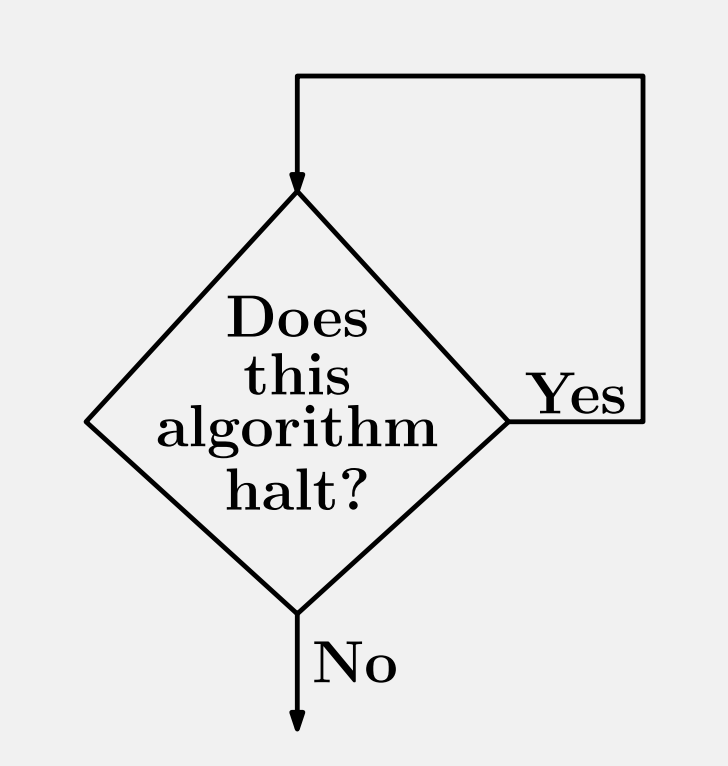
(Πρόχειρες) σημειώσεις στη ΘΕΩΡΙΑ ΑΝΑΔΡΟΜΗΣ



Δημήτρης Ζώρος

Μεταπτυχιακό Πρόγραμμα Λογική και Διακριτά Μαθηματικά-2016

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΑΛΓΟΡΙΘΜΟΙ, ΛΟΓΙΚΗ ΚΑΙ ΔΙΑΚΡΙΤΑ ΜΑΘΗΜΑΤΙΚΑ»

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 0

ΕΙΣΑΓΩΓΗ

Οι πρωτοποριακές εργασίες του *Georg Cantor* που έμελε να γεννήσουν τη Θεωρία Συνόλων (της θεωρίας που ενοποιεί το σύνολο των μαθηματικών που χρησιμοποιούμε) είχαν μία πάρα πολύ σημαντική αδυναμία: την *Αρχή της Συμπερίληψης*. Σύμφωνα με αυτήν την αρχή, η συλλογή οποιονδήποτε αντικειμένων που ικανοποιούν κάποια συγκεκριμένη ιδιότητα αποτελεί ένα σύνολο. Η αρχή αυτή καθαυτή δεν είναι εσφαλμένη, η μη ελεγχόμενη εφαρμογή της όμως μας οδηγεί σε διάφορα παράδοξα. Παραδείγματος χάρη, μπορούμε να ορίσουμε το σύνολο $\{x \mid x \notin x\}$ (το σύνολο όλων των συνόλων που δεν ανήκουν στον εαυτό τους) ή ακόμα το σύνολο $\{x \mid x = x\}$ (το σύνολο όλων των συνόλων). Ο *Bertrand Russell* το 1901 παρατήρησε ότι αυτά τα σύνολα δεν μπορούν να υπάρξουν [1] και διατύπωσε το γνωστό *Παράδοξο του Russell*. Τέτοιου είδους παράδοξα κλόνισαν τα θεμέλια των μαθηματικών και ώθησαν τους μαθηματικούς στην αναζήτηση τρόπων να εξαλειφθούν. Σε αντίθετη περίπτωση υπήρχε ο κίνδυνος να απορριφθούν οι θεωρίες και τα αποτελέσματα που είχαν μέχρι τότε αποδειχθεί ως αίολα. Ο μόνος τρόπος να αποφευχθεί αυτό ήταν να τεθούν συγκεκριμένα *Αξιώματα* (κοινώς αποδεχτές αλήθειες, για τις οποίες δεν απαιτείται απόδειξη) και να θεμελιωθούν τα μαθηματικά πάνω σε αυτά, έτσι ώστε οι μαθηματικές αλήθειες να είναι τυπικές απόρροιές τους. Ο *David Hilbert* εξέφρασε ρητά αυτόν τον στόχο στο λεγόμενο *Πρόγραμμα του Hilbert*:

> *« ...Να θεμελιωθούν οι υπάρχουσες θεωρίες πάνω σε ένα πεπερασμένο σύνολο αξιωμάτων που θα μπορεί να αποδείξει όλες τις αλήθειες της εκάστοτε θεωρίας. Επιπλέον θα πρέπει αυτό το σύνολο αξιωμάτων να είναι συνεπές... »*

Ως αφετηρία για το εγχείρημα πρότεινε τη στοιχειώδη αριθμητική (στους φυσικούς αριθμούς), έχοντας κατά νου ότι η συνέπεια των υπόλοιπων θεωριών θα μπορούσε να προκύψει μέσα από τη συνέπεια της αριθμητικής. Πιο συγκεκριμένα τα στάδια του προγράμματος ήταν τα ακόλουθα:

[1] Μπορείτε να δείτε γιατί;

1. *Φορμαλισμός Μαθηματικών:* Εδραίωση μίας γλώσσας ικανής να εκφράσει τις μαθηματικές προτάσεις με σαφή και (κυρίως) τυπικό τρόπο. Ο φορμαλισμός αυτός θα περιέχει και το αξιωματικό σύστημα μέσα από το οποίο θα αποδεικνύονται οι αληθείς μαθηματικές εκφράσεις της γλώσσας.

Στον φορμαλισμό αυτό, *τυπική απόδειξη* μιας πρότασης θα είναι μία πεπερασμένη ακολουδία προτάσεων που θα καταλήγει στην προς απόδειξη πρόταση (δες Παράγραφο Α.3). Συνεπώς, όχι μόνο οι προτάσεις (εκφρασμένες τυπικά στη γλώσσα) αλλά ακόμα και οι αποδείξεις τους (ως ακολουδίες εκφράσεων) θα αποτελούν σαφώς ορισμένα μαθηματικά αντικείμενα.

Τα αξιώματα που θα επιλεγούν θα πρέπει απαραιτήτως να ικανοποιούν τις ακόλουθες ιδιότητες:

2. *Συνέπεια:* Στα πλαίσια του αξιωματικού συστήματος δεν μπορεί να προκύψει κάποια αντίφαση.

3. *Πληρότητα:* Κάθε αληθής μαθηματική πρόταση μπορεί να αποδειχδεί τυπικά στα πλαίσια του αξιωματικού συστήματος.

Μάλιστα, η συνέπεια και η πληρότητα θα πρέπει να μπορούν να αποδειχδούν μέσα από το αξιωματικό σύστημα (καθώς και αυτές μπορούν να εκφραστούν ως προτάσεις της γλώσσας).

Η αναζήτηση απόδειξης στον φορμαλισμό αυτό δεν θα αποτελεί αναζήτηση μιας ακολουδίας «επιχειρημάτων» εκφρασμένα σε κάποια φυσική γλώσσα, αλλά θα αποτελεί έλεγχο για την ύπαρξη ενός μαθηματικού αντικειμένου με συγκεκριμένες ιδιότητες. Αυτό ενέπνευσε τον Hilbert να οραματιστεί την ύπαρξη συστηματικής διαδικασίας που θα φέρνει εις πέρας αυτόν τον έλεγχο:

4. *Αποφανσιμότητα:* Εύρεση μίας πεπερασμένης διαδικασίας που θα αποφασίζει αν μία δοσμένη μαθηματική πρόταση (εκφρασμένη στην τυπική γλώσσα) είναι αληθής ή ψευδής (το πρόβλημα αυτό είναι γνωστό ως *Entscheidungsproblem* [1]).

Το πρόγραμμα του Hilbert αποτέλεσε ίσως τη μεγαλύτερη πηγή έμπνευσης για τους μαθηματικούς του εικοστού αιώνα. Δυστυχώς όμως πολύ γρήγορα αποδείχθηκε ότι δεν μπορεί να πετύχει:

- Όσον αφορά τον φορμαλισμό, η Μαθηματική Λογική και η «γλώσσα» που χρησιμοποιεί έχει τη δυνατότητα να τυποποιήσει τόσο την αριθμητική όσο και γενικότερα το σύνολο των μαθηματικών (αυτή η πτυχή του προγράμματος στέφθηκε με επιτυχία).

- Όσον αφορά όμως την συνέπεια/πληρότητα του συστήματος που χρησιμοποιείται π.χ. στην αριθμητική, ο *Kurt Gödel* το 1931 έδειξε ότι αυτές είναι δύο ιδιότητες που δεν μπορούν να ισχύουν ταυτόχρονα (δες Θεώρημα 7.3.8 ή *Πρώτο Θεώρημα Μη-πληρότητας* στη βιβλιογραφία).

Για να το δείξει αυτό υπέθεσε ότι η αριθμητική είναι συνεπής και κατασκεύασε μια πρόταση που ενώ είναι αληθής δεν μπορεί να αποδειχδεί. Το πρόβλημα στην ουσία δεν ήταν η

[1] Ελεύθερη μετάφραση: *Το Πρόβλημα Απόφασης Λογικών Θεωριών.*

συγκεκριμένη πρόταση, καθώς ακόμα και αν θεωρηθεί και αυτή αξίωμα τότε θα υπάρξει άλλη αληθής πρόταση που δεν μπορεί να αποδειχθεί. Το πρόβλημα είναι θεμελιώδες και καταδυκνείει το γεγονός ότι στην πραγματικότητα σε οποιονδήποτε φορμαλισμό των μαθηματικών θα υπάρχουν πάντα τριών ειδών προτάσεις: οι αληθείς, οι ψευδής και οι *μη αποδείξιμες*.

