q_i \notin F$, για κάθε $0 \leq i \leq n$.

Λύνουμε το σύστημα και αποκτούμε τη γλώσσα $L(\mathcal{A}) = X_0$ του CFA $\mathcal{A}$.

Ασκήσεις

1) Να σχεδιάσετε το CFA $\mathcal{A} = (\{q_0, q_1, q_2\}, \{a, b\}, q_0, \delta, \{q_0, q_2\})$ με

δ	a	b
q_0	q_1	q_0
q_1	q_2	q_1
q_2	q_2	q_2

και να βρείτε τη γλώσσα του.

2) Να σχεδιάσετε το CFA $\mathcal{A} = (\{q_0, q_1, q_2, q_3\}, \{a, b, c\}, q_0, \delta, \{q_1, q_3\})$ με

δ	a	b	c
q_0	q_2	q_1	q_0
q_1	q_2	q_3	q_1
q_2	q_2	q_2	q_2
q_3	q_1	q_3	q_0

και να βρείτε τη γλώσσα του. Τι παρατηρείτε σχετικά με τη κατάσταση q_2;

3) Δίνεται το αλφάβητο $A = \{a, b, c, d\}$. Να κατασκευάσετε CFA με αλφάβητο εισόδου το A που αναγνωρίζει ακριβώς όλες τις λέξεις που δεν περιέχουν καμία εμφάνιση του γράμματος c.

4) Δίνεται το αλφάβητο $A = \{a, b, c, d\}$. Να κατασκευάσετε CFA με αλφάβητο εισόδου το A που αναγνωρίζει ακριβώς όλες τις λέξεις που δεν περιέχουν καμία εμφάνιση των γραμμάτων a και d.

5) Δίνεται το αλφάβητο $A = \{a, b, c, d\}$. Να κατασκευάσετε CFA με αλφάβητο εισόδου το A που αναγνωρίζει ακριβώς όλες τις λέξεις που περιέχουν μία εμφάνιση του γράμματος c.

6) Δίνεται το αλφάβητο $A = \{a, b, c, d\}$. Να κατασκευάσετε CFA με αλφάβητο εισόδου το A που αναγνωρίζει ακριβώς όλες τις λέξεις που περιέχουν δύο εμφανίσεις του γράμματος c.

7) Δίνεται το αλφάβητο $A = \{a, b, c, d\}$. Να κατασκευάσετε CFA με αλφάβητο εισόδου το A που αναγνωρίζει ακριβώς όλες τις λέξεις που περιέχουν μία εμφάνιση του γράμματος a και μία εμφάνιση του γράμματος c.

8) Δίνεται το αλφάβητο $A = \{a, b, c, d\}$. Να κατασκευάσετε CFA με αλφάβητο εισόδου το A που αναγνωρίζει ακριβώς όλες τις λέξεις που περιέχουν μία εμφάνιση του γράμματος a, μία εμφάνιση του γράμματος b και μία εμφάνιση του γράμματος c.

9) Δίνεται το αλφάβητο $A = \{a, b, c, d\}$. Να κατασκευάσετε CFA με αλφάβητο εισόδου το A που αναγνωρίζει τη γλώσσα $L = \emptyset$.

10) Δίνεται το αλφάβητο $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Να κατασκευάσετε CFA του οποίου η γλώσσα είναι το σύνολο των άρτιων φυσικών αριθμών.

11) Δίνεται το αλφάβητο $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Να κατασκευάσετε CFA του οποίου η γλώσσα είναι το σύνολο των φυσικών αριθμών που είναι πολλαπλάσια του 5.

12) Δίνεται το αλφάβητο $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Να κατασκευάσετε CFA του οποίου η γλώσσα είναι το σύνολο των φυσικών αριθμών που είναι πολλαπλάσια του 3.

13) Δίνεται το αλφάβητο $A = \{0, 1\}$. Να κατασκευάσετε CFA του οποίου η γλώσσα θα είναι το σύνολο των άρτιων φυσικών αριθμών γραμμένων στο δυαδικό σύστημα αρίθμησης.

Κεφάλαιο 4

Αναγνωρίσιμες γλώσσες

Θεωρούμε ένα αλφάβητο A. Μια γλώσσα $L \subseteq A^*$ θα ονομάζεται *αναγνωρίσμη* αν υπάρχει CFA $\mathcal{A} = (Q, A, q_0, \delta, F)$ του οποίου η γλώσσα να είναι η L, δηλαδή $L = L(\mathcal{A})$. Θα συμβολίζουμε με $\mathrm{Rec}(A)$ τη κλάση όλων των αναγνωρίσιμων γλωσσών από το αλφάβητο A.[1] Στο κεφάλαιο αυτό θα μελετήσουμε καταρχήν ιδότητες κλειστότητας της κλάσης $\mathrm{Rec}(A)$ με τις *boolean* πράξεις, δηλαδή την τομή, την ένωση και το συμπλήρωμα. Συγκεκριμένα, θα δείξουμε ότι η κλάση $\mathrm{Rec}(A)$ είναι κλειστή και με τις τρεις αυτές πράξεις. Στη συνέχεια θα δώσουμε ένα κριτήριο μη-αναγνωρισιμότητας.

Πρόταση 4 *Αν $L, M \in \mathrm{Rec}(A)$, τότε $L \cap M \in \mathrm{Rec}(A)$.*

Απόδειξη Ας είναι $\mathcal{A} = (Q, A, q_0, \delta_{\mathcal{A}}, F)$ και $\mathcal{B} = (P, A, p_0, \delta_{\mathcal{B}}, S)$ δύο πλήρη αυτόματα που αναγνωρίζουν τις γλώσσες L και M αντίστοιχα, δηλαδή $L = L(\mathcal{A})$ και $M = L(\mathcal{B})$. Θα κατασκευάσουμε CFA που αναγνωρίζει τη γλώσσα $L \cap M$. Πριν παρουσιάσουμε το νέο CFA, θα προσπαθήσουμε να εξηγήσουμε διαισθητικά πως πρέπει αυτό να λειτουργεί ώστε να αναγνωρίζει ακριβώς την τομή των δύο γλωσσών. Ας είναι λοιπόν $w = a_1 \ldots a_n \in L \cap M$ μια λέξη που αναγνωρίζεται και από τα δύο CFA. Αυτό σημαίνει ότι υπάρχουν επιτυχείς διαδρομές

$$\to q_0 \stackrel{a_1}{\to} q_1 \stackrel{a_2}{\to} q_2 \ldots q_{n-1} \stackrel{a_n}{\to} q_n \in F$$

και

$$\to p_0 \stackrel{a_1}{\to} p_1 \stackrel{a_2}{\to} p_2 \ldots q_{n-1} \stackrel{a_n}{\to} p_n \in S$$

στο $\mathcal{A}$ και στο $\mathcal{B}$, αντίστοιχα.
Εφόσον η λέξη w θα πρέπει να αναγνωρίζεται από το νέο CFA, θα πρέπει να υπάρχει σε αυτό επιτυχής διαδρομή για την w. Αντίθετα αν η w δεν αναγνωριζόταν είτε από το $\mathcal{A}$ είτε από το $\mathcal{B}$ (είτε και από τα δύο) τότε στο νέο CFA η διαδρομή που ξεκινά από την αρχική κατάσταση με την w δεν θα πρέπει να είναι επιτυχής,

[1] Ο συμβολισμός Rec προκύπτει από την λέξη *recognizable* = αναγνωρίσιμη.

δηλαδή η κατάσταση στην οποία θα τερματίσει δεν θα πρέπει να είναι τελική. Άρα θα πρέπει η διαδρομή του νέου CFA που ξεκινά από την αρχική του κατάσταση για κάθε λέξη, να είναι επιτυχής αν και μόνο αν οι αντίστοιχες διαδρομές στα CFA $\mathcal{A}$ και $\mathcal{B}$ είναι *και οι δύο* επιτυχείς. Με άλλα λόγια θα πρέπει για κάθε λέξη, η διαδρομή που ξεκινά από την αρχική κατάσταση στο νέο CFA για την λέξη αυτή, να προσομοιάζει και τις δύο διαδρομές των CFA $\mathcal{A}$ και $\mathcal{B}$, για την ίδια λέξη, που ξεκινούν αντίστοιχα από τις αρχικές τους καταστάσεις. Για να το πετύχουμε αυτό, είναι επιθυμητό να έχουμε μια διαδρομή στο νέο αυτόματο η οποία να "υλοποιεί" ταυτόχρονα τις διαδρομές και των δύο CFA, για παράδειγμα

$$\to (q_0, p_0) \xrightarrow{a_1} (q_1, p_1) \xrightarrow{a_2} (q_2, p_2) \ldots (q_{n-1}, p_{n-1}) \xrightarrow{a_n} (q_n, p_n).$$

Αυτό μας οδηγεί στο να θεωρήσουμε στο νέο CFA ως σύνολο καταστάσεων το καρτεσιανό γινόμενο των συνόλων των καταστάσεων των δύο αυτομάτων. Ας συνεχίσουμε τώρα την απόδειξή μας με αυστηρά μαθηματικό τρόπο.

Θεωρούμε το CFA $C = (Q \times P, A, (q_0, p_0), \delta_C, F \times S)$ του οποίου η λειτουργία $\delta_C : (Q \times P) \times A \to (Q \times P)$ δίνεται από τη σχέση

$$\delta_C((q, p), a) = (\delta_{\mathcal{A}}(q, a), \delta_{\mathcal{B}}(p, a))$$

για κάθε $(q, p) \in Q \times P, a \in A$.
Καταρχήν θα δείξουμε ότι

$$\delta_C^*((q, p), w) = (\delta_{\mathcal{A}}^*(q, w), \delta_{\mathcal{B}}^*(p, w))$$

για κάθε $(q, p) \in Q \times P, w \in A^*$. Θα χρησιμοποιήσουμε επαγωγή στο μήκος της λέξης w. Πράγματι αν $|w| = 0$, τότε $w = \varepsilon$ οπότε $\delta_C^*((q, p), \varepsilon) = (q, p) = (\delta_{\mathcal{A}}^*(q, \varepsilon), \delta_{\mathcal{B}}^*(p, \varepsilon))$. Υποθέτουμε ότι η πρόταση ισχύει για όλες τις λέξεις με μήκος $\leq k$ και έστω $w \in A^*$ με μήκος $|w| = k + 1$. Τότε $w = ua$ με $u \in A^*, a \in A$ και $|u| = k$. Έχουμε

$$\begin{aligned}
\delta_C^*((q, p), w) &= \delta_C^*((q, p), ua) \\
&= \delta_C(\delta_C^*((q, p), u), a) \\
&= \delta_C((\delta_{\mathcal{A}}^*(q, u), \delta_{\mathcal{B}}^*(p, u)), a) && \text{από την υπόθεση της επαγωγής} \\
&= (\delta_{\mathcal{A}}(\delta_{\mathcal{A}}^*(q, u), a), \delta_{\mathcal{B}}(\delta_{\mathcal{B}}^*(p, u), a)) && \text{από τον ορισμό της } \delta_C \\
&= (\delta_{\mathcal{A}}^*(q, ua), \delta_{\mathcal{B}}^*(p, ua)) \\
&= (\delta_{\mathcal{A}}^*(q, w), \delta_{\mathcal{B}}^*(p, w)).
\end{aligned}$$

Ας είναι τώρα $w \in A^*$. Έχουμε

$$\begin{aligned}
w \in L(C) &\iff \delta_C^*((q_0, p_0), w) \in F \times S \\
&\iff (\delta_{\mathcal{A}}^*(q_0, w), \delta_{\mathcal{B}}^*(p_0, w)) \in F \times S \\
&\iff \delta_{\mathcal{A}}^*(q_0, w) \in F \;\text{ και }\; \delta_{\mathcal{B}}^*(p_0, w) \in S \\
&\iff w \in L(\mathcal{A}) = L \;\text{ και }\; w \in L(\mathcal{B}) = M \\
&\iff w \in L \cap M
\end{aligned}$$

δηλαδή $L(C) = L \cap M$, και συνεπώς η γλώσσα $L \cap M$ είναι αναγνωρίσιμη. □

Πρόταση 5 *Αν* $L \in \mathrm{Rec}(A)$, *τότε* $\overline{L} \in \mathrm{Rec}(A)$, *όπου* $\overline{L} = A^* \setminus L$ *το συμπλήρωμα της* L.

Απόδειξη Ας είναι $\mathcal{A} = (Q, A, q_0, \delta, F)$ CFA[2] τέτοιο ώστε $L(\mathcal{A}) = L$. Θεωρούμε το CFA $\overline{\mathcal{A}} = (Q, A, q_0, \delta, Q \setminus F)$. Θα δείξουμε ότι $\overline{L} = L(\overline{\mathcal{A}})$. Πράγματι, για κάθε $w \in A^*$ έχουμε

$$\begin{aligned} w \in L(\overline{\mathcal{A}}) &\iff \delta^*(q_0, w) \in Q \setminus F \\ &\iff \delta^*(q_0, w) \notin F \\ &\iff w \notin L(\mathcal{A}) \\ &\iff w \notin L \\ &\iff w \in \overline{L} \end{aligned}$$

δηλαδή $L(\overline{\mathcal{A}}) = \overline{L}$, που σημαίνει ότι η $\overline{L}$ είναι αναγνωρίσιμη γλώσσα. □

Πρόταση 6 *Αν* $L, M \in \mathrm{Rec}(A)$, *τότε* $L \cup M \in \mathrm{Rec}(A)$.

Απόδειξη Καθώς

$$L \cup M = \overline{\overline{L} \cap \overline{M}}$$

η απόδειξη προκύπτει από τις Προτάσεις 4 και 5. □

Η απόδειξη της Πρότασης 6 έγινε με αλγεβρικό τρόπο χρησιμοποιώντας τα αποτελέσματα των Προτάσεων 4 και 5 και τον κανόνα *De Morgan*. Καθώς όμως τα τα προβλήματα που μελετάμε στη Θεωρητική Πληροφορική είναι άμεσα συνδεδεμένα με τις πρακτικές εφαρμογές, είναι σημαντικό οι αποδείξεις να συνοδεύονται από τους κατάλληλους αλγόριθμους κατασκευής των μοντέλων που εμπλέκονται σε αυτές (όπου αυτό είναι εφικτό). Εν προκειμένω οι αποδείξεις των Προτάσεων 4 και 5 μας εφοδιάζουν με τον αλγόριθμο κατασκευής του CFA που αναγνωρίζει τη γλώσσα $L \cup M$ της Πρότασης 6. Πράγματι, ας είναι $\mathcal{A} = (Q, A, q_0, \delta_{\mathcal{A}}, F)$ και $\mathcal{B} = (P, A, p_0, \delta_{\mathcal{B}}, S)$ δύο CFA που αναγνωρίζουν τις γλώσσες L και M αντίστοιχα, δηλαδή $L = L(\mathcal{A})$ και $M = L(\mathcal{B})$. Από τη Πρόταση 5 έχουμε ότι $\overline{L} = L(\overline{\mathcal{A}})$ και $\overline{M} = L(\overline{\mathcal{B}})$ όπου $\overline{\mathcal{A}} = (Q, A, q_0, \delta_{\mathcal{A}}, Q \setminus F)$ και $\overline{\mathcal{B}} = (P, A, p_0, \delta_{\mathcal{B}}, P \setminus S)$. Από τη Πρόταση 4, το CFA $C = (Q \times P, A, (q_0, p_0), \delta_C, (Q \setminus F) \times (P \setminus S))$ με

$$\delta_C((q, p), a) = (\delta_{\mathcal{A}}(q, a), \delta_{\mathcal{B}}(p, a))$$

για κάθε $(q, p) \in Q \times P, a \in A$, αναγνωρίζει τη γλώσσα $\overline{L} \cap \overline{M}$. Τέλος με εφαρμογή της Πρότασης 5, το CFA $\overline{C} = (Q \times P, A, (q_0, p_0), \delta_C, (F \times P) \cup (Q \times S))$ αναγνωρίζει την $L \cup M$ (παρατηρείστε ότι $(F \times P) \cup (Q \times S) = (Q \times P) \setminus ((Q \setminus F) \times (P \setminus S))$).

[2]Όπως θα δούμε παρακάτω (καθώς θα ορίσουμε και μη-πλήρη αυτόματα) το γεγονός ότι το πεπερασμένο αυτόματο είναι πλήρες είναι καθοριστικής σημασίας στην απόδειξη αυτή.

Παράδειγμα 13 *Δίνεται το αλφάβητο* $A = \{a, b\}$. *Θα δείξουμε ότι η γλώσσα* $L = \{a^m b^m \mid m \geq 0\}$ *δεν είναι αναγνωρίσιμη.*

Ας υποθέσουμε αντίθετα ότι η $L \in \mathrm{Rec}(A)$ *και έστω* $\mathcal{A} = (Q, A, q_0, \delta, F)$ *ένα* CFA *που την αναγνωρίζει. Θεωρούμε την ακολουθία καταστάσεων*

$$\delta^*(q_0, a^0), \delta^*(q_0, a^1), \delta^*(q_0, a^2), \ldots.$$

Καθώς το Q *είναι πεπερασμένο υπάρχουν δείκτες* $0 \leq i < j$ *έτσι ώστε*

$$\delta^*(q_0, a^i) = \delta^*(q_0, a^j).$$

Φανερά $a^i b^j \notin L(\mathcal{A})$ *και συνεπώς* $\delta^*(q_0, a^i b^j) \notin F$. *Όμως*

$$\delta^*(q_0, a^i b^j) = \delta^*(\delta^*(q_0, a^i), b^j) = \delta^*(\delta^*(q_0, a^j), b^j) = \delta(q_0, a^j b^j) \in F,$$

άτοπο, και συνεπώς η L *δεν είναι αναγνωρίσιμη.*

Παράδειγμα 14 *Δίνεται το αλφάβητο* $A = \{a, b, c, d, e, f, g\}$. *Θα δείξουμε ότι η γλώσσα* $L = \{fedb^m gbaf^m d \mid m \geq 0\}$ *δεν είναι αναγνωρίσιμη.*

Ας υποθέσουμε αντίθετα ότι η $L \in \mathrm{Rec}(A)$ *και έστω* $\mathcal{A} = (Q, A, q_0, \delta, F)$ *ένα* CFA *που την αναγνωρίζει. Θεωρούμε την ακολουθία καταστάσεων*

$$\delta^*(q_0, fedb^0), \delta^*(q_0, fedb^1), \delta^*(q_0, fedb^2), \ldots.$$

Καθώς το Q *είναι πεπερασμένο υπάρχουν δείκτες* $0 \leq i < j$ *έτσι ώστε*

$$\delta^*(q_0, fedb^i) = \delta^*(q_0, fedb^j).$$

Φανερά $fedb^i gbaf^j d \notin L(\mathcal{A})$ *και συνεπώς* $\delta^*(q_0, fedb^i gbaf^j d) \notin F$. *Όμως*

$$\begin{aligned}
\delta^*(q_0, fedb^i gbaf^j d) &= \delta^*(\delta^*(q_0, fedb^i), gbaf^j d) \\
&= \delta^*(\delta^*(q_0, fedb^j), gbaf^j d) \\
&= \delta^*(q_0, fedb^j gbaf^j d) \in F.
\end{aligned}$$

άτοπο, και συνεπώς η L *δεν είναι αναγνωρίσιμη.*

Στη συνέχεια θα αποδείξουμε ένα κριτήριο μη-αναγνωρισιμότητας, δηλαδή ένα αποτέλεσμα που θα μας επιτρέπει να αποφασίζουμε ότι μια γλώσσα δεν είναι αναγνωρίσιμη. Το αποτέλεσμα αυτό είναι γνωστό διεθνώς ως *Pumping Lemma*.

Πρόταση 7 *Για κάθε αναγνωρίσιμη γλώσσα* $L \in A^*$ *υπάρχει φυσικός αριθμός* $n > 0$ *τέτοιος ώστε αν* $w \in L$ *με* $|w| > n$, *τότε η* w *γράφεται* $w = xyz$ *με* $y \neq \varepsilon$ *και* $xy^k z \in L$ *για κάθε* $k \geq 0$.

Απόδειξη Η γλώσσα L είναι αναγνωρίσιμη, συνεπώς υπάρχει αυτόματο $\mathcal{A} = (Q, A, q_0, \delta, F)$ έτσι ώστε $L = L(\mathcal{A})$. Θέτουμε $n = card(Q)$ και έστω λέξη $w = a_1 \dots a_m \in L$ με $|w| = m > n$. Τότε στο $\mathcal{A}$ υπάρχει επιτυχής διαδρομή

$$\to q_0 \xrightarrow{a_1} q_1 \xrightarrow{a_2} q_2 \dots q_{m-1} \xrightarrow{a_m} q_m \in F.$$

Καθώς $m > n$ θα υπάρχουν στην παραπάνω διαδρομή δύο (τουλάχιστο) δείκτες $0 \leq i < j \leq m$ έτσι ώστε $q_i = q_j$, δηλαδή

$$\to q_0 \xrightarrow{a_1} q_1 \dots q_{i-1} \xrightarrow{a_i} q_i \xrightarrow{a_{i+1}} q_{i+1} \dots q_{j-1} \xrightarrow{a_j} q_i \xrightarrow{a_{j+1}} q_{j+1} \dots q_{m-1} \xrightarrow{a_m} q_m \in F.$$

Θέτουμε

$$x = a_1 \dots a_i, \quad y = a_{i+1} \dots a_j, \quad z = a_{j+1} \dots a_m.$$

Προφανώς $w = xyz$, και καθώς $i < j$ ισχύει $y \neq \varepsilon$. Πρόσθετα το γεγονός $q_i = q_j$ σημαίνει πως στην κατάσταση q_i το CFA σχηματίζει ένα *loop* με τη λέξη y. Έτσι για $k = 0, 1, 2, 3, \dots$ υπάρχουν επιτυχείς διαδρομές

$$\to q_0 \overset{x}{\rightsquigarrow} q_i = q_j \overset{z}{\rightsquigarrow} q_m \in F$$

$$\to q_0 \overset{x}{\rightsquigarrow} q_i \overset{y}{\rightsquigarrow} q_i \overset{z}{\rightsquigarrow} q_m \in F$$

$$\to q_0 \overset{x}{\rightsquigarrow} q_i \overset{y}{\rightsquigarrow} q_i \overset{y}{\rightsquigarrow} q_i \overset{z}{\rightsquigarrow} q_m \in F$$

$$\to q_0 \overset{x}{\rightsquigarrow} q_i \overset{y}{\rightsquigarrow} q_i \overset{y}{\rightsquigarrow} q_i \overset{y}{\rightsquigarrow} q_i \overset{z}{\rightsquigarrow} q_m \in F$$

$$\dots$$

αντίστοιχα. Είναι λοιπόν προφανές ότι για κάθε $k \geq 0$ η λέξη $xy^kz \in L$, και η απόδειξη τελείωσε. ☐

Το παραπάνω αποτέλεσμα το χρησιμοποιούμε για να δείξουμε ότι μια γλώσσα δεν είναι αναγνωρίσιμη. Ας ξαναδούμε λοιπόν τη γλώσσα του Παραδείγματος 13.

Υποθέτουμε ότι η $L = \{a^m b^m \mid m \geq 0\} \in \mathrm{Rec}(A)$ και έστω n ο φυσικός που προκύπτει για την L από τη Πρόταση 7. Θεωρούμε τη λέξη $w = a^n b^n$. Καθώς $|w| = 2n$ θα έχουμε $w = xyz$ όπου $y \neq \varepsilon$ και $xy^kz \in L$ για κάθε $k \geq 0$. Για την y διακρίνουμε τις παρακάτω περιπτώσεις.

i) Η y περιέχει μόνο γράμματα a, συνεπώς όλα τα γράμματα b της w βρίσκονται στη λέξη z. Τότε όμως η $xy^2z \in L$ περιέχει n γράμματα b και περισσότερα από n γράμματα a, άτοπο.

ii) Η y περιέχει μόνο γράμματα b, συνεπώς όλα τα γράμματα a της w βρίσκονται στη λέξη x. Τότε όμως η $xy^2z \in L$ περιέχει n γράμματα a και περισσότερα από n γράμματα b, άτοπο.

iii) Η y περιέχει γράμματα a και b, έστω $y = a^\mu b^\nu$. Από την Πρόταση 7, η $xy^2z \in L$, και $xy^2z = xa^\mu b^\nu a^\mu b^\nu z$, άτοπο.

Άρα σε κάθε περίπτωση καταλήξαμε σε άτοπο, συνεπώς η L δεν είναι αναγνωρίσιμη.

Παράδειγμα 15 *Δίνεται το αλφάβητο $A = \{a\}$. Θα δείξουμε ότι η γλώσσα*

$$L = \{a^p \mid p \ \text{ πρώτος αριθμός}\}$$

δεν είναι αναγνωρίσιμη.

Ας υποθέσουμε αντίθετα ότι $L \in \mathrm{Rec}(\{a\})$ και έστω n ο φυσικός που προκύπτει για την L από τη Πρόταση 7. Θεωρούμε τη λέξη $w = a^p$ όπου p πρώτος με $p > n$. Τότε η $w = xyz$ με $y \neq \varepsilon$ και $xy^kz \in L$ για κάθε $k \geq 0$. Έστω $x = a^\mu$, $y = a^\nu$ με $\nu \neq 0$ και $z = a^\xi$. Έτσι για κάθε $k \geq 0$ θα έχουμε $a^\mu a^{k\nu} a^\xi \in L$ δηλαδή για κάθε $k \geq 0$ ο αριθμός $\mu + k\nu + \xi$ είναι πρώτος. Αυτό σημαίνει πως ο αριθμός $\mu + \xi$ (για $k = 0$) είναι πρώτος. Θέτουμε $k = \mu + \xi$ οπότε ο αριθμός $\mu + (\mu + \xi)\nu + \xi = (\nu + 1)(\mu + \xi)$ είναι πρώτος, που φυσικά είναι άτοπο. Συνεπώς η $L \notin \mathrm{Rec}(\{a\})$.

Ασκήσεις

1) Για οποιοδήποτε αλφάβητο A, να αποδείξετε ότι η γλώσσα A^* είναι αναγνωρίσιμη.

2) Δίνονται τα CFA $\mathcal{A} = (\{q_0, q_1, q_2\}, \{a, b\}, q_0, \delta_{\mathcal{A}}, \{q_2\})$ με

$\delta_{\mathcal{A}}$	a	b
q_0	q_1	q_2
q_1	q_0	q_1
q_2	q_2	q_0

και $\mathcal{B} = (\{p_0, p_1, p_2\}, \{a, b\}, p_0, \delta_{\mathcal{B}}, \{p_0, p_2\})$ με

$\delta_{\mathcal{B}}$	a	b
p_0	p_1	p_0
p_1	p_2	p_1
p_2	p_2	p_2

Να βρείτε και να σχεδιάσετε το CFA που αναγνωρίζει α) τη τομή των γλωσσών των δύο CFA, β) την ένωση των γλωσσών των δύο CFA, γ) το συμπλήρωμα της γλώσσας του CFA $\mathcal{A}$ και δ) το συμπλήρωμα της γλώσσας του CFA $\mathcal{B}$.

3) Δίνεται το αλφάβητο $A = \{a, b\}$. Να αποδείξετε ότι οι γλώσσες

$$L_1 = \{a^n b^m \mid n \geq m \geq 0\} \quad \text{και} \quad L_2 = \{a^n b^m \mid m \geq n \geq 0\}$$

δεν είναι αναγνωρίσιμες.

4) Δίνεται το αλφάβητο $A = \{a, b, c, d, e, f, g\}$. Να αποδείξετε ότι οι γλώσσες

   i) $L_1 = \{abc^n agebd^n f \mid n \geq 0\}$,

   ii) $L_2 = \{d^3 f^2 a^4 bg^n ad^3 eba^n gd^2 \mid n \geq 0\}$,

   iii) $L_3 = \{d^3 a^4 bg^n ad^3 eba^n gd^2 d^n ab \mid n \geq 0\}$,

   iv) $L_3 = \{a^{10} d^2 f^4 b^2 f^n ad^3 eba^n gfd^2 d^n ab^n d \mid n \geq 0\}$,

   δεν είναι αναγνωρίσιμες.

5) Δίνεται το αλφάβητο $A = \{a, b, c, d\}$. Να εξετάσετε αν η γλώσσα

$$L = \{b^3 a^{n^m} c^2 b^3 d^{n^m} \mid n \geq 0, m > 0\}$$

   είναι αναγνωρίσιμη ή όχι.

6) Δίνεται το αλφάβητο $A = \{a, b\}$. Για κάθε λέξη $w \in A^*$ συμβολίζουμε με $|w|_a$ (αντίστοιχα $|w|_b$) το πλήθος των εμφανίσεων του a (αντίστοιχα του b) στη λέξη w. Να αποδείξετε ότι οι γλώσσες

$$L_1 = \{w \in A^* \mid |w|_a = |w|_b\},$$

$$L_2 = \{w \in A^* \mid |w|_a = 3|w|_b\}$$

   δεν είναι αναγνωρίσιμες.

7) Να αποδείξετε, χρησιμοποιώντας την Πρόταση 7, ότι η γλώσσα του Παραδείγματος 14 δεν είναι αναγνωρίσιμη.

8) Δίνεται το αλφάβητο $A = \{a\}$. Να αποδείξετε ότι η γλώσσα $L = \{a^{2^n} \mid n \geq 0\}$ δεν είναι αναγνωρίσιμη.

9) Δίνεται το αλφάβητο $A = \{a\}$. Να αποδείξετε ότι η γλώσσα $L = \{a^{n^2} \mid n \geq 0\}$ δεν είναι αναγνωρίσιμη.

10) Δίνεται αλφάβητο A και γλώσσα $L \in \mathrm{Rec}(A)$. Να δείξετε ότι υπάρχει φυσικός αριθμός $n > 0$ τέτοιος ώστε, αν $|w| > n$ για κάποια λέξη $w \in L$, τότε η L είναι άπειρη γλώσσα.

11) Δίνεται αλφάβητο A και γλώσσα $L \in \mathrm{Rec}(A)$. Να δείξετε ότι υπάρχει φυσικός αριθμός $n > 0$ τέτοιος ώστε, αν $w \in L$ με $|w| > n$, τότε η w γράφεται $w = xyz$ με $|xy| \leq n$, $y \neq \varepsilon$ και $xy^k z \in L$ για κάθε $k \geq 0$.

12) Δίνεται αλφάβητο A και γλώσσα $L \in \mathrm{Rec}(A)$. Αν η L είναι άπειρη, να δείξετε ότι υπάρχουν λέξεις $x, y, z \in A^*$ τέτοιες ώστε $y \neq \varepsilon$ και $xy^kz \in L$ για κάθε $k \geq 0$.

13) Για οποιοδήποτε αλφάβητο A, να αποδείξετε ότι κάθε πεπερασμένη γλώσσα $L \subseteq A^*$ είναι αναγνωρίσιμη.

14) Να βρείτε το λάθος στον παρακάτω συλλογισμό: *"Για κάθε $n \geq 0$ η γλώσσα $\{a^n b^n\}$ είναι, σύμφωνα με την Άσκηση 13, αναγνωρίσιμη. Συνεπώς, από τη Πρόταση 6, η γλώσσα $\{a^n b^n \mid n \geq 0\}$ είναι αναγνωρίσιμη."*

15) Δίνεται το αλφάβητο $A = \{a, b\}$. Να αποδείξετε ότι η γλώσσα

$$L = \{w^2 \mid w \in A^*\}$$

δεν είναι αναγνωρίσιμη.

16) Δίνεται το αλφάβητο $A = \{a, b\}$. Να αποδείξετε ότι η γλώσσα

$$L = \{w^3 \mid w \in A^*\}$$

δεν είναι αναγνωρίσιμη.

17) Δίνεται το αλφάβητο $A = \{a, b\}$. Να αποδείξετε ότι η γλώσσα

$$L = \{w \in A^* \mid w = w^\rho\}$$

δεν είναι αναγνωρίσιμη.

18) Δίνεται το αλφάβητο $A = \{a\}$. Να αποδείξετε ότι η γλώσσα

$$L = \{a^{p+1} \mid p \text{ πρώτος αριθμός }\}$$

δεν είναι αναγνωρίσιμη.

19) Δίνεται το αλφάβητο $A = \{a\}$ και θετικός ακέραιος m. Να αποδείξετε ότι η γλώσσα

$$L = \{a^{p+m} \mid p \text{ πρώτος αριθμός }\}$$

δεν είναι αναγνωρίσιμη.

20) Δίνεται το αλφάβητο $A = \{a, b\}$. Να αποδείξετε ότι η γλώσσα

$$L = \{a^p b \mid p \text{ πρώτος αριθμός } \}$$

δεν είναι αναγνωρίσιμη.

21) Δίνεται το αλφάβητο $A = \{a, b, c\}$. Να αποδείξετε ότι η γλώσσα

$$L = \{b a^p c \mid p \text{ πρώτος αριθμός } \}$$

δεν είναι αναγνωρίσιμη.

22) Δίνεται το αλφάβητο $A = \{a, b, c\}$. Να αποδείξετε ότι η γλώσσα

$$L = \{b^2 a^p c^3 \mid p \text{ πρώτος αριθμός } \}$$

δεν είναι αναγνωρίσιμη.

Κεφάλαιο 5

Deterministic και non-deterministic πεπερασμένα αυτόματα

Στο κεφάλαιο αυτό θα μελετήσουμε δύο νέους τύπους αυτομάτων, τα deterministic και τα non-deterministic πεπερασμένα αυτόματα. Θα δείξουμε ότι αν και φαινομενικά πιο ισχυρά μοντέλα από τα CFA, αναγνωρίζουν ακριβώς την κλάση των αναγνωρίσιμων γλωσσών. Με τη βοήθεια των μοντέλων αυτών θα αποδείξουμε ότι η κλάση των αναγνωρίσιμων γλωσσών είναι κλειστή με την πράξη της παράθεσης και της θήκης.
Ξεκινούμε με τα deterministic πεπερασμένα αυτόματα.