Το δεύτερο πλήγμα στο πρόγραμμα του Hilbert δόθηκε και πάλι από τον Gödel καθώς έδειξε ότι εφόσον η αριθμητική είναι συνεπής, η συνέπειά της δεν μπορεί να αποδειχθεί μέσα στα πλαίσιά της: Υπάρχει πρόταση στη γλώσσα της αριθμητικής που εκφράζει το γεγονός ότι η αριθμητική είναι συνεπής, η οποία όμως δεν μπορεί να αποδειχθεί (*Δεύτερο Θεώρημα Μη-πληρότητας*).

Εμάς το ενδιαφέρον μας θα στραφεί στο Entscheidungsproblem, καθώς αυτό αποτέλεσε την απαρχή της *Θεωρίας Αναδρομής* ή *Θεωρία Υπολογισιμότητας*. Δυστυχώς [1] η απάντηση και σε αυτό το πρόβλημα είναι αρνητική (δες Θεώρημα 8.5.12), αν και οι περισσότεροι αναγνώστες θα αναρωτιούνται τι ακριβώς αποτελεί απάντηση στο Entscheidungsproblem. Αν υπήρχε πεπερασμένη διαδικασία ή *Αλγόριθμος* που αποφασίζει αν μία πρόταση είναι αληθής ή όχι, τότε το μόνο που θα είχαμε να κάνουμε θα ήταν να περιγράψουμε τον αλγόριθμο με σαφή τρόπο και έτσι θα απαντούσαμε θετικά. Για να αποδείξουμε όμως ότι δεν υπάρχει τέτοιος αλγόριθμος θα πρέπει αρχικά να δώσουμε έναν ορισμό της έννοιας του αλγορίθμου ως μαθηματικό αντικείμενο. Έπειτα, με μαθηματικές μεθόδους θα πρέπει να δείξουμε ότι το εν λόγω αντικείμενο δεν μπορεί να υπάρξει.

Την εποχή εκείνη προτάθηκαν πολλές και διαφορετικές «προσεγγίσεις» της έννοιας του αλγορίθμου και πολλοί φορμαλισμοί της έννοιας του *Υπολογισμού*, όμως όλες αποδείχθηκαν ισοδύναμες. Αυτό οδήγησε στη λεγόμενη *Θέση Church-Turing* [2] (δες Σελίδα 115) και την τοποθέτηση του Entscheidungsproblem σε αυστηρές μαθηματικές βάσεις. Η θέση φέρει τα ονόματα των *Alonzo Church* και *Alan Turing* δύο ερευνητών που το 1935 και 1936, ανεξάρτητα ο ένας από τον άλλον, απέδειξαν ότι το Entscheidungsproblem δεν επιδέχεται λύσης καθώς δεν μπορεί να υπάρξει *λ-όρος* (Κεφάλαιο 3) ή *Μηχανή Turing* (Κεφάλαιο 1) που να το «λύνει».

Αυτήν την ιστορία θα αναπτύξουμε στις σημειώσεις που ακολουθούν, επισκεπτόμενοι μερικά από τα σημαντικότερα αποτελέσματα που γέννησε. Στο υπόλοιπο του Κεφαλαίου 0 θα εδραιώσουμε τον συμβολισμό που θα χρησιμοποιήσουμε στη συνέχεια και θα υπενθυμίσουμε κάποιους βασικούς ορισμούς από τη Θεωρία Συνόλων.

Έπειτα οι σημειώσεις θα χωρισθούν σε δύο μέρη. Το πρώτο παρουσιάζει τέσσερις από τους σημαντικότερους φορμαλισμούς της Θεωρίας Αναδρομής (τα λεγόμενα και *Μοντέλα Υπολογισμού*), καθώς και τις αποδείξεις ισοδυναμίας μεταξύ μερικών εξ αυτών. Στο κομμάτι αυτό των σημειώσεων θα θεμελιώσουμε την έννοια του αλγορίθμου και, εφόσον πλέον έχει καλλιεργηθεί μέσα μας η πεποίηθηση ότι η Θέση Church-Turing είναι μια εύλογη παραδοχή, θα υιοθετήσουμε τον φορμαλισμό που εισήγαγε ο Turing (για λόγους που θα συζητηθούν στη συνέχεια) και θα περάσουμε στο δεύτερο και πιο βασικό μέρος της Θεωρίας, την *Υπολογισιμότητα*.

[1] Δυστυχώς για το πρόγραμμα του Hilbert, ευτυχώς για τους μαθηματικούς, καθώς θετική απάντηση στο Entscheidungsproblem θα σήμαινε ότι πλέον η δουλειά τους θα περιοριζόταν μόνο στο να κάνουν τις ερωτήσεις και όχι στο να βρίσκουν και τις απαντήσεις!

[2] Θα μπορούσαμε να πούμε ότι η θέση αυτή είναι ο ζητούμενος τυπικός ορισμός της έννοιας του αλγορίθμου.

0.1 Σχέσεις και συναρτήσεις

Συμβολισμός 0.1.1. Στις σημειώσεις αυτές χρησιμοποιούνται κατά κόρον τα ακόλουθα σύμβολα:

$$\varnothing,\ \in,\ 2^A,\ \cup,\ \cap,\ \subseteq,\ \setminus,\ \overline{A},\ |A|,\ \times,\ \wedge,\ \vee,\ \neg,\ \to,\ \leftrightarrow,\ \forall,\ \exists,\ \text{όπου } A \text{ σύνολο}$$

Θεωρούμε ότι ο αναγνώστης είναι στοιχειωδώς εξοικειωμένος με αυτά [1].

Συμβολισμός 0.1.2. Με $\mathbb{N}$ συμβολίζουμε το σύνολο των φυσικών αριθμών [2] και με $\mathbb{Z}$ το σύνολο των ακεραίων αριθμών. Για οικονομία χώρου θα γράφουμε $[n]$ αντί για $\{1, \dots, n\}$, όπου $n \in \mathbb{N} \setminus \{0\}$. Τέλος, με $\mathbb{R}$ συμβολίζουμε το σύνολο των πραγματικών αριθμών.

Ορισμός 0.1.3. P είναι μία *n-μελής σχέση* στο σύνολο A ανν [3] $P \subseteq A^n$ [4], όπου $n \in \mathbb{N} \setminus \{0\}$.

Ορισμός 0.1.4. $\mathcal{R}$ είναι μία *ιδιότητα* του σύνολου A ανν $\mathcal{R} \subseteq 2^A$.

Ορισμός 0.1.5. Η *ανακλαστική* ιδιότητα του συνόλου A^2 είναι η $\mathcal{R}^A_{\text{αν}} = \{P \subseteq A^2 \mid (a,a) \in P \text{ για κάθε } a \in A\}$. Η *μεταβατική* ιδιότητα του συνόλου A^2 είναι η $\mathcal{R}^A_{\text{μετ}} = \{P \subseteq A^2 \mid \text{Αν } (a,b),(b,c) \in P \text{ τότε και } (a,c) \in P\}$.

Ορισμός 0.1.6. Μία διμελής σχέση $P \subseteq A^2$ καλείται *μεταβατική* ανν $P \in \mathcal{R}^A_{\text{μετ}}$.

Ορισμός 0.1.7. Έστω διμελής σχέση $P \subseteq A \times B$, και ιδιότητα $\mathcal{R} \subseteq 2^{A \times B}$. Η *κλειστότητα της P ως προς τη $\mathcal{R}$* είναι η σχέση $P^{\mathcal{R}}$ που προκύπτει από την P αν προσθέσουμε το ελάχιστο απαραίτητο πλήθος ζευγών ώστε $P^{\mathcal{R}} \in \mathcal{R}$.

Παράδειγμα 0.1.8. Η *μεταβατική κλειστότητα* της σχέσης $\{(n,m) \in \mathbb{N}^2 \mid m = n+1\}$ είναι η σχέση $\{(n,m) \in \mathbb{N}^2 \mid n < m\}$. Η *ανακλαστική κλειστότητα* της σχέσης $\{(n,m) \in \mathbb{N}^2 \mid n < m\}$ είναι η σχέση $\{(n,m) \in \mathbb{N}^2 \mid n \leq m\}$.

Ορισμός 0.1.9. f είναι *συνάρτηση από το A στο B*, συμβολισμός $f : A \to B$, ανν

- f διμελής σχέση και
- $((a,b_1) \in f \wedge (a,b_2) \in f) \to b_1 = b_2$.

Αν $(a,b) \in f$ θα γράφουμε $f(a) = b$.

Ορισμός 0.1.10. Έστω $f : A \to B$.

- Το *πεδίο ορισμού* της f είναι το σύνολο $\mathsf{dom}(f) = \{a \in A \mid f(a) \in B\}$.

[1] Για περισσότερες πληροφορίες ανατρέξτε στο [8].

[2] Το 0 θεωρείται φυσικός αριθμός. Στη Θεωρία Συνόλων ορίζεται ως το σύνολο $\varnothing$.

[3] Παρακαλώ μην συγκαταλέξετε το «ανν» στη λίστα των τυπογραφικών λαθών αυτών των σημειώσεων. Το χρησιμοποιούμε σαν συντόμευση του «αν και μόνο αν».

[4] $A^n = \underbrace{A \times \cdots \times A}_{n\text{-φορές}}$

- Το *πεδίο τιμών* της f είναι το σύνολο $\mathsf{im}(f) = \{b \in B \mid \exists a \in A(f(a) = b)\}$.
- Η f είναι *επί του* B ανν $\forall b \in B\ \exists a \in \mathsf{dom}(f)(f(a) = b)$ [1].
- Η f είναι *ένα προς ένα (1-1)* ανν $(f(a_1) = b \wedge f(a_2) = b) \to a_1 = a_2$.

Ορισμός 0.1.11. Έστω $f : A \to B$. Η f είναι *μερική συνάρτηση* ανν $\exists a \in A(a \notin \mathsf{dom}(f))$. Σε αυτήν την περίπτωση θα γράφουμε $f(a) = \perp$, όπου $\perp \notin A \cup B$ [2]. Μία συνάρτηση που δεν είναι μερική καλείται *ολική συνάρτηση* (ή *πλήρης*).