Ορισμός 5 *Ένα deterministic πεπερασμένο αυτόματο (deterministic finite automaton, σύντομα* DFA[1]*) είναι μια πεντάδα της μορφής* $\mathcal{A} = (Q, A, q_0, \delta, F)$ *όπου*

- *Q είναι το πεπερασμένο σύνολο των καταστάσεων,*

- *A είναι το αλφάβητο εισόδου,*

- *$q_0 \in Q$ είναι η αρχική κατάσταση,*

- *$\delta : Q \times A \to Q$ είναι μια μερική απεικόνιση που περιγράφει τη λειτουργία το αυτομάτου, και*

- *$F \subseteq Q$ είναι το σύνολο των τελικών καταστάσεων.*

Το γεγονός ότι η δ είναι μερική απεικόνιση σημαίνει ότι μπορεί να υπάρχουν ζεύγη $(q, a) \in Q \times A$ για τα οποία η $\delta(q, a)$ να μην ορίζεται. Στην περίπτωση αυτή γράφουμε $\delta(q, a) = \emptyset$. Αυτό, για την λειτουργία του DFA, σημαίνει πως αν βρίσκεται στην κατάσταση $q \in Q$ και διαβάζει το γράμμα $a \in A$, τότε η λειτουργία

[1] Ο όρος θα χρησιμοποιείται για τον ενικό και πληθυντικό αριθμό.

του σταματάει στην κατάσταση q.

Η $\delta : Q \times A \to Q$ επεκτείνεται επαγωγικά (στο μήκος των λέξεων) όπως στην περίπτωση του CFA. Μια λέξη $w \in A^*$ *αναγνωρίζεται* από το $\mathcal{A}$ αν $\delta^*(q_0, w) \in F$. Η *γλώσσα* (ή *συμπεριφορά*) του $\mathcal{A}$ που συμβολίζεται με $L(\mathcal{A})$ (ή $|\mathcal{A}|$) ορίζεται όπως στα CFA, δηλαδή

$$L(\mathcal{A}) = \{w \in A^* \mid \delta^*(q_0, w) \in F\}.$$

Για να βρούμε τη γλώσσα ενός DFA κατασκευάζουμε και λύνουμε, όπως και στη περίπτωση του CFA, το γραμμικό σύστημα εξισώσεων που προκύπτει από το DFA.

Δύο πεπερασμένα αυτόματα $\mathcal{A}$ και $\mathcal{B}$ ονομάζονται *ισοδύναμα*, αν $L(\mathcal{A}) = L(\mathcal{B})$.

Καθώς κάθε απεικόνιση είναι μια ειδική περίπτωση μερικής απεικόνισης, είναι φανερό ότι κάθε CFA μπορεί να θεωρηθεί σαν DFA. Αυτό σημαίνει ότι οι αναγνωρίσιμες γλώσσες αναγνωρίζονται και από τα DFA. Στη συνέχεια θα δείξουμε ότι από κάθε DFA μπορούμε να κατασκευάσουμε ένα ισοδύναμο CFA.

Πρόταση 8 *Για κάθε* DFA $\mathcal{A}$ *μπορούμε να κατασκευάσουμε ένα ισοδύναμο* CFA $\mathcal{A}'$.

Απόδειξη Ας είναι $\mathcal{A} = (Q, A, q_0, \delta, F)$ ένα DFA. Θεωρούμε το CFA $\mathcal{A}' = (Q \cup \{\overline{q}\}, A, q_0, \delta', F)$ όπου $\overline{q}$ είναι μια νέα κατάσταση που δεν ανήκει στο Q. Η απεικόνιση δ' ορίζεται για κάθε $q \in Q \cup \{\overline{q}\}$, $a \in A$ ως εξής:

$$\delta'(q, a) = \begin{cases} \delta(q, a) & \text{αν } q \in Q \text{ και } \delta(q, a) \neq \emptyset \\ \overline{q} & \text{αν } q \in Q \text{ και } \delta(q, a) = \emptyset \\ \overline{q} & \text{αν } q = \overline{q}. \end{cases}$$

Ας είναι $w = a_1 a_2 \ldots a_n \in L(\mathcal{A})$. Τότε υπάρχει επιτυχής διαδρομή

$$\to q_0 \xrightarrow{a_1} q_1 \xrightarrow{a_2} q_2 \ldots q_{n-1} \xrightarrow{a_n} q_n \in F \quad (1)$$

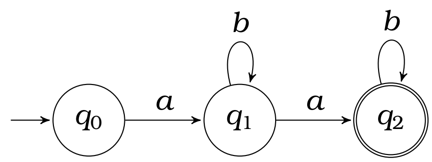
του $\mathcal{A}$ στη w, δηλαδή $\delta^*(q_0, w) \in F$. Αυτό σημαίνει ότι η $\overline{q}$ δεν εμφανίζεται στην (1). Συνεπώς η (1) είναι επιτυχής διαδρομή και στο CFA $\mathcal{A}'$, οπότε η $w \in L(\mathcal{A}')$. Άρα $L(\mathcal{A}) \subseteq L(\mathcal{A}')$. Αντίτροφα, αν η $w \in L(\mathcal{A}')$, τότε υπάρχει επιτυχής διαδρομή

$$\to q_0 \xrightarrow{a_1} q_1' \xrightarrow{a_2} q_2' \ldots q_{n-1}' \xrightarrow{a_n} q_n' \in F \quad (2)$$

του $\mathcal{A}'$ στην w. Από την κατασκευή του $\mathcal{A}'$, η επιτυχής διαδρομή (2) δεν μπορεί να περιέχει την κατάσταση $\overline{q}$, γιατί αν την περιείχε τότε θα ήταν $q_n' = \overline{q} \notin F$ οπότε η διαδρομή (2) δεν θα ήταν επιτυχής. Φανερά λοιπόν η (2) είναι και επιτυχής διαδρομή του DFA $\mathcal{A}$. Συνεπώς $w \in L(\mathcal{A})$ οπότε $L(\mathcal{A}') \subseteq L(\mathcal{A})$. Άρα $L(\mathcal{A}') = L(\mathcal{A})$, και τα αυτόματα $\mathcal{A}$ και $\mathcal{A}'$ είναι ισοδύναμα. □

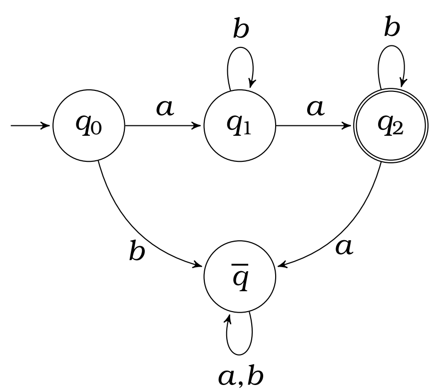
Παράδειγμα 16 *Δίνεται το* DFA $\mathcal{A} = (\{q_0, q_1, q_2\}, A, q_0, \delta, \{q_2\})$ *με*

δ	a	b
q_0	q_1	$\emptyset$
q_1	q_2	q_1
q_2	$\emptyset$	q_2.



Σύμφωνα με τη Πρόταση 8, το DFA $\mathcal{A}' = (\{q_0, q_1, q_2, \overline{q}\}, A, q_0, \delta', \{q_2\})$ *με*

δ'	a	b
q_0	q_1	$\overline{q}$
q_1	q_2	q_1
q_2	$\overline{q}$	q_2
$\overline{q}$	$\overline{q}$	$\overline{q}$



αναγνωρίζει την ίδια γλώσσα με το $\mathcal{A}$.

Στη συνέχεια θα ασχοληθούμε με τα NFA.

Ορισμός 6 *Ένα non-deterministic πεπερασμένο αυτόματο, (non-deterministic finite automaton σύντομα* NFA[2]*) είναι μια πεντάδα της μορφής* $\mathcal{A} = (Q, A, I, \delta, F)$ *όπου*

- *Q είναι το πεπερασμένο σύνολο των καταστάσεων,*

[2]Ο όρος θα χρησιμοποιείται για τον ενικό και πληθυντικό αριθμό.

- *A είναι το αλφάβητο εισόδου,*

- *$I \subseteq Q$ είναι το σύνολο των αρχικών καταστάσεων,*

- *$\delta : Q \times A \to \mathcal{P}(Q)$ είναι η απεικόνιση που περιγράφει τη λειτουργία το αυτομάτου, και*

- *$F \subseteq Q$ είναι το σύνολο των τελικών καταστάσεων.*

Ο ορισμός της απεικόνισης δ σημαίνει πως αν το NFA είναι στην κατάσταση $q \in Q$ και διαβάζει το γράμμα $a \in A$ τότε έχει τη δυνατότητα να μεταβεί σε *οποιαδήποτε* από τις καταστάσεις του συνόλου $\delta(q, a)$ *αλλά όχι σε όλες μαζί.* Θα πρέπει εδώ να σημειώσουμε ότι μπορεί $\delta(q, a) = \emptyset$. Στην περίπτωση αυτή, αν δηλαδή το NFA είναι στην κατάσταση $q \in Q$ και διαβάζει το γράμμα $a \in A$, τότε η λειτουργία του σταματάει στην κατάσταση q.

Η δ επεκτείνεται σε μία απεικόνιση $\delta^* : Q \times A^* \to \mathcal{P}(Q)$, επαγωγικά στο μήκος των λέξεων, ως εξής:

- $\delta^*(q, \varepsilon) = \{q\}$,

- $\delta^*(q, wa) = \bigcup_{q' \in \delta^*(q,w)} \delta(q', a)$

για κάθε $q \in Q, w \in A^*, a \in A$.

Η λέξη $w \in A^*$ *αναγνωρίζεται* από το NFA $\mathcal{A}$ αν υπάρχει αρχική κατάσταση $q_0 \in I$ έτσι ώστε $\delta^*(q_0, w) \cap F \neq \emptyset$. Η γλώσσα όλων των λέξεων που αναγνωρίζονται από το $\mathcal{A}$ ονομάζεται *γλώσσα* (ή *συμπεριφορά*) του $\mathcal{A}$ και συμβολίζεται με $L(\mathcal{A})$ (ή με $|\mathcal{A}|$), δηλαδή

$$L(\mathcal{A}) = \{w \in A^* \mid \text{ υπάρχει } q_0 \in I \text{ έτσι ώστε } \delta^*(q_0, w) \cap F \neq \emptyset\}.$$

Για να βρούμε τη γλώσσα ενός NFA κατασκευάζουμε και λύνουμε, όπως και στη περίπτωση του CFA, το γραμμικό σύστημα εξισώσεων που προκύπτει από την απεικόνιση δ. Η γλώσσα του NFA προκύπτει από την ένωση των συνιστωσών της λύσης του συστήματος που αντιστοιχούν στις αρχικές καταστάσεις του NFA.

Παράδειγμα 17 *Θεωρούμε το* NFA $\mathcal{A} = (\{q_0, q_1, q_2\}, \{a, b, c\}, \{q_0, q_1\}, \delta, \{q_1, q_2\})$ *με*

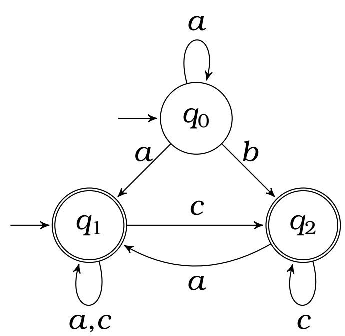
δ	a	b	c
q_0	$\{q_0, q_1\}$	$\{q_2\}$	$\emptyset$
q_1	$\{q_1\}$	$\emptyset$	$\{q_1, q_2\}$
q_2	$\{q_1\}$	$\emptyset$	$\{q_2\}$.

Το σύστημα των εξισώσεων που προκύπτει από το αυτόματο είναι

$$\begin{aligned} X_0 &= aX_0 \cup aX_1 \cup bX_2 \\ X_1 &= (a \cup c)X_1 \cup cX_2 \cup \varepsilon \\ X_2 &= aX_1 \cup cX_2 \cup \varepsilon. \end{aligned}$$

Λύνουμε το σύστημα (η λύση αφήνεται σαν άσκηση στον αναγνώστη) και η ζητούμενη γλώσσα του NFA *είναι η* $L(\mathcal{A}) = X_0 \cup X_1$.

Το γράφημα του NFA *είναι*



Στη συνέχεια θα δείξουμε ότι τα NFA *δεν* είναι στην πραγματικότητα πιο ισχυρά μοντέλα από τα CFA. Καταρχήν, να παρατηρήσουμε ότι κάθε CFA είναι μια ειδική περίπτωση ενός NFA με μία αρχική κατάσταση, και την απεικόνιση δ να προσαρτά σε κάθε ζεύγος κατάστασης και γράμματος μία μοναδική κατάσταση. Ισχύει το επόμενο σημαντικό αποτέλεσμα.

Πρόταση 9 *Για κάθε* NFA $\mathcal{A}$ *μπορούμε να κατασκευάσουμε ένα ισοδύναμο* CFA $\mathcal{A}'$.

Απόδειξη Ας είναι $\mathcal{A} = (Q, A, I, \delta, F)$ ένα NFA. Θεωρούμε το CFA $\mathcal{A}' = (\mathcal{P}(Q), A, I, \delta', F')$ όπου η δ' ορίζεται από τη σχέση

$$\delta'(P, a) = \bigcup_{q \in P} \delta(q, a)$$

για κάθε $P \in \mathcal{P}(Q)$, $a \in A$, και οι τελικές καταστάσεις είναι

$$F' = \{P \in \mathcal{P}(Q) \mid P \cap F \neq \emptyset\}.$$

Αρχικά θα δείξουμε ότι

$$\delta'^*(P, w) = \bigcup_{q \in P} \delta^*(q, w)$$

για κάθε $P \in \mathcal{P}(Q)$, $w \in A^*$.
Θα χρησιμοποιήσουμε επαγωγή στο μήκος της λέξης w. Πράγματι, για $|w| = 0$ έχουμε $w = \varepsilon$ οπότε $\delta'^*(P, \varepsilon) = P$ και $\bigcup_{q \in P} \delta^*(q, \varepsilon) = \bigcup_{q \in P} \{q\} = P$. Υποθέτουμε ότι

η πρόταση ισχύει για όλες τις λέξεις με μήκος $\leq k$ και έστω $w \in A^*$ με μήκος $|w| = k+1$. Τότε $w = ua$ με $u \in A^*, a \in A$ και $|u| = k$. Έχουμε

$$
\begin{aligned}
\delta'^*(P, w) &= \delta'^*(P, ua) \\
&= \delta'(\delta'^*(P, u), a) \\
&= \delta'\left(\bigcup_{q \in P} \delta^*(q, u), a\right) && \text{από την υπόθεση της επαγωγής} \\
&= \bigcup_{q' \in \bigcup_{q \in P} \delta^*(q,u)} \delta(q', a) && \text{από τον ορισμό της } \delta' \\
&= \bigcup_{q \in P} \bigcup_{q' \in \delta^*(q,u)} \delta(q', a) \\
&= \bigcup_{q \in P} \delta^*(q, ua) && \text{από τον ορισμό της } \delta^* \\
&= \bigcup_{q \in P} \delta^*(q, w)
\end{aligned}
$$

όπως το θέλαμε.