Παράδειγμα 0.1.12. Θεωρήστε τη συνάρτηση $f : \mathbb{R} \to \mathbb{R}$ με $f(x) = \sqrt{x}$. Η f προφανώς είναι μερική συνάρτηση, καθώς για οποιοδήποτε $r < 0$ ισχύει ότι $r \notin \mathsf{dom}(f)$ (ή αλλιώς $f(r) = \perp$).

Ορισμός 0.1.13. Έστω $f : A \to B$ 1-1 συνάρτηση. Η *αντίστροφη συνάρτηση της* f είναι η συνάρτηση $f^{-1} : \mathsf{im}(f) \to \mathsf{dom}(f)$ με $f^{-1}(x) = y$, όπου το y είναι τέτοιο ώστε $f(y) = x$.

Ορισμός 0.1.14. Έστω $f : A \to B$ και $g : B \to C$. Η *σύνθεση των* f *και* g είναι η συνάρτηση $g \circ f : A \to C$ με:

$$g \circ f(x) = \begin{cases} g(f(x)) & , \text{ αν } x \in \mathsf{dom}(f) \\ \perp & , \text{ αλλιώς} \end{cases}$$

Ορισμός 0.1.15. Έστω σύνολο B. Η *χαρακτηριστική συνάρτηση* $\chi_A : B \to \{0, 1\}$ ενός συνόλου $A \subseteq B$ ορίζεται ως εξής:

$$\chi_A(a) = \begin{cases} 1 & , \text{αν } a \in A \\ 0 & , \text{αλλιώς} \end{cases}$$

Ορισμός 0.1.16. Ένα σύνολο A είναι *πεπερασμένο* αν $|A| \in \mathbb{N}$ και *άπειρο* αν $|A| \notin \mathbb{N}$. Δύο σύνολα A, B είναι *ισοπληθικά* ανν υπάρχει 1-1 και επί συνάρτηση $f : A \to B$.Ένα σύνολο A είναι *αριθμησίμως άπειρο* αν είναι ισοπληθικό με το $\mathbb{N}$ (σε αυτήν την περίπτωση θα γράφουμε $|A| = \aleph_0$).

Θεώρημα 0.1.17. Για κάθε σύνολο A ισχύει ότι $|A| < |2^A|$ [3].

Απόδειξη. Έστω (προς άτοπο) 1-1 και επί συνάρτηση $f : A \to 2^A$. Θεωρούμε το σύνολο $B = \{x \in A \mid x \notin f(x)\}$. Αφού $B \subseteq A$ και η f είναι επί του 2^A, υπάρχει $b \in A$ τέτοιο ώστε $f(b) = B$. Όμως τότε $b \in B$ ανν $b \notin B$. Άτοπο. □

Κλείνοντας αυτή την παράγραφο, να αναφέρουμε ότι στο Κεφάλαιο 2 που πραγματευόμαστε συναρτήσεις φυσικών αριθμών χρησιμοποιούμε τα σύμβολα:

$$x! : \text{το παραγοντικό του } x$$
$$x \bmod y : \text{το υπόλοιπο της διαίρεσης του } x \text{ με το } y$$
$$x \mid y : \text{το } x \text{ διαιρεί το } y$$

[1] Κάθε συνάρτηση f είναι επί του $\mathsf{im}(f)$.

[2] Επομένως ισχύει ότι $f(\perp) = \perp$ αφού $\perp \notin \mathsf{dom}(f)$. Το σύμβολο $\perp$ συνήθως καλείται *πάτος*.

[3] Εδώ το σύμβολο $<$ επεκτείνεται πέρα από το $\mathbb{N}$ στους άπειρους πληθάριθμους

0.2 Λέξεις και γλώσσες

Ορισμός 0.2.1. *Αλφάβητο* είναι ένα πεπερασμένο σύνολο συμβόλων.

Παράδειγμα 0.2.2. Παραδείγματα αλφαβήτων είναι τα ακόλουθα:

- $\{0, 1\}$
- $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
- $\{q, w, e, r, t, y, u, i, o, p, a, s, d, f, g, h, j, k, l, z, x, c, v, b, n, m, \ , ., ?, !\}$ [1]

Ορισμός 0.2.3. Μία *λέξη* (ή *συμβολοσειρά*) του αλφάβητου Σ είναι μια πεπερασμένη ακολουθία συμβόλων του Σ.

Παράδειγμα 0.2.4.

- 101010101010110 είναι μία λέξη του $\{0, 1\}$
- 1917 είναι μία λέξη του $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
- $mpla$ είναι μια λέξη του $\{q, w, e, r, t, y, u, i, o, p, a, s, d, f, g, h, j, k, l, z, x, c, v, b, n, m, \sqcup, ., ?, !\}$

Ορισμός 0.2.5. Έστω w μία λέξη του αλφάβητου Σ. Το *μήκος* της w, συμβολισμός $|w|$, είναι το πλήθος συμβόλων της [2].

Παράδειγμα 0.2.6.

- $|101010101010110| = 15$
- $|1917| = 4$
- $|mpla| = 4$

Συμβολισμός 0.2.7.

- Με ϵ συμβολίζουμε την *κενή λέξη*, δηλαδή τη μοναδική λέξη με μήκος 0.
- Ορίζουμε τα σύνολα $\Sigma^i = \{w \text{ λέξη του } \Sigma \mid |w| = i\}$, $i \in \mathbb{N}$.
- Η *κλειστότητα Kleene (Kleene Star)* του Σ είναι το σύνολο:

$$\Sigma^* = \bigcup_{i \in \mathbb{N}} \Sigma^i$$

Το σύνολο αυτό περιέχει όλες τις (πεπερασμένου μήκους) λέξεις που μπορούν να κατασκευαστούν με σύμβολα από το Σ.

[1] Για λόγους ευκρίνειας για το σύμβολο του κενού θα χρησιμοποιούμε το σύμβολο $\sqcup$.
[2] Μετράμε κάθε εμφάνιση του ίδιου συμβόλου.

- Έστω λέξη w ενός αλφαβήτου. Με w^R συμβολίζουμε την *αντίστροφη λέξη* της w. Για παράδειγμα $mpla^R = alpm$.

Ορισμός 0.2.8. Έστω $w_1 = x_1 \cdots x_m$ και $w_2 = y_1 \cdots y_n$ δύο λέξεις στο Σ^*. Η *παράθεσή* τους, συμβολισμός $w_1 \circ w_2$ (ή και $w_1 w_2$), είναι η λέξη:

$$w_1 \circ w_2 = x_1 \cdots x_m y_1 \cdots y_n$$

Ορισμός 0.2.9. Έστω $w, w' \in \Sigma^*$. Η w' είναι *υπολέξη* της w ανν υπάρχουν $w_1, w_2 \in \Sigma^*$ (ενδεχομένως $w_1 = \epsilon$ ή $w_2 = \epsilon$) τέτοιες ώστε $w = w_1 \circ w' \circ w_2$.

Συμβολισμός 0.2.10. Έστω αλφάβητο Σ και λέξη $x \in \Sigma^*$. Με x^k συμβολίζουμε τη λέξη $\underbrace{x \circ \cdots \circ x}_{k \text{ φορές}}$, όπου $k \in \mathbb{N}$ (όταν $k = 0$ το x^k ισούται την κενή λέξη ϵ) [1].

Ορισμός 0.2.11. Έστω αλφάβητο Σ και αρίθμηση $\sigma : \Sigma \to [|\Sigma|]$ των στοιχείων του. Η *λεξικογραφική διάταξη* των λέξεων του Σ^*, σύμφωνα με τη σ, είναι η διάταξη που χρησιμοποιείται στα λεξικά [2] μόνο που οι λέξεις με μικρότερο μήκος προηγούνται.

Παράδειγμα 0.2.12. Η λεξικογραφική διάταξη του $\{0,1\}^*$ (με την αρίθμηση $\sigma(0) = 1$ και $\sigma(1) = 2$) είναι η: $\epsilon, 0, 1, 00, 01, 10, 11, 000, 001, \ldots$.

Ορισμός 0.2.13. Έστω αλφάβητο Σ, συνάρτηση $\sigma : \Sigma \to [|\Sigma|]$ και $w, w' \in \Sigma^*$. Αν η w βρίσκεται πριν από την w' στη λεξικογραφική διάταξη, σύμφωνα με τη σ, θα γράφουμε $w <_\sigma w'$.

Σύμβαση 0.2.14. Θα θεωρούμε ότι κάθε αλφάβητο Σ συνοδεύεται από μια προσυμφωνημένη λεξικογραφική διάταξη, χωρίς να αναφερόμαστε ρητά στην αρίθμηση σ. Έτσι θα γράφουμε $w < w'$ (ή ακόμα και $w \leq w'$, στην περίπτωση που η w μπορεί να ταυτίζεται με την w').

Παράδειγμα 0.2.15. Σύμφωνα με το Παράδειγμα 0.2.12 $11 < 000$.

Παρατήρηση 0.2.16. Έστω αλφάβητο Σ και συνάρτηση $\sigma : \Sigma \to [|\Sigma|]$. Η λεξικογραφική διάταξη του Σ^* (σύμφωνα με τη σ) είναι μία 1-1 και επί συνάρτηση από το Σ^* στο $\mathbb{N}$. Συνεπώς $|\Sigma^*| = \aleph_0$.

Ορισμός 0.2.17. Έστω αλφάβητο Σ. Κάθε υποσύνολο $L \subseteq \Sigma^*$ καλείται *γλώσσα* του Σ.

Παράδειγμα 0.2.18. Τα παρακάτω σύνολα είναι γλώσσες του $\{0,1\}$:

- $L = \{w \in \{0,1\}^* \mid w = 0^n 1^n,\ n \in \mathbb{N}\}$

[1] Ενίοτε, προς αποφυγή αμφισημιών, θα βάζουμε παρενθέσεις γύρω από τη λέξη. Για παράδειγμα $(01)^2 = 0101$ ενώ $01^2 = 011$.

[2] Παραδείγματος χάρη αν $\$, @ \in \Sigma$ και $\sigma(\$) < \sigma(@)$ τότε οι λέξεις που αρχίζουν από $\$$ προηγούνται αυτών που αρχίζουν από @. Για λέξεις που αρχίζουν με το ίδιο σύμβολο συγκρίνουμε το δεύτερο σύμβολο και ούτω καθεξής.

- $L_{\text{Παλίνδρομο}} = \{w \in \{0,1\}^* \mid w = w^R\}$
- $L = \varnothing$ (κενή γλώσσα)
- $L = \{\epsilon\}$ (η γλώσσα που περιέχει μόνο την κενή λέξη)

Ορισμός 0.2.19. Έστω αλφάβητο Σ, $a \in \Sigma$ και γλώσσα $L \subseteq \Sigma^*$. Ορίζουμε τη γλώσσα:

$$aL = \{w \in \Sigma^* \mid \exists x \in L(w = a \circ x)\}$$

Ορισμός 0.2.20. Έστω αλφάβητο Σ και γλώσσες $L_1, L_2 \subseteq \Sigma^*$. Ορίζουμε τη γλώσσα:

$$L_1L_2 = \{w \in \Sigma^* \mid \exists w_1 \in L_1 \ \exists w_2 \in L_2(w = w_1 \circ w_2)\}$$

Ορισμός 0.2.21. Έστω αλφάβητο Σ και γλώσσα $L \subseteq \Sigma^*$. Ορίζουμε:

$$\begin{aligned} L^0 &= \{\epsilon\} \\ L^1 &= L \\ L^n &= LL^{n-1} \\ L^* &= \bigcup_{i \in \mathbb{N}} L^i \end{aligned}$$

Ορισμός 0.2.22. Έστω αλφάβητο Σ. *Κανονική έκφραση* του Σ είναι κάθε λέξη του αλφαβήτου $\Sigma \cup \{[,], \varnothing, \varepsilon, \sqcup, ^\star\}$ που κατασκευάζεται σύμφωνα με τους ακόλουθους κανόνες:

1. Το $\varnothing$, το ε και κάθε σύμβολο του Σ είναι κανονική έκφραση.
2. Αν a, b κανονικές εκφράσεις τότε και η $[\mathsf{ab}]$ είναι κανονική έκφραση.
3. Αν a, b κανονικές εκφράσεις τότε και η $[\mathsf{a} \sqcup \mathsf{b}]$ είναι κανονική έκφραση.
4. Αν a κανονική έκφραση τότε και η $\mathsf{a}^\star$ είναι κανονική έκφραση.

Συμβολίζουμε με R_Σ το σύνολο των κανονικών εκφράσεων του Σ.

Παράδειγμα 0.2.23. Οι λέξεις $[0^\star 1^\star], [0^\star \sqcup 1^\star], [[01^\star]0], [01] \sqcup \varnothing$ είναι κανονικές εκφράσεις του $\{0,1\}$.

Ορισμός 0.2.24. Έστω αλφάβητο Σ. Θεωρούμε τη συνάρτηση $\mathcal{L} : R_\Sigma \to 2^{\Sigma^*}$ που αντιστοιχεί σε κάθε κανονική έκφραση μία γλώσσα ως εξής:

$$\mathcal{L}(\mathsf{x}) = \begin{cases} \varnothing & , \text{ αν } \mathsf{x} = \varnothing \\ \{\epsilon\} & , \text{ αν } \mathsf{x} = \varepsilon \\ \{a\} & , \text{ αν } \mathsf{x} = a \in \Sigma \\ \mathcal{L}(\mathsf{a})\mathcal{L}(\mathsf{b}) & , \text{ αν } \mathsf{x} = [\mathsf{ab}] \text{ όπου } \mathsf{a}, \mathsf{b} \in R_\Sigma \\ \mathcal{L}(\mathsf{a}) \cup \mathcal{L}(\mathsf{b}) & , \text{ αν } \mathsf{x} = [\mathsf{a} \sqcup \mathsf{b}] \text{ όπου } \mathsf{a}, \mathsf{b} \in R_\Sigma \\ \mathcal{L}(\mathsf{a})^* & , \text{ αν } \mathsf{x} = \mathsf{a}^\star \text{ όπου } \mathsf{a} \in R_\Sigma \end{cases}$$

Παράδειγμα 0.2.25. Η $\mathcal{L}$ αντιστοιχεί στην κανονική έκφραση $[[0 \sqcup 1]^\star 0]$ του $\{0,1\}$ τη γλώσσα:

$$\begin{aligned}
\mathcal{L}([[0 \sqcup 1]^\star 0]) &= \mathcal{L}([0 \sqcup 1]^\star)\mathcal{L}(0) \\
&= \mathcal{L}([0 \sqcup 1])^*\{0\} \\
&= (\mathcal{L}(0) \cup \mathcal{L}(1))^*\{0\} \\
&= (\{0\} \cup \{1\})^*\{0\} \\
&= \{0,1\}^*\{0\} \\
&= \{w \in \{0,1\}^* \mid \exists w_1 \in \{0,1\}^* \ (w = w_1 \circ 0)\}
\end{aligned}$$

ΜΕΡΟΣ Ι

ΜΟΝΤΕΛΑ ΥΠΟΛΟΓΙΣΜΟΥ

ΚΕΦΑΛΑΙΟ 1

ΜΗΧΑΝΕΣ TURING

Στις αρχές του $20^{ου}$ αιώνα, στα πλαίσια της γενικευμένης ανάγκης να λυθούν τα παράδοξα που είχαν προκύψει στη Θεωρία Συνόλων, ο *David Hilbert* έθεσε μια σειρά από ερωτήματα-στόχους στην επιστημονική κοινότητα. Στα ερωτήματα αυτά εκφραζόταν ρητά η απαίτηση για την τυπική θεμελίωση των μαθηματικών και καταδεικνυόταν η αναγκαιότητα διερεύνησης των ορίων της *Αλγοριθμικής Υπολογισιμότητας*. Ως γνωστόν, οι απαντήσεις που δόθηκαν σε αυτά τα ερωτήματα ήταν αρνητικές: Πρώτα ο *Kurt Gödel* έδειξε ότι δεν είναι δυνατό να υπάρξει αξιωματικοποίηση των μαθηματικών που να είναι συνεπής και παράλληλα ικανή να αποδείξει όλες τις αλήθειες των μαθηματικών, και έπειτα οι *Alonzo Church* και *Alan Turing* απέδειξαν ότι το Entscheidungsproblem (δες Σελίδα 2) δεν μπορεί να λυθεί αλγοριθμικά καθώς δεν μπορεί να υπάρξει διαδικασία που να ελέγχει αν μια μαθηματική έκφραση είναι αληθής είτε όχι (δες Θεώρημα 8.5.12).

Κύριο πόνημά μας στις σημειώσεις αυτές είναι να παρουσιάσουμε αναλυτικά τη θεωρία που δημιουργήθηκε από τα παραπάνω γεγονότα. Ο αρχικός μας στόχος είναι να δώσουμε τυπικούς ορισμούς των συναρτήσεων που είναι *αλγοριθμικά υπολογίσιμες*. Για την ακρίβεια θα δώσουμε τέσσερις διαφορετικούς – αλλά ισοδύναμους – ορισμούς, βασιζόμενοι κάθε φορά και σε μία διαφορετική «προσέγγιση» της έννοιας του *Αλγορίθμου*. Η πρώτη πηγάζει στη δουλειά του Alan Turing και παρουσιάζεται σε αυτό το κεφάλαιο (οι υπόλοιπες θα παρουσιαστούν στα Κεφάλαια 2, 3 και 4).

1.1 Ορισμός Μηχανής Turing και Υπολογισμού

Ορισμός 1.1.1. *Μηχανή Turing (TM)* είναι μια εξάδα $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{τέλος}})$ όπου Q, Σ, Γ πεπερασμένα σύνολα, και:

1. Q είναι το *σύνολο των καταστάσεων*

2. $q_0, q_{\text{τέλος}} \in Q$, q_0 είναι η *αρχική κατάσταση* και $q_{\text{τέλος}}$ η *τερματική κατάσταση*

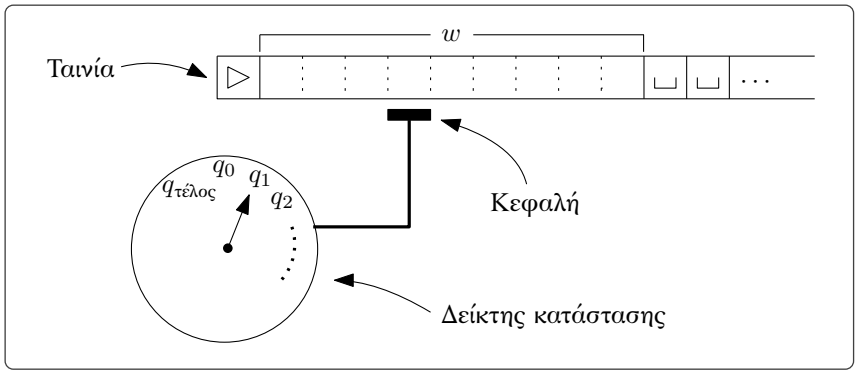
3. Σ είναι το *αλφάβητο εισόδου*
4. Γ είναι το *αλφάβητο ταινίας*
5. $\Sigma \subset \Gamma$
6. $\triangleright, \sqcup \in \Gamma \setminus \Sigma$, το $\triangleright$ είναι το *μαξιλαράκι* και $\sqcup$ το *σύμβολο του κενού*
7. $\delta : Q \times \Gamma \to Q \times \Gamma \times \{\mathrm{A}, \Delta\}$ είναι η *συνάρτηση μετάβασης*, τα A, Δ συμβολίζουν τις δύο κατευθύνσεις (αριστερά και δεξιά αντίστοιχα), και η συνάρτηση αυτή ικανοποιεί τους ακόλουθους περιορισμούς:
   - $\forall a \in \Gamma(\delta(q_{\text{τέλος}}, a) = \bot)$
   - $\forall q \in Q \setminus \{q_{\text{τέλος}}\} \forall q' \in Q \ \forall a \in \Gamma(\delta(q, \triangleright) = (q', a, x) \to x = \Delta \wedge a = \triangleright)$