Για κάθε λέξη $w \in A^*$ έχουμε

$$
\begin{aligned}
w \in L(\mathcal{A}') &\iff \delta'^*(I, w) \in F' \\
&\iff \bigcup_{q \in I} \delta^*(q, w) \in F' \\
&\iff \bigcup_{q \in I} \delta^*(q, w) \cap F \neq \emptyset \\
&\iff \text{υπάρχει } q_0 \in I \text{ τέτοιο ώστε } \delta^*(q_0, w) \cap F \neq \emptyset \\
&\iff w \in L(\mathcal{A})
\end{aligned}
$$

δηλαδή $L(\mathcal{A}') = L(\mathcal{A})$, και συνεπώς το CFA $\mathcal{A}'$ είναι ισοδύναμο με το NFA $\mathcal{A}$. □

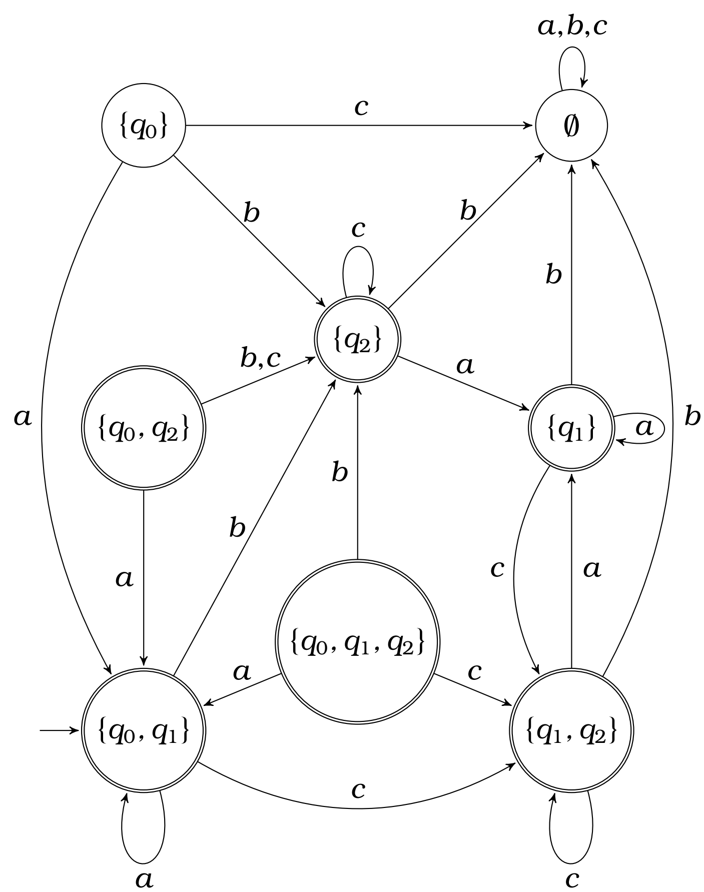
Παράδειγμα 18 *Θα κατασκευάσουμε το* CFA $\mathcal{A}'$ *που είναι ισοδύναμο με το* NFA $\mathcal{A}$ *του Παραδείγματος 17.*

Σύμφωνα με τη παραπάνω πρόταση, έχουμε $\mathcal{A}' = (\mathcal{P}(\{q_0, q_1, q_2\}), \{a, b, c\}, \{q_0, q_1\}, \delta', F')$ *όπου* $\mathcal{P}(\{q_0, q_1, q_2\}) = \{\emptyset, \{q_0\}, \{q_1\}, \{q_2\}, \{q_0, q_1\}, \{q_0, q_2\}, \{q_1, q_2\}, Q\}$ *και* $F' =$

$\{\{q_1\}, \{q_2\}, \{q_1, q_2\}, \{q_0, q_1\}, \{q_0, q_2\}, Q\}$ *ενώ η* δ' *δίνεται από τον πίνακα*

δ	a	b	c
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{q_0\}$	$\{q_0, q_1\}$	$\{q_2\}$	$\emptyset$
$\{q_1\}$	$\{q_1\}$	$\emptyset$	$\{q_1, q_2\}$
$\{q_2\}$	$\{q_1\}$	$\emptyset$	$\{q_2\}$
$\{q_0, q_1\}$	$\{q_0, q_1\}$	$\{q_2\}$	$\{q_1, q_2\}$
$\{q_0, q_2\}$	$\{q_0, q_1\}$	$\{q_2\}$	$\{q_2\}$
$\{q_1, q_2\}$	$\{q_1\}$	$\emptyset$	$\{q_1, q_2\}$
$\{q_0, q_1, q_2\}$	$\{q_0, q_1\}$	$\{q_2\}$	$\{q_1, q_2\}$.

Το γράφημα του CFA $\mathcal{A}'$ *είναι*



Είναι φανερό ότι τα NFA δεν αποτελούν ένα “καλό” μοντέλο για την υλοποίηση αλγορίθμων, καθώς το κάθε βήμα ενός αλγορίθμου πρέπει να είναι απολύτως προσδιορισμένο. Εντούτοις, το αποτέλεσμα της Πρότασης 9 μας επιτρέπει να χρησιμοποιούμε NFA για την αναγνώριση γλωσσών. Τα NFA είναι “χαμηλότερης πολυπλοκότητας" από τα αντίστοιχα πλήρη. Πράγματι, από τη Πρόταση 9, είναι φανερό ότι αν για την αναγνώριση μιας γλώσσας απαιτείται ένα NFA με n καταστάσεις, τότε το αντίστοιχο ισοδύναμο CFA θα έχει 2^n καταστάσεις. Για να γίνει αυτό καλύτερα αντιληπτό, καλούμε τον αναγνώστη να κατασκευάσει ένα NFA που αναγνωρίζει όλες τις λέξεις, από το αλφάβητο $A = \{a, b, c, d\}$, που περιέχουν την υπολέξη da^2c^3 ή την υπολέξη c^3d. Στη συνέχεια να προσπαθήσει να κατασκευάσει ένα CFA που αναγνωρίζει τη ίδια γλώσσα.

Στη συνέχεια θα δείξουμε ότι η κλάση των αναγνωρίσιμων γλωσσών είναι κλειστή με την πράξη της παράθεσης και της θήκης. Για το σκοπό αυτό θα χρειαστούμε την έννοια του κανονικοποιημένου αυτομάτου. Συγκεκριμένα, ένα NFA $\mathcal{A} = (Q, A, I, \delta, F)$ θα ονομάζεται *κανονικοποιημένο* αν $I = \{q_{in}\}$, $F = \{q_t\}$, $q_{in} \neq q_t$ και ισχύουν οι συνθήκες

- $q_{in} \notin \delta(q, a)$, για κάθε $q \in Q, a \in A$,
- $\delta(q_t, a) = \emptyset$, για κάθε $a \in A$.

Στη περίπτωση αυτή γράφουμε $\mathcal{A} = (Q, A, q_{in}, \delta, q_t)$.

Πρόταση 10 *Για κάθε* NFA $\mathcal{A}$ *μπορούμε να κατασκευάσουμε ένα κανονικοποιημένο* NFA $\overline{\mathcal{A}}$ *τέτοιο ώστε* $L(\overline{\mathcal{A}}) = L(\mathcal{A}) \setminus \{\varepsilon\}$.

Απόδειξη Ας είναι $\mathcal{A} = (Q, A, I, \delta, F)$ ένα NFA. Θεωρούμε δύο νέες καταστάσεις q_{in}, q_t που δεν ανήκουν στο σύνολο Q και το NFA $\overline{\mathcal{A}} = (Q \cup \{q_{in}, q_t\}, A, q_{in}, \overline{\delta}, q_t)$ όπου η απεικόνιση $\overline{\delta}$ ορίζεται για κάθε $q \in Q \cup \{q_{in}, q_t\}, a \in A$ ως εξής:

$$\overline{\delta}(q, a) = \begin{cases} \delta(q, a) & \text{αν } q \in Q \text{ και } \delta(q, a) \cap F = \emptyset \\ \delta(q, a) \cup \{q_t\} & \text{αν } q \in Q \text{ και } \delta(q, a) \cap F \neq \emptyset \\ \bigcup\limits_{q' \in I} \delta(q', a) \cup P & \text{αν } q = q_{in}, \text{ όπου } P = \{q_t\} \text{ αν } \bigcup\limits_{q' \in I} \delta(q', a) \cap F \neq \emptyset, \\ & \qquad\qquad\qquad \text{και } P = \emptyset \text{ διαφορετικά} \\ \emptyset & \text{αν } q = q_t. \end{cases}$$

Από τον τρόπο ορισμού του, το $\overline{\mathcal{A}}$ είναι προφανώς κανονικοποιμένο. Θεωρούμε μια λέξη $w \in L(\mathcal{A}) \setminus \{\varepsilon\}$. Αν $w = a \in A$, τότε θα υπάρχει $q_0 \in I$ έτσι ώστε $\delta(q_0, a) \cap F \neq \emptyset$. Από τον ορισμό της $\overline{\delta}$ έχουμε ότι $q_t \in \overline{\delta}(q_{in}, a)$ και συνεπώς $w \in L(\overline{\mathcal{A}})$. Αν $w = a_1a_2 \ldots a_n$ με $n > 1$, τότε θα υπάρχει επιτυχής διαδρομή

$$\rightarrow q_0 \xrightarrow{a_1} q_1 \xrightarrow{a_2} q_2 \ldots q_{n-1} \xrightarrow{a_n} q_n \in F$$

του $\mathcal{A}$ στην w. Από τον ορισμό της $\overline{\delta}$, θα υπάρχει διαδρομή

$$\rightarrow q_{in} \xrightarrow{a_1} q_1 \xrightarrow{a_2} q_2 \ldots q_{n-1} \xrightarrow{a_n} q_t$$

του $\overline{\mathcal{A}}$ στην w η οποία είναι επιτυχής. Άρα $w \in L(\overline{\mathcal{A}})$ και συνεπώς $L(\mathcal{A}) \setminus \{\varepsilon\} \subseteq L(\overline{\mathcal{A}})$.

Αντίστροφα ας είναι $w \in L(\overline{\mathcal{A}})$. Καθώς $q_{in} \neq q_t$ θα έχουμε $w \neq \varepsilon$. Έστω ότι $w = a \in A$ που σημαίνει ότι $q_t \in \overline{\delta}(q_{in}, a)$. Από τον τρόπο ορισμού της $\overline{\delta}$ συμπεραίνουμε ότι υπάρχει $q_0 \in I$ έτσι ώστε $\delta(q_0, a) \cap F \neq \emptyset$, δηλαδή $w \in L(\mathcal{A}) \setminus \{\varepsilon\}$. Έστω τώρα ότι $w = a_1 a_2 \ldots a_n$ με $n > 1$, και

$$\to q_{in} \overset{a_1}{\to} q_1 \overset{a_2}{\to} q_2 \ldots q_{n-1} \overset{a_n}{\to} q_t$$

επιτυχής διαδρομή του $\overline{\mathcal{A}}$ στην w. Από τον τρόπο ορισμού της $\overline{\delta}$, θα υπάρχουν $q_0 \in I, q_n \in F$ και διαδρομή

$$\to q_0 \overset{a_1}{\to} q_1 \overset{a_2}{\to} q_2 \ldots q_{n-1} \overset{a_n}{\to} q_n \in F$$

του $\mathcal{A}$ στην w, η οποία είναι προφανώς επιτυχής. Άρα $w \in L(\mathcal{A}) \setminus \{\varepsilon\}$, που σημαίνει ότι $L(\overline{\mathcal{A}}) \subseteq L(\mathcal{A}) \setminus \{\varepsilon\}$ και η απόδειξή μας τελείωσε. □

Με τη βοήθεια της Πρότασης 10, θα αποδείξουμε περαιτέρω ιδιότητες για τη κλάση $\mathrm{Rec}(A)$.

Πρόταση 11 *Αν $L, M \in \mathrm{Rec}(A)$, τότε $LM \in \mathrm{Rec}(A)$.*

Απόδειξη Διακρίνουμε τις παρακάτω περιπτώσεις.

α) $\varepsilon \notin L \cup M$. Τότε από την Πρόταση 10, υπάρχουν κανονικοποιημένα NFA $\mathcal{A} = (Q, A, q_{in}, \delta_{\mathcal{A}}, q_t)$ και $\mathcal{B} = (P, A, p_{in}, \delta_{\mathcal{B}}, p_t)$ που αναγνωρίζουν τις γλώσσες L και M, αντίστοιχα. Χωρίς περιορισμό της γενικότητας[3] θεωρούμε ότι $Q \cap P = \emptyset$. Θεωρούμε το NFA $C = ((Q \cup P) \setminus \{p_{in}\}, A, q_{in}, \delta_C, p_t)$ με την απεικόνιση δ_C να ορίζεται για κάθε $r \in (Q \cup P) \setminus \{p_{in}\}, a \in A$ ως εξής:

$$\delta_C(r, a) = \begin{cases} \delta_{\mathcal{A}}(r, a) & \text{αν } r \in Q \setminus \{q_t\} \\ \delta_{\mathcal{B}}(p_{in}, a) & \text{αν } r = q_t \\ \delta_{\mathcal{B}}(r, a) & \text{αν } r \in P \setminus \{p_{in}\}. \end{cases}$$

Ας είναι $w = a_1 a_2 \ldots a_n \in LM$, δηλαδή $w = w_1 w_2$ με $w_1 = a_1 \ldots a_m \in L$ και $w_2 = a_{m+1} \ldots a_n \in M$. Τότε υπάρχει επιτυχής διαδρομή

$$\to q_{in} \overset{a_1}{\to} q_1 \ldots q_{m-1} \overset{a_m}{\to} q_t$$

του $\mathcal{A}$ στην w_1, και επιτυχής διαδρομή

$$\to p_{in} \overset{a_{m+1}}{\to} p_1 \ldots p_{n-(m+1)} \overset{a_n}{\to} p_t$$

του $\mathcal{B}$ στην w_2.
Από τον ορισμό της δ_C, υπάρχει η διαδρομή

$$\to q_{in} \overset{a_1}{\to} q_1 \ldots q_{m-1} \overset{a_m}{\to} q_t \overset{a_{m+1}}{\to} p_1 \ldots p_{n-(m+1)} \overset{a_n}{\to} p_t$$

[3] Αν υπάρχουν κοινές καταστάσεις μετονομάζουμε το ένα από τα δύο σύνολα καταστάσεων.

του C στην w, η οποία είναι προφανώς επιτυχής και συνεπώς $w \in L(C)$, δηλαδή $LM \subseteq L(C)$.

Αντίστροφα, ας είναι $w = a_1 \dots a_n \in L(C)$ και

$$\rightarrow q_{in} \xrightarrow{a_1} r_1 \dots r_{n-1} \xrightarrow{a_n} p_t$$

επιτυχής διαδρομή του C στην w. Εφόσον η παραπάνω διαδρομή ξεκινά από κατάσταση του NFA $\mathcal{A}$ και καταλήγει σε κατάσταση του NFA $\mathcal{B}$, από τον ορισμό της δ_C, προκύπτει ότι υπάρχει ένας δείκτης $1 \leq m \leq n-1$ τέτοιος ώστε $r_1, \dots, r_m \in Q$ με $r_m = q_t$ και $r_{m+1}, \dots, r_{n-1} \in P$ δηλαδή

$$\rightarrow q_{in} \xrightarrow{a_1} r_1 \dots r_{m-1} \xrightarrow{a_m} q_t \xrightarrow{a_{m+1}} r_{m+1} \dots r_{n-1} \xrightarrow{a_n} p_t.$$

Λαμβάνοντας υπόψη ακόμη μία φορά τον ορισμό της δ_C, στα ζεύγη της μορφής (q_t, a), συνάγουμε ότι από τη παραπάνω διαδρομή προκύπτουν οι διαδρομές

$$\rightarrow q_{in} \xrightarrow{a_1} r_1 \dots r_{m-1} \xrightarrow{a_m} q_t$$

και

$$\rightarrow p_{in} \xrightarrow{a_{m+1}} r_{m+1} \dots r_{n-1} \xrightarrow{a_n} p_t$$

των NFA $\mathcal{A}$ και $\mathcal{B}$ στις $a_1 \dots a_m$ και $a_{m+1} \dots a_n$, αντίστοιχα.
Έτσι $a_1 \dots a_m \in L$ και $a_{m+1} \dots a_n \in M$, δηλαδή $w = a_1 \dots a_n \in LM$, και συνεπώς $L(C) \subseteq LM$. Άρα η γλώσσα LM αναγνωρίζεται από το NFA C που σημαίνει ότι $LM \in \mathrm{Rec}(A)$.

β) $\varepsilon \in L$ και $\varepsilon \notin M$. Τότε $LM = (L \setminus \{\varepsilon\})M \cup M$ και το αποτέλεσμά μας προκύπτει από το α) και τις Προτάσεις 10 και 6.

γ) $\varepsilon \notin L$ και $\varepsilon \in M$. Ισχύει $LM = L(M \setminus \{\varepsilon\}) \cup L$ και συνεχίζουμε όπως στο β).

δ) $\varepsilon \in L \cap M$. Στην περίπτωση αυτή έχουμε $LM = (L \setminus \{\varepsilon\})(M \setminus \{\varepsilon\}) \cup (L \setminus \{\varepsilon\}) \cup (M \setminus \{\varepsilon\}) \cup \{\varepsilon\}$, και το αποτέλεσμά μας προκύπτει από το α), τις Προτάσεις 10, 6 και το γεγονός ότι η γλώσσα $\{\varepsilon\}$ αναγνωρίζεται από ένα NFA με μία κατάσταση (που είναι αρχική και τελική) και κενό αλφάβητο εισόδου. □

Πρόταση 12 *Αν* $L \in \mathrm{Rec}(A)$, *τότε* $L^* \in \mathrm{Rec}(A)$.