Η *λέξη εισόδου* (ή απλά η *είσοδος*) μίας ΤΜ $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{τέλος}})$ είναι μία λέξη $w \in \Sigma^*$. Μπορούμε να φανταστούμε την M ως εξής (δες Σχήμα 1.1.1):

> *Η M αποτελείται από μια άπειρη (από τα δεξιά) ταινία, χωρισμένη σε κελιά που μπορούν να περιέχουν ακριβώς ένα σύμβολο του Γ, έναν δείκτη καταστάσεων (ή αλλιώς έναν ελεγκτή) και μία κεφαλή που κινείται πάνω στην ταινία και μπορεί να διαβάζει το περιεχόμενο ενός κελιού ή να γράφει ένα σύμβολο του Γ σε αυτό.*

Το πρώτο κελί της ταινίας περιέχει το σύμβολο $\triangleright$, πάνω στο οποίο δεν μπορεί να γράψει η κεφαλή της M. Τα επόμενα $|w|$ κελιά περιέχουν την είσοδο w και τα υπόλοιπα κελιά το σύμβολο $\sqcup$. Σε κάθε «βήμα λειτουργίας» της M η κεφαλή βρίσκεται σε ένα κελί της ταινίας (που φυσικά περιέχει ένα σύμβολο του Γ) και ο ελεγκτής δείχνει μία κατάσταση του Q (έχουμε δηλαδή ένα όρισμα για τη συνάρτηση μετάβασης δ). Η «λειτουργία» της M με είσοδο w εξελίσσεται ως εξής:

1. Διαβάζουμε το σύμβολο που περιέχει το κελί που βρίσκεται η κεφαλή και την κατάσταση που δείχνει ο ελεγκτής.
2. Συμβουλευόμαστε τη συνάρτηση μεταβάσεων δ (βλέπουμε δηλαδή την τιμή της για το δεδομένο όρισμα) και βρίσκουμε:
   - το σύμβολο που πρέπει να γράψουμε στην ταινία,
   - τη νέα κατάσταση που πρέπει να δείξει ο ελεγκτής και
   - τη φορά που πρέπει να κινήσουμε την κεφαλή πάνω στην ταινία.
3. Γράφουμε το καινούριο σύμβολο στο κελί που βρίσκεται η κεφαλή (στη θέση του παλιού συμβόλου).
4. Αλλάζουμε τον δείκτη του ελεγκτή ώστε να δείχνει τη νέα κατάσταση.



Σχήμα 1.1.1: *Σχηματική αναπαράσταση μίας ΤΜ.*

5. Κινούμε την κεφαλή ένα κελί αριστερά αν έχουμε Α ή ένα κελί δεξιά αν έχουμε Δ.

Είναι ιδιαίτερα βοηθητικό να φανταζόμαστε τη συνάρτηση δ σαν τις εντολές του αλγορίθμου που υλοποιεί η μηχανή Turing. Οι εντολές αυτές δεν θυμίζουν τις εντολές που συνήθως χρησιμοποιούμε στον προγραμματισμό (εντολές ανάθεσης, εντολές ελέγχου ροής κ.λπ.). Η υλοποίηση του αλγορίθμου μέσω μίας μηχανής Turing μοιάζει περισσότερο με τον προγραμματισμό σε μία «χαμηλού επιπέδου» γλώσσα προγραμματισμού (π.χ. τη *γλώσσα μηχανής*).

Παράδειγμα 1.1.2. Έστω ότι $(q_3, 0, q_4, 3, \text{Α}) \in \delta$, το Σχήμα 1.1.2 δείχνει τις αλλαγές που γίνονται στην ΤΜ.

Ορισμός 1.1.3. Έστω ΤΜ $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{τέλος}})$ και $w \in \Sigma^*$. Κάθε δυνατός συνδυασμός λέξης στην ταινία, θέσης κεφαλής και κατάστασης κατά τη λειτουργία της M με είσοδο την w καλείται *φάση* ή *στιγμιότυπο* λειτουργίας. (Από εδώ και στο εξής αντί για «η λειτουργία της M με είσοδο την w» χάριν συντομίας θα γράφουμε $M(w)$.)

Συμβολισμός 1.1.4. Έστω ΤΜ $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{τέλος}})$ και $w \in \Sigma^*$. Θα συμβολίζουμε ένα στιγμιότυπο λειτουργίας με μία λέξη του $(\Gamma \cup Q)^*$ ως εξής: Θα προσθέτουμε στη λέξη που αναγράφεται στην ταινία (τα σύμβολα ␣ δεν θα τα αναφέρουμε [1]), στη θέση που βρίσκεται η κεφαλή, το σύμβολο από το Q που αντιστοιχεί στην κατάσταση που δείχνει ο ελεγκτής.

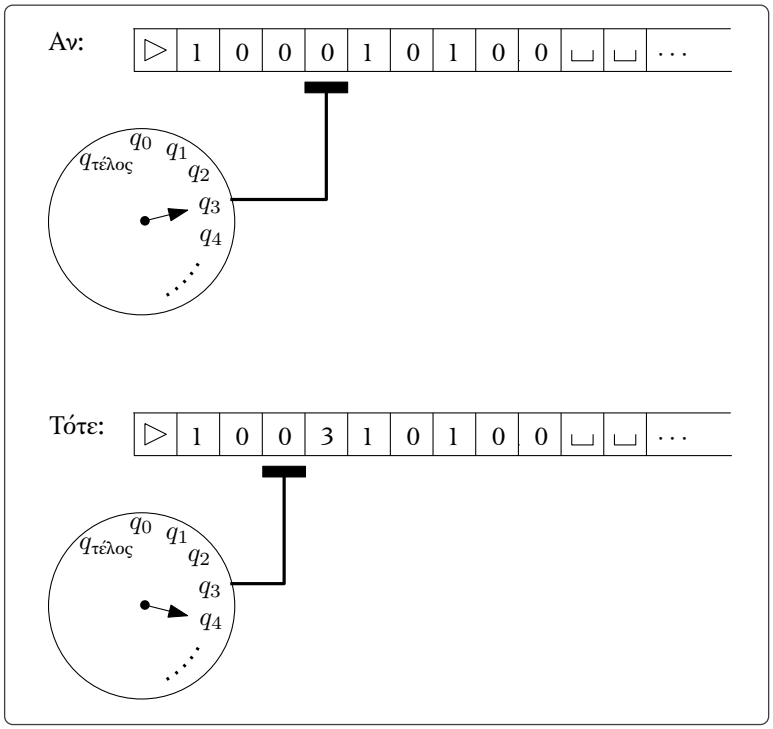
Παράδειγμα 1.1.5. Ας δούμε το στιγμιότυπο λειτουργίας που αντιστοιχεί στο «Αν» του Σχήματος 1.1.2: Η ταινία γράφει τη λέξη $\triangleright\, 100010100$, η κεφαλή βρίσκεται στο πέμπτο κελί και ο δείκτης δείχνει την q_3. Αυτό το στιγμιότυπο λειτουργίας το συμβολίζουμε με τη λέξη $\triangleright\, 100q_3010100 \in (\Gamma \cup Q)^*$.

Ορισμός 1.1.6. Έστω ΤΜ $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{τέλος}})$ και λέξη $w \in \Sigma^*$.

- Το *αρχικό στιγμιότυπο* της $M(w)$ είναι το: $\triangleright\, q_0 w$.
- *Καταληκτικό στιγμιότυπο* της $M(w)$ είναι κάθε στιγμιότυπο της μορφής: $\triangleright\, w_1 q_{\text{τέλος}} w_2$, όπου $w_1, w_2 \in \Gamma^*$ [2].

[1] Τυπικά θα πρέπει να αναφέρουμε μόνο ένα.

[2] Δεν είναι απαραίτητο ότι υπάρχει καταληκτικό στιγμιότυπο για την $M(w)$. Περισσότερα σε λίγο...



Σχήμα 1.1.2: *Παράδειγμα λειτουργίας ΤΜ που περιέχει τη μετάβαση* $(q_3, 0, q_4, 3, \mathrm{A})$.

Ορισμός 1.1.7. Έστω ΤΜ $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{τέλος}})$ και στιγμιότυπο:

$$\triangleright\, a_1 a_2 \cdots a_{i-1} q a_i \cdots a_n$$

όπου $a_i \in \Gamma,\ i \in [n]$ και $q \in Q$.

- Αν $\delta(q, a_i) = (p, b, \mathrm{A})$ και $i > 1$ τότε το *επόμενο στιγμιότυπο* είναι το:

$$\triangleright\, a_1 a_2 \cdots a_{i-2} p a_{i-1} b a_{i+1} \cdots a_n$$

- Αν $\delta(q, a_i) = (p, b, \Delta)$ και $i > 1$ τότε το *επόμενο στιγμιότυπο* είναι το:

$$\triangleright\, a_1 a_2 \cdots a_{i-1} b p a_{i+1} \cdots a_n$$

- Αν $\delta(q, a_i) = \perp$ τότε δεν υπάρχει επόμενο στιγμιότυπο και θα λέμε ότι η M *σταματάει τη λειτουργία της* αν $q = q_{\text{τέλος}}$ ή ότι *κολλάει* αν $q \neq q_{\text{τέλος}}$.

Ορισμός 1.1.8. Έστω ΤΜ $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{τέλος}})$, $w \in \Sigma^*$ και C_1, C_2 στιγμιότυπα λειτουργίας της $M(w)$.

- Αν το C_2 είναι επόμενο στιγμιότυπο του C_1 θα γράφουμε $C_1 \vdash_M C_2$ και θα λέμε ότι από το C_1 *μεταβαίνουμε* στο C_2 (σύμφωνα με τη δ).

- Έστω $\vdash_M^*$ η ανακλαστική και μεταβατική κλειστότητα της σχέσης $\vdash_M$. Αν $C_1 \vdash_M^* C_2$ θα λέμε ότι το C_1 *παράγει* το C_2.

Ορισμός 1.1.9. Έστω ΤΜ $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{τέλος}})$ και $w \in \Sigma^*$. *Υπολογισμός* της $M(w)$ είναι μια ακολουθία στιγμιοτύπων $C_0, C_1, ...$ (πιθανώς πεπερασμένη) όπου:

1. C_0 είναι το αρχικό στιγμιότυπο και
2. $C_i \vdash_M C_{i+1}$ για κάθε $i \in \mathbb{N}$.

Μπορούμε να φανταστούμε τον υπολογισμό της $M(w)$ σαν ένα (πιθανώς άπειρο) διατεταγμένο γραφο-θεωρητικό μονοπάτι με κορυφές του τα στιγμιότυπα λειτουργίας της $M(w)$ και ακμές μεταξύ προηγούμενου και επόμενου στιγμιοτύπου.

Ο υπολογισμός της $M(w)$ *τερματίζει* ανν υπάρχουν $w_1, w_2 \in \Gamma^*$ τέτοια ώστε:

$$\triangleright\, q_0 w \vdash_M^* \triangleright\, w_1 q_{\text{τέλος}} w_2$$

δηλαδή από το αρχικό στιγμιότυπο μεταβαίνουμε σε ένα καταληκτικό στιγμιότυπο.

Στην περίπτωση που έχουμε τερματισμό η ακολουθία στιγμιοτύπων είναι πεπερασμένη [1]. Σε αυτήν την περίπτωση θα γράφουμε $M(w) \downarrow$. Αν ο υπολογισμός της $M(w)$ *δεν τερματίζει* θα γράφουμε $M(w) \uparrow$ [2].

Συμβολισμός 1.1.10. Όταν μας ενδιαφέρει το *πλήθος βημάτων*, δηλαδή το πλήθος στιγμιοτύπων λειτουργίας στην ακολουθία υπολογισμού, που χρειάζεται μία ΤΜ M με είσοδο $w \in \Sigma^*$ για να τερματίσει θα χρησιμοποιούμε τον συμβολισμό $M(w) \downarrow^t$, όπου $t \in \mathbb{N}$ το πλήθος βημάτων. Τέλος, θα γράφουμε $M(w) \downarrow_q$ για μία κατάσταση q θέλοντας να δηλώσουμε το γεγονός ότι η $M(w)$ μεταβαίνει σε στιγμιότυπο που περιέχει την q (και αν επιπλέον μας ενδιαφέρει και το πλήθος βημάτων θα γράφουμε $M(w) \downarrow_q^t$).

1.2 Τι κάνουν οι Μηχανές Turing;

Η συνάρτηση μεταβάσεων μίας ΤΜ μπορεί να μην προσεγγίζει καθόλου την έννοια του αλγορίθμου που έχουμε συναντήσει στα μαθηματικά, όπως και ο τυπικός ορισμός του υπολογισμού μπορεί να μη θυμίζει σε τίποτα τον υπολογισμού από έναν Ηλεκτρονικό Υπολογιστή (Η/Υ), όμως, όπως θα δούμε, στην πραγματικότητα η ΤΜ είναι μία πολύ καλή μαθηματική θεμελίωση του Αλγορίθμου και ο υπολογισμός μία αρκετά πιστή περιγραφή των στοιχειωδών εργασιών που κάνει ο Η/Υ μας κατά τη λειτουργία του.

Σε αυτήν την παράγραφο θα εξετάσουμε τις τρεις βασικές λειτουργίες που μπορούν να φέρουν εις πέρας οι ΤΜ και θα επιχειρηματολογήσουμε ότι μπορούμε να τις θεωρήσουμε τις βασικές λειτουργίες ενός Η/Υ. Οι λειτουργίες αυτές είναι:

[1] Λόγω του πρώτου περιορισμού που θέσαμε στη συνάρτηση μετάβασης δεν θα υπάρξει επόμενο στιγμιότυπο, συνεπώς η ακολουθία θα είναι πεπερασμένη.

[2] Ο υπολογισμός μπορεί να μην τερματίζει είτε επειδή η ακολουθία στιγμιοτύπων είναι άπειρη, είτε επειδή η M κολλάει, οπότε η ακολουθία στιγμιοτύπων ναι μεν είναι πεπερασμένη, αλλά το τελευταίο στιγμιότυπο της δεν είναι καταληκτικό. Παρατηρήστε ότι η πρώτη περίπτωση μη τερματισμού είναι η ουσιαστική καθώς τη δεύτερη θα μπορούσαμε να την αποφύγουμε αν είχαμε προνοήσει να ορίσουμε τη δ για όλες τις δυνατές εισόδους που μπορούν να προκύψουν (εκτός φυσικά από την περίπτωση όπου η κατάσταση εισόδου είναι τερματική).

- Ο *υπολογισμός συναρτήσεων.*
- Η *αναγνώριση* ή η *απόφαση γλωσσών.*
- Η *απαρίθμηση γλωσσών.*

1.2.1 Υπολογισμός συναρτήσεων

Σε αυτές τις σημειώσεις ενδιαφερόμαστε κυρίως για μία ειδική κατηγορία αριθμητικών συναρτήσεων (δες Κεφάλαιο 2). Όμως, όπως είδαμε στην προηγούμενη παράγραφο, ο υπολογισμός μίας Μηχανής Turing αφορά τις λέξεις του αλφάβητου εισόδου της. Το *αντικείμενο του υπολογισμού* δηλαδή είναι μία λέξη και όχι ένας αριθμός όπως θα επιθυμούσαμε. Αυτό το πρόβλημα μπορεί εύκολα να ξεπεραστεί αν συμφωνήσουμε σε έναν τρόπο να «κωδικοποιούμε» τους αριθμούς σε κάποιο αλφάβητο [1]. Έτσι παρόλο που το αντικείμενο του υπολογισμού θα παραμένει μία λέξη ο υπολογισμός θα αφορά κάποιον αριθμό.

Ας δούμε με ποιον τρόπο οι μηχανές Turing μπορούν να υπολογίσουν μία συνάρτηση.

Ορισμός 1.2.1. Μία συνάρτηση $f : \Sigma^* \to \Sigma^*$ καλείται *(Turing) υπολογίσιμη* ανν υπάρχει ΤΜ $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{τέλος}})$ τέτοια ώστε:

$$\forall w \in \mathsf{dom}(f)(\triangleright\, q_0 w \vdash_M^* \triangleright\, q_{\text{τέλος}} f(w)) \text{ και } \forall w \notin \mathsf{dom}(f)(M(w)\uparrow)$$

Στην περίπτωση αυτή θα λέμε ότι η M *υπολογίζει* την f.

Παράδειγμα 1.2.2. Έστω $\mathsf{id} : \{0,1\}^* \to \{0,1\}^*$ η *ταυτοτική συνάρτηση* με $\mathsf{id}(x) = x$. Η ΤΜ $M = (Q, \Sigma, \Gamma, \delta, q_{\text{τέλος}}, q_{\text{τέλος}})$ [2] με $Q = \{q_{\text{τέλος}}\}$, $\Sigma = \{0,1\}$, $\Gamma = \{\triangleright, \sqcup, 0, 1\}$ και $\delta = \varnothing$ την υπολογίζει [3].

Το Παράδειγμα 1.2.2 είναι ένα «ακραίο» δείγμα υπολογισμού συνάρτησης (τα παραδείγματα που ακολουθούν θα είναι πιο διδακτικά).

Αντί να παρουσιάζουμε αναλυτικά τη συνάρτηση μεταβάσεων δ (που όπως θα δούμε συνήθως έχει πάρα πολλά στοιχεία) θα δίνουμε μια συμβολική περιγραφή της, το λεγόμενο *διάγραμμα καταστάσεων* (δες Παράδειγμα 1.2.3).

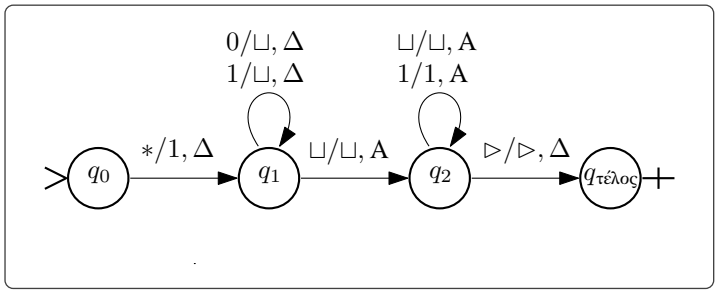
Παράδειγμα 1.2.3. Έστω $f : \{0,1\}^* \to \{0,1\}^*$ η *σταθερή συνάρτηση* $f(x) = 1$. Η $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{τέλος}})$ με $Q = \{q_0, q_1, q_2, q_{\text{τέλος}}\}$, $\Sigma = \{0,1\}$, $\Gamma = \{\triangleright, \sqcup, 0, 1\}$ και

$$\begin{aligned}\delta \;=\; \{&(q_0, 0, q_1, 1, \Delta), (q_0, 1, q_1, 1, \Delta), (q_0, \sqcup, q_1, 1, \Delta),\\ &(q_1, 0, q_1, \sqcup, \Delta), (q_1, 1, q_1, \sqcup, \Delta), (q_1, \sqcup, q_2, \sqcup, \mathrm{A}),\\ &(q_2, \sqcup, q_2, \sqcup, \mathrm{A}), (q_2, 1, q_2, 1, \mathrm{A}), (q_2, \triangleright, q_{\text{τέλος}}, \triangleright, \Delta)\}\end{aligned}$$

[1] Για παράδειγμα μπορούμε να κωδικοποιήσουμε τους φυσικούς αριθμούς στο αλφάβητο $\{0,1\}$, παίρνοντας τη δυαδική αναπαράστασή τους, όπως επίσης θα μπορούσαμε απλά να ορίσουμε ΤΜ με αλφάβητο εισόδου το $\{0,1,2,3,4,5,6,7,8,9\}$. Και στις δύο περιπτώσεις θα πρέπει να δώσουμε μεγάλη προσοχή κατά τον σχεδιασμό της ΤΜ έτσι ώστε να χειρίζεται ειδικά τις λέξεις που δεν αντιστοιχούν σε φυσικούς αριθμούς (όπως π.χ. τη 0000).