Απόδειξη Ας είναι $\mathcal{A} = (Q, A, q_{in}, \delta, q_t)$ ένα κανονικοποιημένοNFA που αναγνωρίζει τη γλώσσα $L \setminus \{\varepsilon\}$. Θεωρούμε το NFA $\mathcal{A}' = (Q \setminus \{q_t\}, A, q_{in}, \delta', \{q_{in}\})$ όπου η απεικόνιση δ' ορίζεται για κάθε $q \in Q \setminus \{q_t\}, a \in A$ ως εξής:

$$\delta'(q, a) = \begin{cases} \delta(q, a) & \text{αν } q_t \notin \delta(q, a) \\ (\delta(q, a) \setminus \{q_t\}) \cup \{q_{in}\} & \text{αν } q_t \in \delta(q, a). \end{cases}$$

Είναι εύκολο τώρα να δείξουμε ότι $L(\mathcal{A}') = L^*$ (ο αναγνώστης καλείται να δώσει την λεπτομερή απόδειξη σαν άσκηση), και συνεπώς η $L^* \in \mathrm{Rec}(A)$. □

Θεώρημα 2 *Η κλάση* $\mathrm{Rec}(A)$ *των αναγνωρίσιμων γλωσσών από ένα αλφάβητο* A *είναι κλειστή με τις πράξεις της ένωσης, της τομής, του συμπηρώματος, της παράθεσης και της θήκης.*

Απόδειξη Προκύπτει άμεσα από τις Προτάσεις 4, 5, 6, 11 και 12. □

Ασκήσεις

1) Ας είναι $\mathcal{A} = (Q, A, q_0, \delta', F)$ οποιοδήποτε DFA, αλλά όχι CFA. Να δείξετε ότι δεν μπορούμε να εφαρμόσουμε στο $\mathcal{A}$ τον αλγόριθμο της Πρότασης 5 για να βρούμε το συμπλήρωμα της $L(\mathcal{A})$.

2) Θεωρούμε το NFA $\mathcal{A} = (\{q_0, q_1, q_2\}, \{a, b, c\}, \{q_0, q_2\}, \delta, \{q_0, q_2\})$ με

δ	a	b	c
q_0	$\{q_1, q_2\}$	$\emptyset$	$\{q_2\}$
q_1	$\{q_1\}$	$\emptyset$	$\{q_1, q_2\}$
q_2	$\{q_1\}$	$\emptyset$	$\{q_2\}$.

Να σχεδιάσετε το NFA $\mathcal{A}$, να βρείτε τη γλώσσα του και να κατασκευάσετε και να σχεδιάσετε ένα ισοδύναμο CFA.

3) Θεωρούμε το NFA $\mathcal{A} = (\{q_0, q_1, q_2\}, \{a, b, c\}, \{q_2\}, \delta, \{q_2\})$ με

δ	a	b	c
q_0	$\{q_0, q_2\}$	$\emptyset$	$\{q_2\}$
q_1	$\{q_2\}$	$\emptyset$	$\{q_0, q_2\}$
q_2	$\{q_0, q_1\}$	$\emptyset$	$\{q_1\}$.

Να σχεδιάσετε το NFA $\mathcal{A}$, να βρείτε τη γλώσσα του και να κατασκευάσετε και να σχεδιάσετε ένα ισοδύναμο πλήρες.

4) Θεωρούμε το NFA $\mathcal{A} = (\{q_0, q_1, q_2\}, \{a, b, c\}, \{q_0, q_1, q_2\}, \delta, \{q_2\})$ με

δ	a	b	c
q_0	$\{q_0\}$	$\{q_0\}$	$\{q_2\}$
q_1	$\{q_1\}$	$\emptyset$	$\emptyset$
q_2	$\{q_1\}$	$\{q_0\}$	$\{q_2\}$.

Να σχεδιάσετε το NFA $\mathcal{A}$, να βρείτε τη γλώσσα του και να κατασκευάσετε και να σχεδιάσετε ένα ισοδύναμο CFA.

5) Δίνεται το αλφάβητο $A = \{a, b, c, d\}$. Να κατασκευάσετε NFA που αναγνωρίζουν τις γλώσσες

$$A^* dacA^*, \quad aA^* d^3 a^3 c^3 A^* a, \quad ab^2 A^* cbA^* dA^* d.$$

6) Να δείξετε ότι η κλάση $\mathrm{Rec}(A)$ είναι κλειστή με την πράξη της ένωσης χρησιμοποιώντας NFA.

7) Να κατασκευάσετε αυτόματο που αναγνωρίζει το συμπλήρωμα της γλώσσας του NFA της Άσκησης 2.

8) Να κατασκευάσετε αυτόματο που αναγνωρίζει το συμπλήρωμα της γλώσσας του NFA της Άσκησης 3.

9) Να κατασκευάσετε αυτόματο που αναγνωρίζει το συμπλήρωμα της γλώσσας του NFA της Άσκησης 4.

10) Να κατασκευάσετε NFA που αναγνωρίζει την ένωση των γλωσσών των αυτομάτων των Ασκήσεων 2 και 3.

11) Να κατασκευάσετε NFA που αναγνωρίζει την ένωση των γλωσσών των αυτομάτων των Ασκήσεων 2 και 4.

12) Να κατασκευάσετε NFA που αναγνωρίζει την ένωση των γλωσσών των αυτομάτων των Ασκήσεων 3 και 4.

13) Να κατασκευάσετε NFA που αναγνωρίζει την ένωση των γλωσσών των αυτομάτων των Ασκήσεων 2, 3 και 4.

14) Δίνεται NFA $\mathcal{A} = (Q, A, \{q_0\}, \delta, \{q_0\})$. Να δείξετε ότι η γλώσσα $L(\mathcal{A})$ αποτελεί μονοειδές με την πράξη της παράθεσης.

15) Να κατασκευάσετε τα κανονικοποιημένα NFA που προκύπτουν από τα αυτόματα των Ασκήσεων 2, 3, 4.

16) Δίνονται CFA $\mathcal{A} = (Q, A, q_0, \delta_{\mathcal{A}}, F)$ και $\mathcal{B} = (P, A, p_0, \delta_{\mathcal{B}}, S)$. Να κατασκευάσετε CFA που αναγνωρίζει τη γλώσσα $L(\mathcal{A})L(\mathcal{B})$.

17) Δίνεται CFA $\mathcal{A} = (Q, A, q_0, \delta_{\mathcal{A}}, F)$. Να κατασκευάσετε CFA που αναγνωρίζει τη γλώσσα $L(\mathcal{A})^*$.

18) Αν $L, M \in \mathrm{Rec}(A)$, τότε $alt(L, M) \in \mathrm{Rec}(A)$ (για τον ορισμό της πράξης alt βλ. Άσκηση 8, Κεφάλαιο 2).

19) Αν $L, M \in \mathrm{Rec}(A)$, τότε $L \sqcup\!\sqcup M \in \mathrm{Rec}(A)$ (για τον ορισμό της πράξης $L \sqcup\!\sqcup M$ βλ. Άσκηση 9, Κεφάλαιο 2).

20) Δίνεται αλφάβητο A, γλώσσα $L \subseteq A^*$, γράμμα $b \notin A$, και η γλώσσα $M = \{ubv \mid u, v \in A^* \text{ και } uv \in L\}$. Να δείξετε ότι

$$L \in \mathrm{Rec}(A) \implies M \in \mathrm{Rec}(A \cup \{b\}).$$

21) Δίνεται αλφάβητο A, γλώσσα $L \subseteq A^*$, γράμμα $b \notin A$, και η γλώσσα $M = \{ubbv \mid u, v \in A^* \text{ και } uv \in L\}$. Να δείξετε ότι

$$L \in \mathrm{Rec}(A) \implies M \in \mathrm{Rec}(A \cup \{b\}).$$

22) Δίνεται αλφάβητο A, γλώσσα $L \subseteq A^*$, γράμμα $b \notin A$, και η γλώσσα $M = \{ubbbv \mid u, v \in A^* \text{ και } uv \in L\}$. Να δείξετε ότι

$$L \in \mathrm{Rec}(A) \implies M \in \mathrm{Rec}(A \cup \{b\}).$$

23) Δίνονται αλφάβητα A, B τέτοια ώστε $A \cap B = \emptyset$, γλώσσα $L \subseteq A^*$, λέξη $w = b_1 \dots b_n \in B^+$ και η γλώσσα $M = \{uwv \mid u, v \in A^* \text{ και } uv \in L\}$. Να δείξετε ότι

$$L \in \mathrm{Rec}(A) \implies M \in \mathrm{Rec}(A \cup B).$$

24) Δίνονται τα DFA $\mathcal{A} = (\{q_0, q_1, q_2\}, \{a, b\}, q_0, \delta_{\mathcal{A}}, \{q_2\})$ με

$\delta_{\mathcal{A}}$	a	b
q_0	q_1	$\emptyset$
q_1	q_0	q_1
q_2	q_2	q_0

και $\mathcal{B} = (\{p_0, p_1, p_2\}, \{a, b\}, p_0, \delta_{\mathcal{B}}, \{p_0, p_2\})$ με

$\delta_{\mathcal{B}}$	a	b
p_0	p_1	$\emptyset$
p_1	p_2	p_1
p_2	$\emptyset$	p_2

Να βρείτε και να σχεδιάσετε το αυτόματο που αναγνωρίζει α) τη τομή των γλωσσών των δύο DFA, β) την ένωση των γλωσσών των δύο DFA, γ) το συμπλήρωμα της γλώσσας του DFA $\mathcal{A}$ και δ) το συμπλήρωμα της γλώσσας του DFA $\mathcal{B}$.

25) Δίνεται το αλφάβητο $A = \{a, b\}$. Να εξετάσετε αν η γλώσσα

$$L = \{a^{2n}b^m \mid n, m \geq 0\}$$

είναι αναγνωρίσιμη ή όχι.

26) Δίνεται το αλφάβητο $A = \{a, b, c\}$. Να εξετάσετε αν η γλώσσα

$$L = \{a^{2n}b^m c^l \mid n, m, l \geq 0\}$$

είναι αναγνωρίσιμη ή όχι.

27) Δίνεται το αλφάβητο $A = \{a, b\}$. Να εξετάσετε αν η γλώσσα $L \subseteq A^*$ που αποτελείται από όλες τις λέξεις από το A που περιέχουν άρτιο πλήθος γραμμάτων a και οποιοδήποτε πλήθος γραμμάτων b, είναι αναγνωρίσιμη ή όχι.

28) Δίνεται το αλφάβητο $A = \{a, b, c\}$. Να εξετάσετε αν η γλώσσα $L \subseteq A^*$ που αποτελείται από όλες τις λέξεις από το A που περιέχουν άρτιο πλήθος γραμμάτων a και οποιοδήποτε πλήθος γραμμάτων b και c, είναι αναγνωρίσιμη ή όχι.

Κεφάλαιο 6

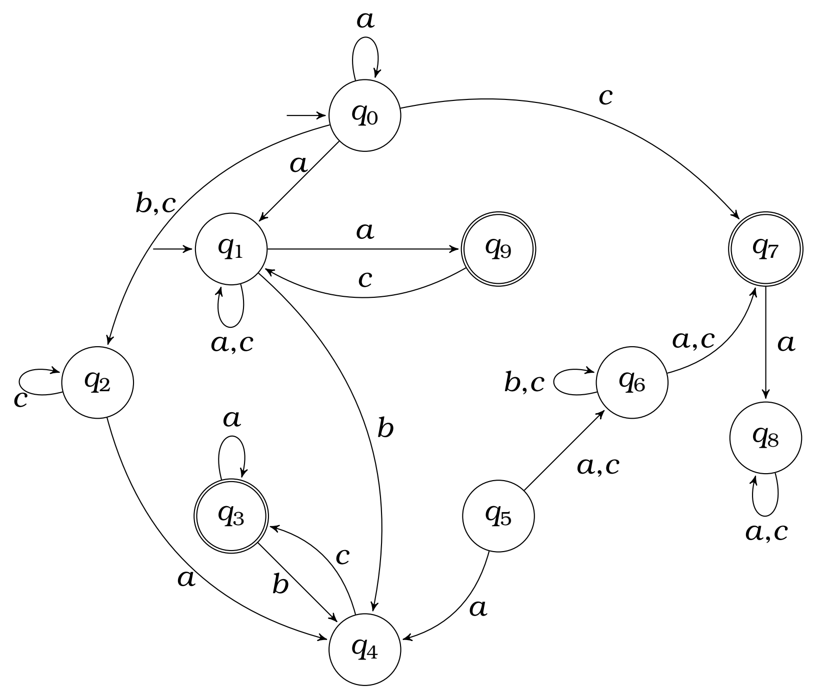
Αλγόριθμοι ελαχιστοποίησης πεπερασμένων αυτομάτων

Στο κεφάλαιο αυτό θα ασχοληθούμε με την ελαχιστοποίηση πεπερασμένων αυτομάτων. Συγκεκριμένα, θα δείξουμε ότι μπορούμε σε κάθε πεπερασμένο αυτόματο να αποφασίσουμε ποιές καταστάσεις είναι "άχρηστες", δηλαδή δεν συνεισφέρουν στον υπολογισμό της γλώσσας του πεπερασμένου αυτομάτου, και να τις απομακρύνουμε κάνοντας το πεπερασμένο αυτόματό μας πιο οικονομικό χωρίς να αλλάζει η συμπεριφορά του. Η διαδικασία της ελαχιστοποίησης αυτομάτων, δεν μας εφοδιάζει μόνο με οικονομικότερα αυτόματα. Μας δίνει την δυνατότητα να απαντήσουμε και σε προβλήματα απόφασης που αφορούν τα πεπερασμένα αυτόματα.

Ας ξεκινήσουμε με ένα παράδειγμα. Θεωρούμε το NFA $\mathcal{A} = (\{q_0, q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9\}, \{a, b, c\}, \{q_0, q_1\}, \delta, \{q_3, q_7, q_9\})$ με

δ	a	b	c
q_0	$\{q_0, q_1\}$	$\{q_2\}$	$\{q_2, q_7\}$
q_1	$\{q_1, q_9\}$	$\{q_4\}$	$\{q_1\}$
q_2	$\{q_4\}$	$\emptyset$	$\{q_2\}$
q_3	$\{q_3\}$	$\{q_4\}$	$\emptyset$
q_4	$\emptyset$	$\emptyset$	$\{q_3\}$
q_5	$\{q_4, q_6\}$	$\emptyset$	$\{q_6\}$
q_6	$\{q_7\}$	$\{q_6\}$	$\{q_6, q_7\}$
q_7	$\{q_8\}$	$\emptyset$	$\emptyset$
q_8	$\{q_8\}$	$\emptyset$	$\{q_8\}$
q_9	$\emptyset$	$\emptyset$	$\{q_1\}$

Παρατηρώντας το γράφημα του NFA, στην επόμενη σελίδα, βλέπουμε ότι δεν υπάρχει επιτυχής διαδρομή του NFA που να περνάει από τις καταστάσεις q_5, q_6 ή q_8, Συνεπώς αν "αφαιρέσουμε" αυτές τις καταστάσεις από το διάγραμμα του $\mathcal{A}$, το NFA που θα προκύψει θα έχει την ίδια γλώσσα με το $\mathcal{A}$.



Στη συνέχεια θα δείξουμε με αυστηρό τρόπο πως μπορούμε να βρούμε τις άχρηστες καταστάσεις ενός πεπερασμένου αυτομάτου. Ας είναι λοιπόν $\mathcal{A} = (Q, A, I, \delta, F)$ ένα NFA. Μία κατάσταση $q \in Q$ ονομάζεται *προσιτή* αν υπάρχει αρχική κατάσταση $q_0 \in I$ και λέξη $w \in A^*$ έτσι ώστε $q \in \delta^*(q_0, w)$. Η q θα ονομάζεται *συμπροσιτή* αν υπάρχει λέξη $u \in A^*$ έτσι ώστε $\delta^*(q, u) \cap F \neq \emptyset$. Τέλος θα ονομάζεται *χρήσιμη* αν είναι προσιτή και συμπροσιτή. Θα συμβολίζουμε με Q^{ac} (αντίστοιχα Q^{coac}, Q^t) το σύνολο των προσιτών (αντίστοιχα συμπροσιτών, χρήσιμων) καταστάσεων του $\mathcal{A}$.

Πρόταση 13 *Ας είναι* $\mathcal{A} = (Q, A, I, \delta, F)$ *ένα* NFA. *Το σύνολο* Q^{ac} *υπολογίζεται σε πεπερασμένου πλήθους βήματα.*

Απόδειξη Θεωρούμε την ακολουθία υποσυνόλων $(I_n)_{n\geq 0}$ του Q η οποία ορίζεται ως εξής:
$I_0 = I,$
$I_1 = \{q \mid q \in Q, \text{ υπάρχουν } q_0 \in I_0, a \in A \text{ έτσι ώστε } q \in \delta(q_0, a)\} \setminus I_0,$
$I_2 = \{q \mid q \in Q, \text{ υπάρχουν } q_1 \in I_1, a \in A \text{ έτσι ώστε } q \in \delta(q_1, a)\} \setminus (I_0 \cup I_1),$
$\ldots$
$I_{n+1} = \{q \mid q \in Q, \text{ υπάρχουν } q_n \in I_n, a \in A \text{ έτσι ώστε } q \in \delta(q_n, a)\} \setminus (I_0 \cup \ldots \cup I_n),$
για κάθε $n \geq 0$.

Τα σύνολα I_n, $n \geq 0$, είναι ανά δύο ξένα μεταξύ τους, συνεπώς υπάρχει δείκτης $m < card(Q)$ έτσι ώστε $I_m \neq \emptyset$ και $I_i = \emptyset$ για κάθε $i > m$. Από τον τρόπο ορισμού της ακολουθίας $(I_n)_{n\geq 0}$ είναι φανερό ότι

$$Q^{ac} = \bigcup_{0\leq k\leq m} I_k.$$

□

Πρόταση 14 *Από κάθε* NFA $\mathcal{A} = (Q, A, I, \delta, F)$ *μπορούμε να κατασκευάσουμε ένα ισοδύναμο* NFA $\mathcal{A}^{ac}$ *του οποίου όλες οι καταστάσεις είναι προσιτές.*

Απόδειξη Με τον αλγόριθμο που περιγράφεται στην απόδειξη της Πρότασης 13, υπολογίζουμε το σύνολο Q^{ac} των προσιτών καταστάσεων του $\mathcal{A}$. Στη συνέχεια, είναι εύκολο να δείξουμε ότι το NFA $\mathcal{A}^{ac} = (Q^{ac}, A, I, \delta^{ac}, F^{ac})$, όπου δ^{ac} είναι ο περιορισμός της δ στο $Q^{ac} \times A$ και $F^{ac} = F \cap Q^{ac}$, έχει όλες του τις καταστάσεις προσιτές και είναι ισοδύναμο με το $\mathcal{A}$. Η αυστηρή απόδειξη αφήνεται σαν άσκηση στον αναγνώστη. □

Θα χρησιμοποιήσουμε τον αλγόριθμο που περιγράψαμε στην απόδειξη της προηγούμενης πρότασης για να βρούμε το NFA $\mathcal{A}^{ac}$ που προκύπτει από το NFA της σελίδας 63. Έχουμε $I = \{q_0, q_1\}$, οπότε

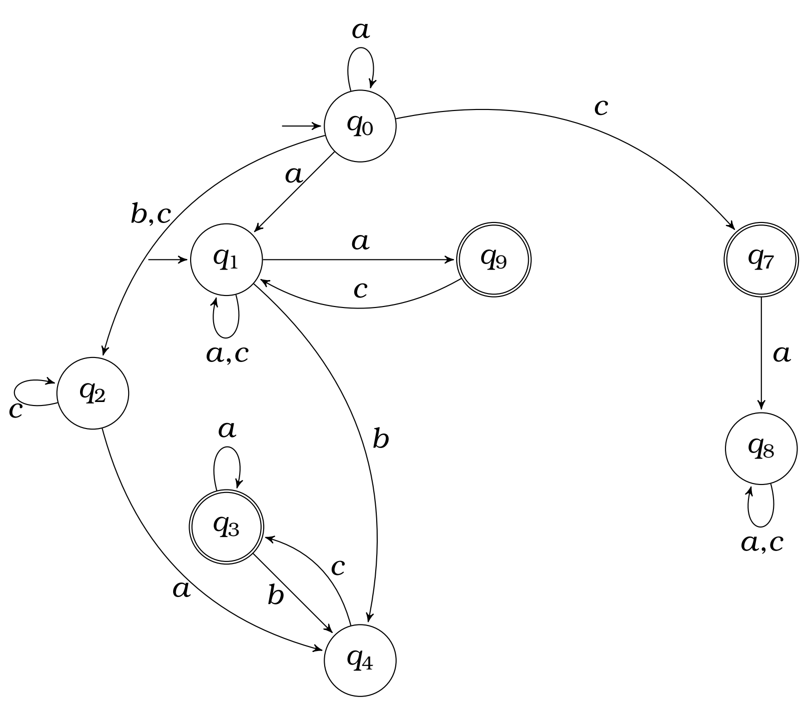
$I_0 = I = \{q_0, q_1\}$,

$I_1 = \{q_2, q_4, q_7, q_9\}$,

$I_2 = \{q_3, q_8\}$,

$I_3 = \emptyset$, και συνεπώς $I_i = \emptyset$ για κάθε $i \geq 3$.

Έτσι $Q^{ac} = I_0 \cup I_1 \cup I_2 = \{q_0, q_1, q_2, q_3, q_4, q_7, q_8, q_9\}$. Το NFA $\mathcal{A}^{ac}$ δίνεται από το επόμενο διάγραμμα



Πρόταση 15 *Ας είναι* $\mathcal{A} = (Q, A, I, \delta, F)$ *ένα* NFA. *Το σύνολο* Q^{coac} *υπολογίζεται σε πεπερασμένου πλήθους βήματα.*

Απόδειξη Θεωρούμε την ακολουθία υποσυνόλων $(F_n)_{n\geq 0}$ του Q η οποία ορίζεται ως εξής:
$F_0 = F$,
$F_1 = \{p \mid p \in Q,$ υπάρχουν $p_0 \in F_0, a \in A$ έτσι ώστε $p_0 \in \delta(p, a)\} \setminus F_0$,
$F_2 = \{p \mid p \in Q,$ υπάρχουν $p_1 \in F_1, a \in A$ έτσι ώστε $p_1 \in \delta(p, a)\} \setminus (F_0 \cup F_1)$,
...
$F_{n+1} = \{p \mid p \in Q,$ υπάρχουν $p_n \in F_n, a \in A$ έτσι ώστε $p_n \in \delta(p, a)\} \setminus (F_0 \cup \ldots \cup F_n)$, για κάθε $n \geq 0$.

Τα σύνολα F_n, $n \geq 0$, είναι ανά δύο ξένα μεταξύ τους, συνεπώς υπάρχει δείκτης $l < card(Q)$ έτσι ώστε $F_l \neq \emptyset$ και $F_i = \emptyset$ για κάθε $i > l$. Από τον τρόπο ορισμού της ακολουθίας $(F_n)_{n\geq 0}$ είναι φανερό ότι

$$Q^{coac} = \bigcup_{0\leq k\leq l} F_k.$$

□

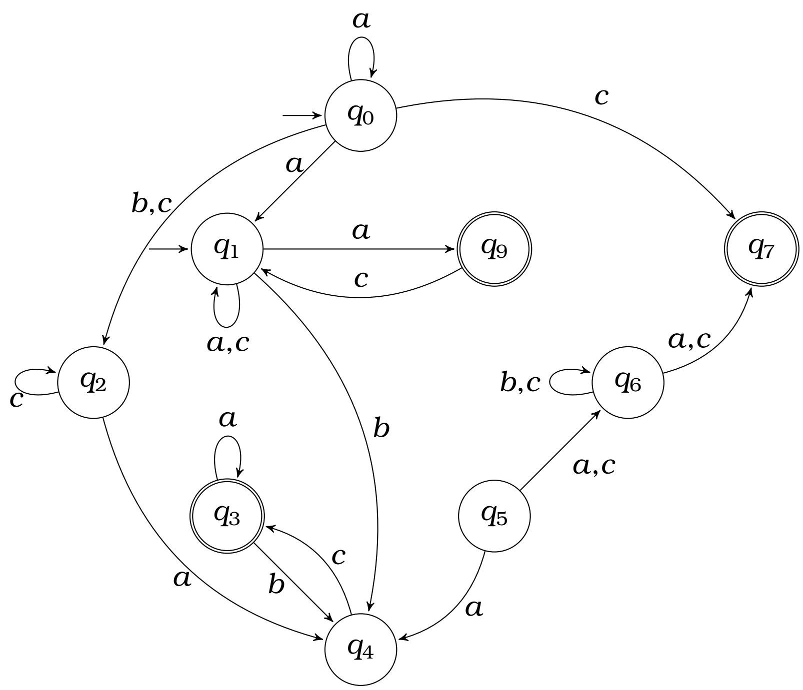
Πρόταση 16 *Από κάθε* NFA $\mathcal{A} = (Q, A, I, \delta, F)$ *μπορούμε να κατασκευάσουμε ένα ισοδύναμο* NFA $\mathcal{A}^{coac}$ *του οποίου όλες οι καταστάσεις είναι συμπροσιτές.*

Απόδειξη Με τον αλγόριθμο που περιγράφεται στην απόδειξη της Πρότασης 15, υπολογίζουμε το σύνολο Q^{coac} των συμπροσιτών καταστάσεων του $\mathcal{A}$. Στη συνέχεια, είναι εύκολο να δείξουμε ότι το NFA $\mathcal{A}^{coac} = (Q^{coac}, A, I^{coac}, \delta^{coac}, F)$, όπου δ^{coac} είναι ο περιορισμός της δ στο $Q^{coac} \times A$ και $I^{coac} = I \cap Q^{coac}$, έχει όλες του τις καταστάσεις συμπροσιτές και είναι ισοδύναμο με το $\mathcal{A}$. Η αυστηρή απόδειξη αφήνεται σαν άσκηση στον αναγνώστη. □

Θα χρησιμοποιήσουμε τώρα τον αλγόριθμο που περιγράψαμε στην απόδειξη της Πρότασης 16 για να βρούμε το NFA $\mathcal{A}^{coac}$ που προκύπτει από το αυτόματο της σελίδας 63. Έχουμε $F = \{q_3, q_7, q_9\}$, οπότε
$F_0 = F = \{q_3, q_7, q_9\}$,
$F_1 = \{q_0, q_1, q_4, q_6\}$,
$F_2 = \{q_2, q_5\}$,
$F_3 = \emptyset$, και συνεπώς $F_i = \emptyset$ για κάθε $i \geq 3$.
Έτσι $Q^{coac} = F_0 \cup F_1 \cup F_2 = \{q_0, q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_9\}$. Το NFA $\mathcal{A}^{coac}$ δίνεται από το διάγραμμα της σελίδας 67.

Πρόταση 17 *Ας είναι* $\mathcal{A} = (Q, A, I, \delta, F)$ *ένα* NFA. *Το σύνολο* Q^t *υπολογίζεται σε πεπερασμένου πλήθους βήματα.*

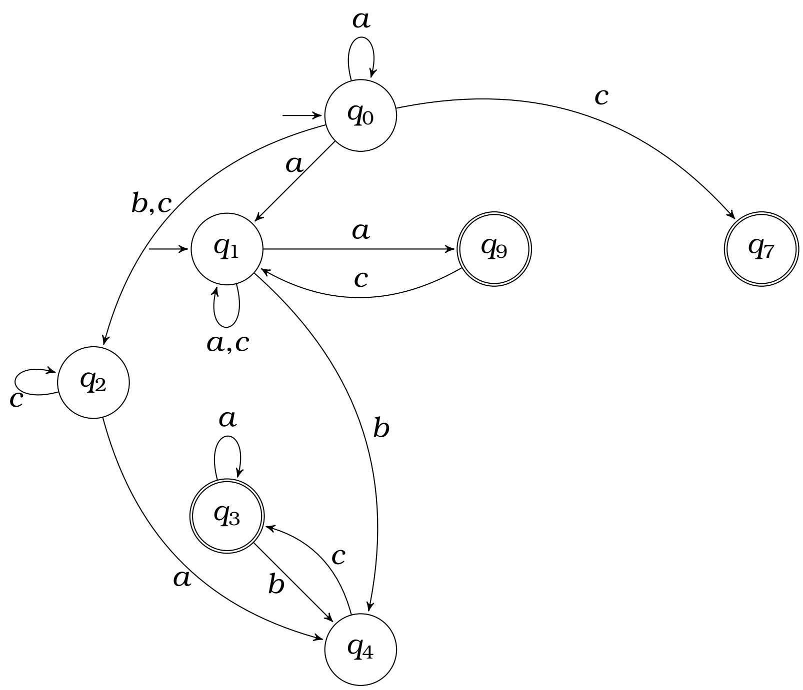
Απόδειξη Εφαρμόζουμε διαδοχικά τον αλγόριθμο που περιγράφεται στην απόδειξη της Πρότασης 13 και τον αλγόριθμο που περιγράφεται στην απόδειξη της Πρότασης 15. □



Θεώρημα 3 *Από κάθε* NFA $\mathcal{A} = (Q, A, I, \delta, F)$ *μπορούμε να κατασκευάσουμε ένα ισοδύναμο* NFA *του οποίου όλες οι καταστάσεις είναι χρήσιμες.*

Απόδειξη Από το $\mathcal{A}$ κατασκευάζουμε το NFA $\mathcal{A}^{ac}$ και στη συνέχεια το $(\mathcal{A}^{ac})^{coac}$. Από τις Προτάσεις 14 και 16, είναι φανερό ότι το NFA $(\mathcal{A}^{ac})^{coac}$ είναι ισοδύναμο με το $\mathcal{A}$ και έχει όλες τις καταστάσεις του χρήσιμες. □

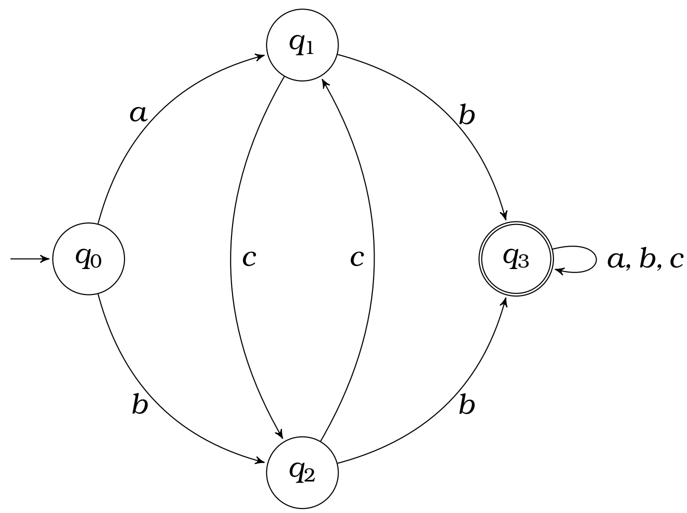
Έτσι αν εφαρμόσουμε στο NFA της σελίδας 63, τον αλγόριθμο που περιγράψαμε στην απόδειξη του Θεωρήματος 3, θα βρούμε το ισοδύναμο NFA $(\mathcal{A}^{ac})^{coac}$ που έχει όλες τις καταστάσεις του χρήσιμες. Το διάγραμμα του $(\mathcal{A}^{ac})^{coac}$ είναι το



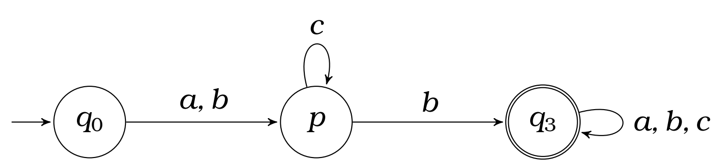
Θα δείξουμε στη συνέχεια, ότι ένα DFA του οποίου όλες οι καταστάσεις είναι χρήσιμες, ενδεχομένως να επιδέχεται περαιτέρω ελαχιστοποίηση. Ας θεωρήσουμε για παράδειγμα το DFA $\mathcal{A} = (Q, A, q_0, \delta, F)$ με $A = \{a, b, c\}$, $Q = \{q_0, q_1, q_2, q_3\}$, $F = \{q_3\}$ και την απεικόνιση δ που ορίζεται από τον πίνακα

δ	a	b	c
q_0	q_1	q_2	$\emptyset$
q_1	$\emptyset$	q_3	q_2
q_2	$\emptyset$	q_3	q_1
q_3	q_3	q_3	q_3.

Από το διάγραμμα του $\mathcal{A}$, στη σελίδα 69, είναι φανερό ότι όλες οι καταστάσεις του είναι χρήσιμες. "Φαίνεται" όμως ότι οι καταστάσεις q_1 και q_2 "συμπεριφέρονται" ακριβώς με τον ίδιο τρόπο. Άραγε, αν τις "ταυτίσουμε" θα έχουμε ένα ισοδύναμο DFA;



Πράγματι είναι εύκολο να διαπιστώσουμε ότι το αυτόματο $\mathcal{A}'$, με διάγραμμα



είναι ισοδύναμο με το $\mathcal{A}$. Το παράδειγμα αυτό δείχνει, ότι ακόμη κι αν ένα DFA δεν έχει άχρηστες καταστάσεις, ενδέχεται να μπορούμε να ταυτίσουμε κάποιες από τις καταστάσεις του, και συνεπώς να κατασκευάσουμε ένα ισοδύναμο αλλά "οικονομικότερο" πεπερασμένο αυτόματο. Στη συνέχεια θα μελετήσουμε την περίπτωση αυτή.

Θεωρούμε ένα DFA $\mathcal{A} = (Q, A, q_0, \delta, F)$ με όλες του τις καταστάσεις χρήσιμες. Στο σύνολο Q ορίζουμε τη σχέση $\equiv$ ως εξής:

$$q \equiv q' \quad \text{αν-ν} \quad (\delta^*(q, w) \in F \iff \delta^*(q', w) \in F \quad \text{για κάθε } w \in A^*).$$

Είναι εύκολο να διαπιστώσουμε ότι η $\equiv$ είναι σχέση ισοδυναμίας στο Q. Θα δείξουμε ότι

$$\text{αν} \quad [q] = [q'] \quad \text{τότε} \quad [\delta^*(q, w)] = [\delta^*(q', w)] \;\; \text{για κάθε} \;\; w \in A^*. \tag{6.1}$$

Πράγματι ας είναι $w \in A^*$ και $p \in [\delta^*(q, w)]$. Αυτό σημαίνει ότι για κάθε $u \in A^*$ θα έχουμε

$$\begin{aligned} \delta^*(p, u) \in F \quad &\iff \quad \delta^*(\delta^*(q, w), u) \in F \\ &\iff \quad \delta^*(q, wu) \in F \\ &\iff \quad \delta^*(q', wu) \in F \\ &\iff \quad \delta^*(\delta^*(q', w), u) \in F \end{aligned}$$

όπου η τρίτη ισοδυναμία ισχύει διότι $q \equiv q'$.