[2] Ο Ορισμός 1.1.1 επιτρέπει η αρχική και η τερματική κατάσταση να ταυτίζονται.

[3] Θεωρούμε ότι η κενή συνάρτηση ικανοποιεί τετριμμένα τις προϋποθέσεις της συνάρτησης μετάβασης στη Σελίδα 14.



Σχήμα 1.2.1: *Η TM που υπολογίζει τη συνάρτηση του Παραδείγματος 1.2.3 (το σύμβολο $*$ παίρνει όλες τις τιμές του $\Sigma \setminus \{\triangleright\}$).*

την υπολογίζει [1]. Το διάγραμμα καταστάσεων της δ φαίνεται στο Σχήμα 1.2.1.

Σημείωση 1.2.4. Από εδώ και πέρα (αν δεν συντρέχει σημαντικός λόγος) θα παρουσιάζουμε μόνο το διάγραμμα καταστάσεων μίας TM καθώς αυτό περιέχει όλη την πληροφορία που χρειαζόμαστε [2].

Παράδειγμα 1.2.5. Έστω $f : \{0,1\}^* \to \{0,1\}^*$ με:

$$f(x) = \begin{cases} 0 & , \text{ αν } x \in \{0^n \mid n \in \mathbb{N}\} \\ \perp & , \text{ αλλιώς} \end{cases}$$

Η TM του Σχήματος 1.2.2 την υπολογίζει.

Παράδειγμα 1.2.6. Έστω $\emptyset\!\!: \Sigma^* \to \Sigma^*$ η *κενή συνάρτηση* με $\emptyset(x) = \perp$. Η TM του Σχήματος 1.2.3 την υπολογίζει.

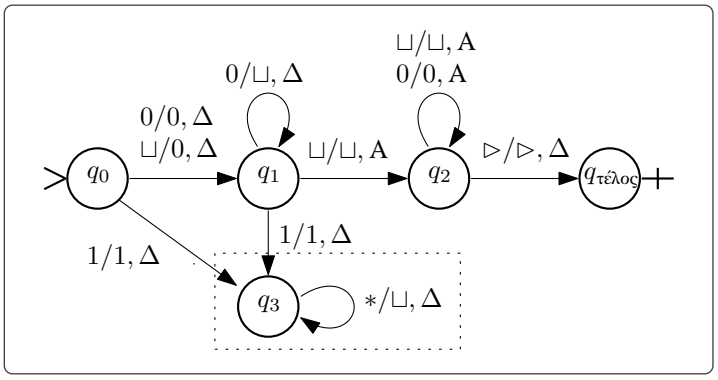
---

[1] Μπορούμε να φανταστούμε ότι η M υλοποιεί το ακόλουθο πρόγραμμα:

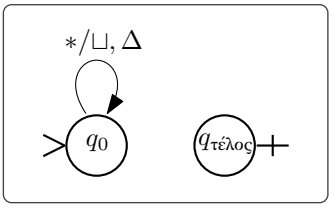
1. **while** $1 > 0$
2. **if** $q_0 0$ **then** $q_1 1\Delta$
3. **elseif** $q_0 1$ **then** $q_1 1\Delta$
4. **elseif** $q_0 \sqcup$ **then** $q_1 1\Delta$
5. **elseif** $q_1 0$ **then** $q_1 \sqcup \Delta$
6. **elseif** $q_1 1$ **then** $q_1 \sqcup \Delta$
7. **elseif** $q_1 \sqcup$ **then** $q_2 \sqcup \mathrm{A}$
8. **elseif** $q_2 \sqcup$ **then** $q_2 \sqcup \mathrm{A}$
9. **elseif** $q_2 1$ **then** $q_2 1\mathrm{A}$
10. **else** $q_2 \triangleright$ **then** $q_{\text{τέλος}} \triangleright \Delta$ **; break**

Η επανάληψη θα τελειώσει μόνο αν φτάσουμε στο **break** στο βήμα 10.

[2] Το μόνο ενδεχομένως που δεν είναι ξεκάθαρο στο διάγραμμα καταστάσεων είναι το αλφάβητο εισόδου της TM (και το αν υπάρχουν σύμβολα στο αλφάβητο ταινίας που δεν χρησιμοποιούνται). Στην επόμενη παράγραφο θα δούμε ότι (χωρίς βλάβη της γενικότητας) μπορούμε να θεωρήσουμε πως όλες οι TM έχουν ως αλφάβητο εισόδου το $\{0,1\}$.



Σχήμα 1.2.2: *Η ΤΜ που υπολογίζει τη συνάρτηση του Παραδείγματος 1.2.5 (το σύμβολο $*$ παίρνει όλες τις τιμές του $\Sigma \setminus \{\triangleright\}$). Παρατηρήστε ότι η ΤΜ «κολλάει» στην κατάσταση q_3.*



Σχήμα 1.2.3: *Το διάγραμμα καταστάσεων της ΤΜ του Παραδείγματος 1.2.21 (το σύμβολο $*$ παίρνει όλες τις τιμές του $\Sigma \setminus \{\triangleright\}$).*

Σύμβαση 1.2.7. Για να απλοποιήσουμε τη σχεδίαση των ΤΜ θα «χαλαρώσουμε» την απαίτηση να γυρίζουν την κεφαλή στην αρχή της ταινίας πριν τερματίσουν [1].

Παράδειγμα 1.2.8. Έστω $\mathsf{next} : \{0,1\}^* \to \{0,1\}^*$ με:

$$\mathsf{next}(x) = \text{«Η επόμενη λέξη της } x \text{ στη λεξικογραφική διάταξη του } \{0,1\}^*\text{»} \ [2]$$

Η ΤΜ M_{next} του Σχήματος 1.2.4 την υπολογίζει.

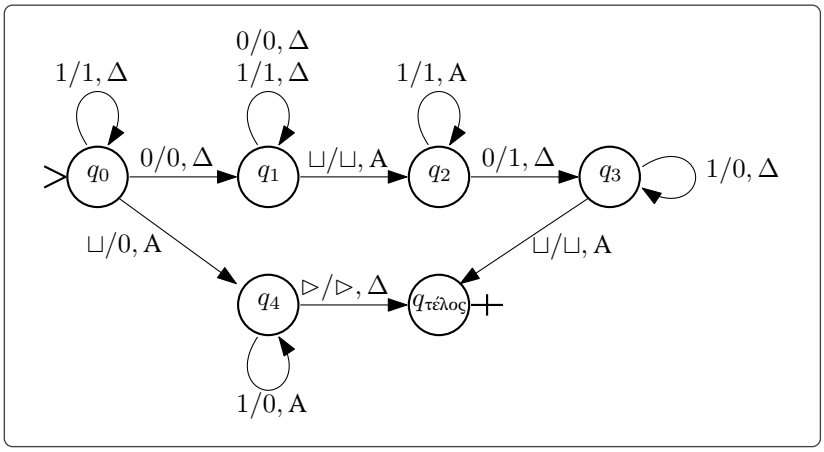
Παράδειγμα 1.2.9. Έστω $\mathsf{space} : \{0,1,\_\}^* \to \{0,1,\_\}^*$ με:

$$\mathsf{space}(x) = \begin{cases} \_x & , \text{ αν } x \in \{0,1\}^* \\ \perp & , \text{ αλλιώς} \end{cases}$$

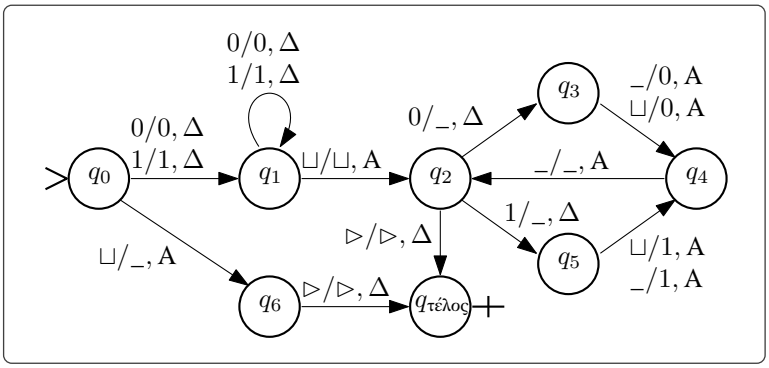
Η ΤΜ M_{space} του Σχήματος 1.2.5 την υπολογίζει.

[1] Ούτως ή άλλως, όπως θα καταλάβατε, αυτό το κομμάτι του υπολογισμού το φέρει εις πέρας η ίδια πάντα «υπορουτίνα» (με ενδεχομένως πολύ μικρές διαφοροποιήσεις).

[2] Η next, αν λάβουμε υπόψιν ότι πολλές λέξεις του $\{0,1\}^*$ δεν αντιστοιχούν σε δυαδική αναπαράσταση φυσικών αριθμών, μπορεί να τροποποιηθεί στη συνάρτηση $f(x) = x + 1$ στο δυαδικό σύστημα.



Σχήμα 1.2.4: *Η TM που υπολογίζει την επόμενη λέξη στην λεξικογραφική διάταξη του* $\{0,1\}^*$.