Άρα $p \equiv \delta^*(q', w)$, που σημαίνει ότι $p \in [\delta^*(q', w)]$ και συνεπώς $[\delta^*(q, w)] \subseteq [\delta^*(q', w)]$. Ο αντίστροφος εγκλεισμός αποδεικνύεται ανάλογα, οπότε $[\delta^*(q, w)] = [\delta^*(q', w)]$.

Στη συνέχεια θα δείξουμε για κάθε $q \in Q$, ότι

$$\text{αν} \quad q \in F \quad \text{τότε} \quad [q] \subseteq F. \tag{6.2}$$

Πράγματι ας είναι $q \in F$ και $q' \in [q]$. Τότε $\delta^*(q', w) \in F \iff \delta^*(q, w) \in F$ για κάθε $w \in A^*$, και καθώς $q \in F$ θα έχουμε $q = \delta^*(q, \varepsilon) \in F$, οπότε και $q' = \delta^*(q', \varepsilon) \in F$. Άρα $[q] \subseteq F$.

Τέλος θα αποδείξουμε ότι το σύνολο πηλίκο $Q/\equiv$ προσδιορίζεται σε πεπερασμένου πλήθους βήματα. Για κάθε $n \geq 0$, θεωρούμε στο Q τη σχέση ισοδυναμίας $\equiv_n$ ως εξής:

$$q \equiv_n q' \quad \text{αν-ν} \quad (\delta^*(q, w) \in F \iff \delta^*(q', w) \in F \quad \text{για κάθε } w \in A^* \text{ με } |w| \leq n)$$

για κάθε $q, q' \in Q$.
Είναι φανερό ότι για κάθε $n \geq 0$ και $q, q' \in Q$, έχουμε $q \equiv_{n+1} q' \implies q \equiv_n q'$ και συνεπώς

$$\equiv_0 \supseteq \equiv_1 \supseteq \equiv_2 \ldots \supseteq \bigcap_{n \geq 0} \equiv_n = \equiv$$

που σημαίνει ότι

$$card(Q/\equiv_0) \leq card(Q/\equiv_1) \leq card(Q/\equiv_2) \leq \ldots .$$

Καθώς όμως το σύνολο Q είναι πεπερασμένο, θα υπάρχει $k < card(Q)$ τέτοιο ώστε $Q/\equiv_i = Q/\equiv_k$ για κάθε $i \geq k$. Έτσι $\equiv = \equiv_k$ που σημαίνει ότι για να ελέγξουμε αν $q \equiv q'$, για $q, q' \in Q$, αρκεί να ελέγξουμε αν $\delta^*(q, w) \in F \iff \delta^*(q', w) \in F$ για κάθε $w \in A^*$ με $|w| < card(Q)$. Συνεπώς το σύνολο πηλίκο $Q/\equiv$ προσδιορίζεται σε πεπερασμένου πλήθους βήματα.

Ένα DFA $\mathcal{A} = (Q, A, q_0, \delta, F)$ με όλες τις καταστάσεις του χρήσιμες, στο οποίο η ισοδυναμία $\equiv$ που ορίσθηκε παραπάνω είναι ισότητα, ονομάζεται *αναγμένο.*

Πρόταση 18 *Για κάθε* DFA $\mathcal{A} = (Q, A, q_0, \delta, F)$ *με όλες τις καταστάσεις του χρήσιμες, μπορούμε να κατασκευάσουμε ένα ισοδύναμο αναγμένο* DFA.

Απόδειξη Θεωρούμε το DFA $\mathcal{A}' = (Q/\equiv, A, [q_0], \delta', F')$, με $F' = \{[q] \mid q \in F\}$ και η απεικόνιση δ' ορίζεται από τη σχέση

$$\delta'([q], a) = [\delta(q, a)]$$

για κάθε $q \in Q$, $a \in A$. Λόγω της (6.1), η δ είναι καλά ορισμένη. Θα δείξουμε ότι

$$\delta'^*([q], w) = [\delta^*(q, w)]$$

για κάθε $q \in Q$, $w \in A^*$. Θα χρησιμοποιήσουμε επαγωγή στο μήκος της λέξης w. Πράγματι για $|w| = 0$ έχουμε $w = \varepsilon$ και $\delta'^*([q], \varepsilon) = [q] = [\delta^*(q, \varepsilon)]$. Υποθέτουμε ότι ισχύει για όλες τις λέξεις με μήκος $\leq k$ και έστω $w \in A^*$ με μήκος $|w| = k + 1$. Αυτό σημαίνει ότι $w = ua$ με $u \in A^*$, $a \in A$ και $|u| = k$. Τότε

$$\begin{aligned}
\delta'^*([q], w) &= \delta'^*([q], ua) \\
&= \delta'(\delta'^*([q], u), a) \\
&= \delta'([\delta^*(q, u)], a) \\
&= [\delta(\delta^*(q, u), a)] \\
&= [\delta^*(q, ua)] \\
&= [\delta^*(q, w)]
\end{aligned}$$

όπου η τρίτη ισότητα ισχύει από την υπόθεση της επαγωγής και η τέταρτη από τον ορισμό της δ'.

Το DFA $\mathcal{A}'$ έχει όλες τις καταστάσεις του χρήσιμες και είναι φανερά αναγμένο. Απομένει συνεπώς να αποδείξουμε ότι είναι και ισοδύναμο του $\mathcal{A}$. Πράγματι, για κάθε $w \in A^*$ έχουμε

$$\begin{aligned}
w \in L(\mathcal{A}') &\Longleftrightarrow \delta'^*([q_0], w) \in F' \\
&\Longleftrightarrow [\delta^*(q_0, w)] \in F' \\
&\Longleftrightarrow \delta^*(q_0, w) \in F \\
&\Longleftrightarrow w \in L(\mathcal{A})
\end{aligned}$$

όπου η τρίτη ισοδυναμία ισχύει λόγω της (6.2). Συνεπώς $L(\mathcal{A}') = L(\mathcal{A})$, και η απόδειξή μας τελείωσε. □

Στη συνέχεια θα ασχοληθούμε με προβλήματα απόφασης που αφορούν τα πεπερασμένα αυτόματα.

Πρόταση 19 *Για οποιοδήποτε πεπερασμένο αυτόματο $\mathcal{A}$ μπορούμε να αποφασίσουμε αν $L(\mathcal{A}) = \emptyset$ ή όχι.*

Απόδειξη Από το πεπερασμένο αυτόματο $\mathcal{A} = (Q, A, I, \delta, F)$ κατασκευάζουμε (Θεώρημα 3) ένα ισοδύναμο $\mathcal{A}' = (Q^t, A, I', \delta', F')$ που έχει όλες τις καταστάσεις του χρήσιμες. Τότε έχουμε

$$L(\mathcal{A}) = \emptyset \Longleftrightarrow L(\mathcal{A}') = \emptyset \Longleftrightarrow Q^t = \emptyset.$$

Καθώς το Q^t είναι πεπερασμέμο μπορούμε να αποφασίσουμε αν $Q^t = \emptyset$, και συνεπώς αν $L(\mathcal{A}) = \emptyset$ ή όχι. □

Πρόταση 20 *Για δύο πεπερασμένα αυτόματα $\mathcal{A}$ και $\mathcal{B}$ μπορούμε να αποφασίσουμε αν $L(\mathcal{A}) \subseteq L(\mathcal{B})$ ή όχι.*

Απόδειξη Ισχύει

$$L(\mathcal{A}) \subseteq L(\mathcal{B}) \iff L(\mathcal{A}) \cap \overline{L(\mathcal{B})} = \emptyset$$

όπου $\overline{L(\mathcal{B})}$ είναι το συμπλήρωμα της γλώσσας $L(\mathcal{B})$. Από την Πρόταση 5, η γλώσσα $\overline{L(\mathcal{B})}$ είναι αναγνωρίσιμη, και συνεπώς από την Πρόταση 4 και η γλώσσα $L(\mathcal{A}) \cap \overline{L(\mathcal{B})}$ είναι αναγνωρίσμη. Έτσι η απόδειξή μας ολοκληρώνεται αν λάβουμε υπόψη την Πρόταση 19. □

Στη συνέχεια αποδεικνύουμε ότι για δύο οποιαδήποτε πεπερασμένα αυτόματα μπορούμε να αποφασίσουμε αν είναι ισοδύναμα ή όχι.

Θεώρημα 4 *Για δύο πεπερασμένα αυτόματα $\mathcal{A}$ και $\mathcal{B}$ μπορούμε να αποφασίσουμε αν $L(\mathcal{A}) = L(\mathcal{B})$ ή όχι.*

Απόδειξη Το θεώρημά μας ισχύει λόγω της σχέσης

$$L(\mathcal{A}) = L(\mathcal{B}) \iff (L(\mathcal{A}) \subseteq L(\mathcal{B}) \text{ και } L(\mathcal{B}) \subseteq L(\mathcal{A}))$$

και της Πρότασης 20. □

Τέλος δείχνουμε ότι για οποιοδήποτε πεπερασμένο αυτόματο από ένα αλφάβητο A, μπορούμε να αποδείξουμε αν αναγνωρίζει όλες τις λέξεις από το A, δηλαδή αν η γλώσσα του είναι η A^* ή όχι.

Πρόταση 21 *Για οποιοδήποτε πεπερασμένο αυτόματο $\mathcal{A}$ με αλφάβητο εισόδου A μπορούμε να αποφασίσουμε αν $L(\mathcal{A}) = A^*$ ή όχι.*

Απόδειξη Θεωρούμε το CFA $\mathcal{B} = (\{q_0\}, A, q_0, \delta, \{q_0\})$ με $\delta(q_0, a) = q_0$ για κάθε $a \in A$. Είναι προφανές ότι $L(\mathcal{B}) = A^*$ και συνεπώς

$$L(\mathcal{A}) = A^* \iff L(\mathcal{A}) = L(\mathcal{B}).$$

Για την τελευταία ισότητα όμως μπορούμε να αποφασίσουμε αν ισχύει ή όχι, όπως προκύπτει από το προηγούμενο θεώρημα. Συνεπώς μπορούμε να αποφασίσουμε αν $L(\mathcal{A}) = A^*$ ή όχι. □

Ασκήσεις

1) Δίνεται το NFA $\mathcal{A} = (\{q_0, q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9\}, \{a, b, c\}, \{q_0, q_3\}, \delta, \{q_5, q_9\})$ με

δ	a	b	c
q_0	$\{q_0, q_1\}$	$\{q_2\}$	$\{q_2, q_7\}$
q_1	$\{q_1, q_9\}$	$\{q_4\}$	$\{q_1\}$
q_2	$\{q_4\}$	$\emptyset$	$\{q_2\}$
q_3	$\{q_3\}$	$\{q_4\}$	$\emptyset$
q_4	$\emptyset$	$\emptyset$	$\{q_3\}$
q_5	$\{q_4, q_6\}$	$\emptyset$	$\{q_6\}$
q_6	$\{q_7\}$	$\{q_6\}$	$\{q_6, q_7\}$
q_7	$\{q_8\}$	$\emptyset$	$\emptyset$
q_8	$\{q_8\}$	$\emptyset$	$\{q_8\}$
q_9	$\emptyset$	$\emptyset$	$\{q_1\}$

Να σχεδιάσετε το NFA $\mathcal{A}$, και να βρείτε ένα ισοδύναμο NFA που έχει όλες τις καταστάσεις του χρήσιμες.

2) Δίνεται το NFA $\mathcal{A} = (\{q_0, q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9\}, \{a, b, c\}, \{q_4\}, \delta, \{q_8\})$ με

δ	a	b	c
q_0	$\{q_0, q_1\}$	$\{q_2\}$	$\{q_2, q_7\}$
q_1	$\{q_1, q_9\}$	$\{q_4\}$	$\{q_1\}$
q_2	$\{q_4\}$	$\emptyset$	$\{q_2\}$
q_3	$\{q_3, q_5\}$	$\{q_4\}$	$\emptyset$
q_4	$\emptyset$	$\emptyset$	$\{q_3\}$
q_5	$\{q_4, q_6\}$	$\emptyset$	$\{q_6\}$
q_6	$\{q_7\}$	$\{q_6\}$	$\{q_6, q_7\}$
q_7	$\{q_8\}$	$\emptyset$	$\emptyset$
q_8	$\{q_8\}$	$\emptyset$	$\{q_8\}$
q_9	$\emptyset$	$\emptyset$	$\{q_1\}$

Να σχεδιάσετε το NFA $\mathcal{A}$, και να βρείτε ένα ισοδύναμο NFA που έχει όλες τις καταστάσεις του χρήσιμες.

3) Δίνεται το NFA $\mathcal{A} = (\{q_0, q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9\},$

$\{a, b, c\}, \{q_8\}, \delta, \{q_8\})$ με

δ	a	b	c
q_0	$\{q_0, q_1\}$	$\{q_2\}$	$\{q_2, q_7\}$
q_1	$\{q_1, q_9\}$	$\{q_4\}$	$\{q_1\}$
q_2	$\{q_4\}$	$\emptyset$	$\{q_2\}$
q_3	$\{q_3\}$	$\{q_4\}$	$\emptyset$
q_4	$\emptyset$	$\emptyset$	$\{q_3\}$
q_5	$\{q_4, q_6\}$	$\emptyset$	$\{q_6\}$
q_6	$\{q_7\}$	$\{q_6\}$	$\{q_6, q_7\}$
q_7	$\{q_8\}$	$\emptyset$	$\emptyset$
q_8	$\{q_8\}$	$\emptyset$	$\{q_8\}$
q_9	$\emptyset$	$\emptyset$	$\{q_1\}$

Να σχεδιάσετε το NFA $\mathcal{A}$, και να βρείτε ένα ισοδύναμο NFA που έχει όλες τις καταστάσεις του χρήσιμες.

4) Θεωρούμε το DFA $\mathcal{A} = (Q, A, q_0, \delta, F)$ με $A = \{a, b, c\}$, $Q = \{q_0, q_1, q_2, q_3, q_4, q_5, q_6, q_7\}$, $F = \{q_5, q_7\}$ και την απεικόνιση δ που ορίζεται από τον πίνακα

δ	a	b	c
q_0	q_1	q_2	q_6
q_1	q_3	$\emptyset$	q_1
q_2	q_4	q_6	q_2
q_3	$\emptyset$	q_4	q_5
q_4	$\emptyset$	q_3	q_5
$0q_5$	q_5	$\emptyset$	$\emptyset$
q_6	$\emptyset$	q_6	q_6
q_7	q_6	$\emptyset$	$\emptyset$

Να βρείτε ένα αναγμένο DFA, ισοδύναμο του $\mathcal{A}$.

5) Δίνονται δύο NFA $\mathcal{A}$ και $\mathcal{B}$ με ίδιο αλφάβητο εισόδου A. Να γράψετε τον αλγόριθμο που θα ακολουθήσετε για να αποφασίσετε αν $L(\mathcal{A}) = L(\mathcal{B})$ ή όχι.

Κεφάλαιο 7

Ρητές γλώσσες

Στο κεφάλαιο αυτό θα εισάγουμε την έννοια των ρητών γλωσσών και θα αποδείξουμε το θεώρημα του *Kleene* που θεμελιώνει μια αλγεβρική περιγραφή των αναγνωρίσιμων γλωσσών. Οι πράξεις της ένωσης, της παράθεσης και τη θήκης γλωσσών θα ονομάζονται *ρητές πράξεις*.

Ορισμός 7 *Ας είναι A ένα αλφάβητο. Μια γλώσσα $L \subseteq A^*$ θα ονομάζεται ρητή αν προκύπτει από κάποια γράμματα του αλφαβήτου A με εφαρμογή πεπερασμένου πλήθους φορών των ρητών πράξεων.*

Για παράδειγμα, αν $A = \{a, b, c, d\}$, τότε οι παρακάτω γλώσσες

$$a^*b^2, \quad b(cd^3)^*, \quad a^*b^*, \quad (((b^*a)^*d)^*c^*)b^* \cup db, \quad ((db)^*ac^*)^* \cup c^3 \cup ab^*c^3$$

είναι όλες ρητές. Αντίθετα, όπως θα προκύψει από το θεώρημα του *Kleene*, η γλώσσα $\{a^n b^n \mid n \geq 0\}$ δεν είναι ρητή.

Η κλάση όλων των ρητών γλωσσών από ένα αλφάβητο A θα συμβολίζεται[1] με $\mathrm{Rat}(A)$.

Πρόταση 22 *Η κλάση $\mathrm{Rat}(A)$ είναι η ελάχιστη κλάση γλωσσών από το αλφάβητο A που περιέχει τις πεπερασμένες γλώσσες και είναι κλειστή με τις ρητές πράξεις.*

Απόδειξη Ας είναι $L = \{w_1, \ldots, w_n\}$ μια πεπερασμένη γλώσσα. Τότε $L = \{w_1\} \cup \ldots \cup \{w_n\}$, και κάθε μονοσύνολο $\{w_i\}$ $(1 \leq i \leq n)$ είναι ρητή γλώσσα καθώς η λέξη w_i προκύπτει από την παράθεση των γραμμάτων της. Ας είναι τώρα $L, M \in \mathrm{Rat}(A)$. Η L (αντίστοιχα η M) προκύπτει από κάποια γράμματα του A με εφαρμογή πεπερασμένου πλήθους φορών των ρητών πράξεων. Έτσι η $L \cup M$ προκύπτει από τα γράμματα και τις ρητές πράξεις που προκύπτουν οι L και M με εφαρμογή και της πράξης της ένωσης. Συνεπώς η γλώσσα $L \cup M$ ειναι ρητή. Όμοια δείχνουμε ότι $LM, L^* \in \mathrm{Rat}(A)$. Άρα η κλάση $\mathrm{Rat}(A)$ είναι κλειστή με τις ρητές πράξεις.

Στη συνέχεια θεωρούμε μία κλάση γλωσσών $\mathcal{L}$, από το αλφάβητο A, η οποία περιέχει τις πεπερασμένες γλώσσες και είναι κλειστή με τις ρητές πράξεις. Θα

[1] Ο συμβολισμός *Rat* προκύπτει από την λέξη *rational* = ρητή.

δείξουμε ότι $\mathrm{Rat}(A) \subseteq \mathcal{L}$. Ας είναι $L \in \mathrm{Rat}(A)$. Η L παράγεται από κάποια γράμματα, έστω τα $a_1, \ldots, a_n$, του αλφαβήτου A με εφαρμογή πεπερασμένου πλήθους φορών των ρητών πράξεων. Τα γράμματα $a_1, \ldots, a_n$ αποτελούν γλώσσες της κλάσης $\mathcal{L}$, συνεπώς από την υπόθεσή μας για την κλάση $\mathcal{L}$ συνάγουμε ότι $L \in \mathcal{L}$, και η απόδειξή μας τελείωσε. □

Παράδειγμα 19 *Δίνεται το αλφάβητο $A = \{a, b, c, d\}$. Θα δείξουμε ότι η γλώσσα από το A που περιέχει ακριβώς όλες τις λέξεις που περιέχουν μία εμφάνιση του a είναι ρητή. Πράγματι η γλώσσα αυτή είναι η*

$$(b \cup c \cup d)^* a (b \cup c \cup d)^*.$$

Παράδειγμα 20 *Δίνεται το αλφάβητο $A = \{a, b, c, d\}$. Θα δείξουμε ότι η γλώσσα από το A που περιέχει ακριβώς όλες τις λέξεις που περιέχουν τρείς εμφανίσεις του a είναι ρητή. Πράγματι η γλώσσα αυτή είναι η*

$$(b \cup c \cup d)^* a (b \cup c \cup d)^* a (b \cup c \cup d)^* a (b \cup c \cup d)^*.$$

Παράδειγμα 21 *Δίνεται το αλφάβητο $A = \{a, b, c, d, e\}$. Θα δείξουμε ότι η γλώσσα από το A που περιέχει ακριβώς όλες τις λέξεις που περιέχουν δύο εμφανίσεις του a και δύο εμφανίσεις του c είναι ρητή. Παρατηρούμε ότι σε κάθε λέξη της γλώσσας αυτής, τα δύο a και τα δύο c θα εμφανίζονται με τη σειρά*

i) *a, a, c, c, δηλαδή η λέξη θα ανήκει στο σύνολο*

$$L_1 = (b \cup d \cup e)^* a (b \cup d \cup e)^* a (b \cup d \cup e)^* c (b \cup d \cup e)^* c (b \cup d \cup e)^*$$

ή

ii) *a, c, a, c, δηλαδή η λέξη θα ανήκει στο σύνολο*

$$L_2 = (b \cup d \cup e)^* a (b \cup d \cup e)^* c (b \cup d \cup e)^* a (b \cup d \cup e)^* c (b \cup d \cup e)^*$$

ή

iii) *a, c, c, a, δηλαδή η λέξη θα ανήκει στο σύνολο*

$$L_3 = (b \cup d \cup e)^* a (b \cup d \cup e)^* c (b \cup d \cup e)^* c (b \cup d \cup e)^* a (b \cup d \cup e)^*$$

ή

iv) *c, a, c, a, δηλαδή η λέξη θα ανήκει στο σύνολο*

$$L_4 = (b \cup d \cup e)^* c (b \cup d \cup e)^* a (b \cup d \cup e)^* c (b \cup d \cup e)^* a (b \cup d \cup e)^*$$

ή

v) c, c, a, a, δηλαδή η λέξη θα ανήκει στο σύνολο

$$L_5 = (b \cup d \cup e)^* c (b \cup d \cup e)^* c (b \cup d \cup e)^* a (b \cup d \cup e)^* a (b \cup d \cup e)^*$$

ή

vi) c, a, a, c, δηλαδή η λέξη θα ανήκει στο σύνολο

$$L_6 = (b \cup d \cup e)^* c (b \cup d \cup e)^* a (b \cup d \cup e)^* a (b \cup d \cup e)^* c (b \cup d \cup e)^*.$$

Άρα η η γλώσσα είναι η

$$L_1 \cup L_2 \cup L_3 \cup L_4 \cup L_5 \cup L_6$$

που είναι ρητή καθώς οι $L_1, L_2, L_3, L_4, L_5, L_6$ είναι όλες ρητές.

Στη συνέχεια θα αποδείξουμε το θεώρημα του *Kleene*. Για αυτό θα μας χρειαστούν οι δύο επόμενες προτάσεις.

Πρόταση 23 *Αν $L \in \mathrm{Rat}(A)$, τότε $L \in \mathrm{Rec}(A)$.*

Απόδειξη Κάθε πεπερασμένη γλώσσα είναι αναγνωρίσιμη (βλ. Άσκηση 13, Κεφάλαιο 4). Επίσης, σύμφωνα με τις Προτάσεις 6, 11 και 12, η κλάση των αναγνωρισίμων γλωσσών είναι κλειστή με τις ρητές πράξεις. Έτσι συνάγουμε την απόδειξή μας χρησιμοποιώντας την Πρόταση 22. □

Πρόταση 24 *Αν $L \in \mathrm{Rec}(A)$, τότε $L \in \mathrm{Rat}(A)$.*

Απόδειξη Θεωρούμε μια γλώσσα $L \in \mathrm{Rec}(A)$ και ένα CFA $\mathcal{A} = (Q, A, q_0, \delta, F)$ που την αναγνωρίζει. Έστω $Q = \{q_0, q_1, \ldots, q_n\}$. Για κάθε $0 \leq i, j \leq n$ και $k \geq 0$ ονομάζουμε $P_{ij}^{(k)}$ το σύνολο των διαδρομών του αυτομάτου που ξεκινούν από την κατάσταση q_i, καταλήγουν στην κατάσταση q_j, και δεν περνούν από καταστάσεις με δείκτη μεγαλύτερο ή ίσο του k. Θέτουμε $L_{ij}^{(k)}$ για τη γλώσσα των μη κενών λέξεων που εμφανίζονται σε όλες τις παραπάνω διαδρομές. Θα αποδείξουμε ότι για $0 \leq i, j \leq n$, $k \geq 0$ η γλώσσα $L_{ij}^{(k)}$ είναι ρητή. Θα χρησιμοποιήσουμε επαγωγή στο k. Για $k = 0$ έχουμε

$$L_{ij}^{(k)} = \{a \mid a \in A \text{ και } \delta(q_i, a) = q_j\}$$

που είναι προφανώς ρητή γλώσσα. Υποθέτουμε ότι ο ισχυρισμός μας ισχύει για $k > 0$. Τότε για κάθε διαδρομή (Δ) του $P_{ij}^{(k+1)}$ διακρίνουμε δύο περιπτώσεις.
(i) Η κατάσταση q_k δεν εμφανίζεται στην (Δ). Αυτό σημαίνει ότι η $(\Delta) \in P_{ij}^{(k)}$.
(ii) Η κατάσταση q_k εμφανίζεται στην (Δ). Τότε η (Δ) θα είναι της μορφής

$$(\Delta): \qquad q_i \overset{w_1}{\rightsquigarrow} q_k \overset{w_2}{\rightsquigarrow} q_k \ldots q_k \overset{w_{m-1}}{\rightsquigarrow} q_k \overset{w_m}{\rightsquigarrow} q_j$$

όπου οι διαδρομές

$$
\begin{aligned}
(\Delta_1): &\qquad q_i \overset{w_1}{\rightsquigarrow} q_k,\\
(\Delta_2): &\qquad q_k \overset{w_2}{\rightsquigarrow} q_k,\\
&\qquad \ldots\\
(\Delta_{m-1}): &\qquad q_k \overset{w_{m-1}}{\rightsquigarrow} q_k,\\
(\Delta_m): &\qquad q_k \overset{w_m}{\rightsquigarrow} q_j
\end{aligned}
$$

περνούν από καταστάσεις με δείκτη το πολύ $k-1$.
Από τα παραπάνω συνάγουμε ότι

$$L_{ij}^{(k+1)} \subseteq L_{ij}^{(k)} \cup L_{ik}^{(k)} \left(L_{kk}^{(k)}\right)^* L_{kj}^{(k)}.$$

Ο αντίστροφος εγκλεισμός είναι προφανής από τον ορισμό των γλωσσών $L_{ij}^{(k+1)}$. Έτσι συνάγουμε ότι

$$L_{ij}^{(k+1)} = L_{ij}^{(k)} \cup L_{ik}^{(k)} \left(L_{kk}^{(k)}\right)^* L_{kj}^{(k)}.$$

Από την υπόθεση της επαγωγής, οι γλώσσες $L_{ij}^{(k)}, L_{ik}^{(k)}, L_{kk}^{(k)}, L_{kj}^{(k)}$ είναι ρητές και συνεπώς η γλώσσα $L_{ij}^{(k+1)}$ είναι και αυτή ρητή.

Υποθέτουμε τώρα ότι $F = \{q_{i_1}, \ldots, q_{i_m}\}$ για κάποια $0 \leq i_1 < \ldots < i_m \leq n$. Φανερά ισχύει

$$L = L_{0i_1}^{(n+1)} \cup \ldots \cup L_{0i_m}^{(n+1)}$$

αν η $q_0 \notin F$, ενώ

$$L = L_{0i_1}^{(n+1)} \cup \ldots \cup L_{0i_m}^{(n+1)} \cup \{\varepsilon\}$$

αν η $q_0 \in F$. Συνεπώς σε κάθε περίπτωση η γλώσσα L είναι ρητή. □

Θεώρημα 5 *(Kleene 1956)* $\mathrm{Rec}(A) = \mathrm{Rat}(A)$.

Απόδειξη Προκύπτει άμεσα από τις Προτάσεις 23 και 24. □

Ασκήσεις

1) Δίνεται αλφάβητο A και έστω $a, b \in A$. Να αποδείξετε ότι οι γλώσσες

$$A^*, \quad a^3A^3b^3, \quad a^*(A^*)^*b^5, \quad (((A^*)^*)^*)^*$$

είναι ρητές.

2) Δίνεται το αλφάβητο $A = \{a, b, c, d\}$. Να αποδείξετε ότι η γλώσσα από το A που περιέχει ακριβώς όλες τις λέξεις που δεν περιέχουν καμία εμφάνιση του a είναι ρητή.

3) Δίνεται το αλφάβητο $A = \{a, b, c, d, e, f\}$. Να αποδείξετε ότι η γλώσσα από το A που περιέχει ακριβώς όλες τις λέξεις που περιέχουν μία εμφάνιση του a, μία εμφάνιση του d και μία εμφάνιση του f είναι ρητή.

4) Δίνεται το αλφάβητο $A = \{a, b, c, d, e, f\}$. Να αποδείξετε ότι η γλώσσα από το A που περιέχει ακριβώς όλες τις λέξεις που περιέχουν δύο εμφανίσεις του a, μία εμφάνιση του d και μία εμφάνιση του f είναι ρητή.

5) Να κατασκευάσετε πεπερασμένα αυτόματα που να αναγνωρίζουν τις παρακάτω ρητές γλώσσες

$$a^*b^*, \quad a^*b^*c^3, \quad a^*b^*(ab \cup b^5), \quad (ab)^* \cup b^2(a^3), \quad b^5a^4((ab)^*)^*.$$

6) Να δείξετε ότι η γλώσσα $\{a^nb^n \mid n \geq 0\}$ δεν είναι ρητή.

7) Δίνεται το αλφάβητο $A = \{a, b, c, d\}$. Να αποδείξετε ότι η γλώσσα από το A που περιέχει ακριβώς όλες τις λέξεις που περιέχουν ίσες εμφανίσεις του a και του d δεν είναι ρητή.

8) Δίνεται αλφάβητο A. Να εξετάσετε αν η κλάση $\mathrm{Rat}(A)$ είναι κλειστή με την πράξη της τομής.

9) Δίνεται αλφάβητο A. Να εξετάσετε αν η κλάση $\mathrm{Rat}(A)$ είναι κλειστή με την πράξη του συμπληρώματος.

10) Δίνεται αλφάβητο A και ρητή γλώσσα $L \in \mathrm{Rat}(A)$. Μπορούμε να αποφασίσουμε αν

   i) $L = \emptyset$;

   ii) $L = A^*$;

11) Δίνεται αλφάβητο A και ρητές γλώσσες $L, M \in \mathrm{Rat}(A)$. Μπορούμε να αποφασίσουμε αν $L \subseteq M$;

12) Δίνεται αλφάβητο A και ρητές γλώσσες $L, M \in \mathrm{Rat}(A)$. Μπορούμε να αποφασίσουμε αν $L = M$;

13) Δίνεται αλφάβητο A και ρητές γλώσσες $L, M \in \mathrm{Rat}(A)$. Να εξετάσετε αν η ελάχιστη λύση της εξίσωσης

$$X = LX \cup M$$

είναι ρητή ή όχι.

14) Δίνεται αλφάβητο A και αναγνωρίσιμες γλώσσες $L, M \in \mathrm{Rec}(A)$. Να εξετάσετε αν η ελάχιστη λύση της εξίσωσης

$$X = LX \cup M$$

είναι αναγνωρίσιμη ή όχι.

Βιβλιογραφία

Αγγλική

[1] M. Droste, W. Kuich, H. Vogler eds., *Handbook of Weighted Automata*, Monographs in Theoretical Computer Science. An EATCS Series, Springer, 2009.

[2] S. Eilenberg, *Automata, Languages and Machines*, volume A, Academic Press, New York, 1974.

[3] S. Eilenberg, *Automata, Languages and Machines*, volume B, Academic Press, New York, 1976.

[4] J.E. Hopcroft, R. Motwani, J.D. Ullman, *Introduction to Automata Theory, Languages and Computation*, 3rd edition, Pearson, 2006.

[5] J. Hromkovič, *Theoretical Computer Science: Introduction to Automata, Computability, Complexity, Algorithmics, Randomization, Communication, and Cryptography.* Texts in Theoretical Computer Science. An EATCS Series, Springer, 2004.

[6] B. Khoussainov, A. Nerode, *Automata Theory and its Applications*, Birkhäuser, 2001.

[7] H. Lewis, Ch. Papadimitriou, *Elements of the Theory of Computation*, 2nd edition, Prentice-Hall, 1997.

[8] J.-É. Pin, *Handbook of Automata Theory, volume I, Theoretical Foundations*, European Mathematical Society Press, 2021.

[9] J.-É. Pin, *Handbook of Automata Theory, volume II, Automata in Mathematics and Selected Applications*, European Mathematical Society Press, 2021.

[10] G. Rozenberg, A. Salomaa eds., *Handbook of Formal Languages, volume 1, Word, Language Grammar*, Springer, 1997.

[11] G. Rozenberg, A. Salomaa eds., *Handbook of Formal Languages, volume 2, Linear Modeling: Background and Application*, Springer, 1997.

[12] G. Rozenberg, A. Salomaa eds., *Handbook of Formal Languages, volume 3, Beyond Words*, Springer, 1997.

[13] J. Sakarovitch, *Elements of Automata Theory*, Cambridge, 2009.

[14] A. Salomaa, *Formal Languages*, Academic Press, New York, 1973.

[15] A. Thue, Über nendliche Zeichenreihen, *Norske Vid. Selsk. Skr. I Mat. Nat. Kl.,* Kristriania 7(1906) 1–22.

[16] W. Wechler, *Universal Algebra for Computer Scientists*, Monographs in Theoretical Computer Science. An EATCS Series, Springer, 1992.

Ελληνική

[17] Σ. Μποζαπαλίδη, *Μαθηματικά και Πληροφορική*, Θεσσαλονίκη, 1997.

[18] Σ. Μποζαπαλίδη, *Αυτόματα, Γλώσσες, Γραμματικές*, Θεσσαλονίκη, 1997.