Σχήμα 1.2.5: *Η TM* M_{space} *του Παραδείγματος 1.2.9.*

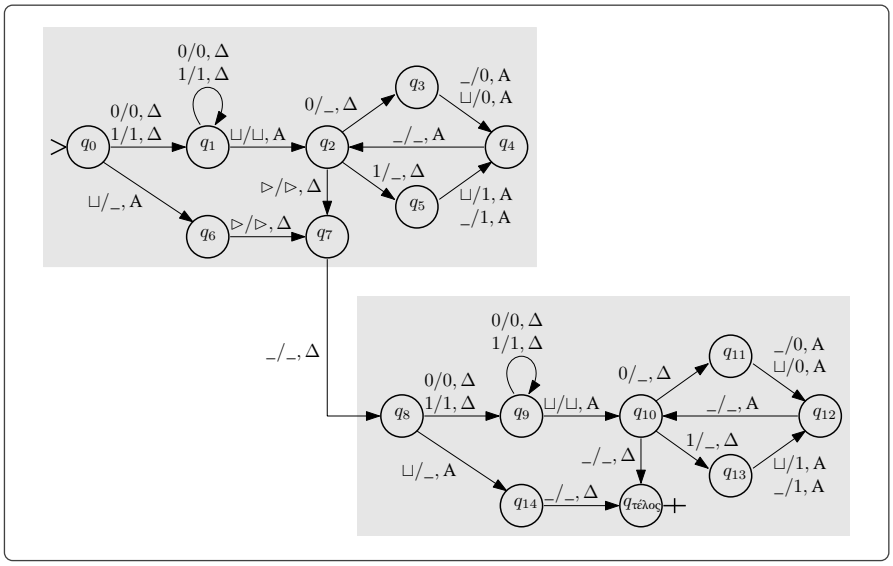
Παράδειγμα 1.2.10. Έστω $f : \{0,1,\_\}^* \to \{0,1,\_\}^*$ με:

$$f(x) = \begin{cases} \_\_x & , \text{ αν } x \in \{0,1\}^* \\ \perp & , \text{ αλλιώς} \end{cases}$$

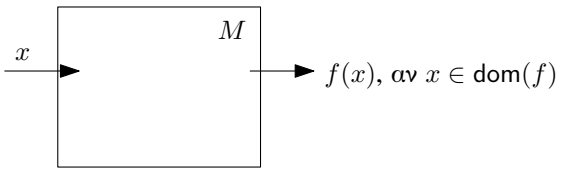
Η ΤΜ του Σχήματος 1.2.6 την υπολογίζει (χρησιμοποιώντας την M_{space} σαν «υπορουτίνα»).

Συμβολισμός 1.2.11 (Κουτάκια). Για διευκόλυνση της παρουσίασης θα χρησιμοποιούμε «κουτάκια» για να περιγράψουμε τις υπορουτίνες των ΤΜ:

1. Αν η $f : \Sigma^* \to \Sigma^*$ είναι υπολογίσιμη συνάρτηση και M είναι μία ΤΜ που την υπολογίζει θα γράφουμε:



Σχήμα 1.2.6: *Η TM που υπολογίζει τη συνάρτηση του Παραδείγματος 1.2.10.*



και θα λέμε ότι η $M(x)$ επιστρέφει $f(x)$.

Ο συμβολισμός με τα κουτάκια μας επιτρέπει να διευκολύνουμε δραστικά την παρουσίαση των TM. Από εδώ και στο εξής θα χρησιμοποιούμε απλές υπορουτίνες σαν «κουτάκια», χωρίς να παρουσιάζουμε τις λεπτομέρειες σχεδιασμού τους [1]. Προκειμένου να γίνει πιο κατανοητός ο συμβολισμός θα τον χρησιμοποιήσουμε για να αποδείξουμε μία πρόταση.

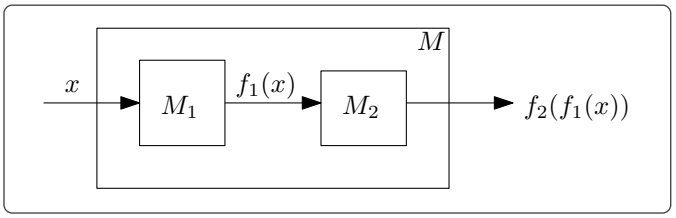
Πρόταση 1.2.12. Έστω $f_1, f_2 : \Sigma^* \to \Sigma^*$ υπολογίσιμες συναρτήσεις. Η συνάρτηση $f_2 \circ f_1$ είναι επίσης υπολογίσιμη.

Απόδειξη. Έστω M_1 και M_2 οι TM που υπολογίζουν τις f_1 και f_2 αντίστοιχα. Παρατηρούμε ότι για την TM M του Σχήματος 1.2.7 ισχύει ότι:

- αν $f_2(f_1(x)) \in \Sigma^*$ η $M(x)$ την επιστρέφει,
- αν $f_1(x) = \perp$ ή $f_2(f_1(x)) = \perp$ η $M(x)$ δεν τερματίζει.

Συνεπώς η M υπολογίζει την $f_2 \circ f_1$. □

[1] Εδώ γίνεται ξεκάθαρος ο λόγος που απαιτήσαμε οι TM να γυρίζουν την κεφαλή στην αρχή της ταινίας προτού τερματίσουν.



Σχήμα 1.2.7: *Η ΤΜ που υπολογίζει τη συνάρτηση $f_2 \circ f_1$.*

Ορισμός 1.2.13. Έστω ΤΜ M. Με ϕ_M θα συμβολίζουμε τη συνάρτηση που υπολογίζει.

Όπως είναι εμφανές κάθε ΤΜ υπολογίζει και κάποια συνάρτηση. Αυτή η αντιστοίχιση όμως δεν είναι 1-1 καθώς υπάρχουν πολλές ΤΜ που υπολογίζουν την ίδια συνάρτηση [1]. Επομένως έχει νόημα ο παρακάτω ορισμός.

Ορισμός 1.2.14. Δύο ΤΜ M_1 και M_2 είναι *ισοδύναμες* ανν $\phi_{M_1} = \phi_{M_2}$.

Σύμβαση 1.2.15. Στην Παράγραφο 1.4 θα δούμε ότι μπορούμε να απαριθμήσουμε τις ΤΜ. Για να ελαφρύνουμε λίγο τον συμβολισμό, όταν έχουμε μία απαρίθμηση των ΤΜ θα αναφερόμαστε στη συνάρτηση που υπολογίζει η ΤΜ M_i γράφοντας ϕ_i αντί για ϕ_{M_i}, όπου $i \in \mathbb{N}$ η σειρά της ΤΜ σύμφωνα με την απαρίθμηση.

1.2.2 Αναγνώριση ή απόφαση γλώσσων

Στη *θεωρητική πληροφορική* είναι πολύ σημαντικό να μπορούμε να ελέγχουμε αν μία είσοδος στον ηλεκτρονικό υπολογιστή αποτελεί *θετικό-στιγμιότυπο* ή *αρνητικό-στιγμιότυπο* για το πρόβλημα που εξετάζουμε. Πιο απλά, μας ενδιαφέρει να μπορούμε να απαντάμε με ένα «ναι» ή ένα «όχι» στα λεγόμενα *προβλήματα απόφασης*. Στη δική μας θεωρία τα προβλήματα απόφασης εισάγονται ως εξής: Οι είσοδοι είναι κωδικοποιημένες σε ένα αλφάβητο Σ, οπότε τα θετικά-στιγμιότυπα αποτελούν ένα υποσύνολο του Σ^*, δηλαδή μία γλώσσα [2].

Σε αυτήν την παράγραφο θα δούμε πως οι ΤΜ μπορούν να χρησιμοποιηθούν ως «αλγόριθμοι» που ελέγχουν αν η είσοδος τους είναι θετικό ή αρνητικό στιγμιότυπο του προβλήματος. Μάλιστα θα δούμε ότι μία μηχανή μπορεί είτε απλά να «αναγνωρίζει» τα θετικά στιγμιότυπα ενός προβλήματος είτε να «αποφασίζει» αν ένα στιγμιότυπο είναι θετικό ή όχι. Παρόλο που η διαφορά μεταξύ των δύο μοιάζει λεπτή, το δεύτερο είναι πολύ πιο ισχυρό. Όταν έχουμε απλή αναγνώριση μίας γλώσσας η ΤΜ μας επιστρέφει θετική απάντηση για τα

[1] Για την ακρίβεια για κάθε συνάρτηση υπάρχουν αριθμησίμως άπειρες ΤΜ που την υπολογίζουν. Γιατί;

[2] Πάρτε για παράδειγμα το πρόβλημα του *Χρωματισμού Γραφήματος* όπου μας δίνουν ένα *γράφημα* G και έναν ακέραιο k και μας ρωτούν αν είναι δυνατόν να *χρωματιστούν* οι κορυφές του γραφήματος με k χρώματα έτσι ώστε τα άκρα των ακμών να έχουν διαφορετικό χρώμα. Η «τυπική» περιγραφή του προβλήματος είναι η εξής: Τα G, k είναι κωδικοποιημένα σε ένα αλφάβητο, ας πούμε το $\{0,1\}$, και μας ενδιαφέρει να δούμε αν μια λέξη του $\{0,1\}^*$ ανήκει στη γλώσσα $L = \{w \in \{0,1\}^* \mid$ Η w είναι κωδικοποίηση γραφήματος G και ακεραίου k και το G χρωματίζεται με k χρώματα$\}$. Αργότερα (στο Κεφάλαιο 8) θα δούμε ότι ανάλογα με την τυπική περιγραφή μίας γλώσσας (πιο συγκεκριμένα την εναλλαγή ποσοδεικτών σε αυτή) μπορούμε να την κατατάξουμε σε διαφορετική κατηγορία «δυσκολίας».

θετικά στιγμιότυπα αλλά δεν επιστρέφει αρνητική απάντηση για (τουλάχιστον ένα από) τα υπόλοιπα. Στην απόφαση, για κάθε στιγμιότυπο λαμβάνουμε την αντίστοιχη απάντηση.

Παρατήρηση 1.2.16. Κάθε αλφάβητο Σ μπορεί να κωδικοποιηθεί στο $\{0,1\}$ [1]. Επομένως, χωρίς βλάβη της γενικότητας, μπορούμε να θεωρήσουμε ότι όλες οι γλώσσες ανήκουν στο $2^{\{0,1\}^*}$.

Από εδώ και στο εξής θα εστιάσουμε στο αλφάβητο $\{0,1\}$ (αυτό όπως είδαμε δεν θα προκαλέσει βλάβη της γενικότητας).

Ορισμός 1.2.17. Έστω γλώσσα $L \subseteq \{0,1\}^*$ και χ_L η χαρακτηριστική της συνάρτηση (δες Ορισμό 0.1.15). Η L είναι *αποφάνσιμη* ανν υπάρχει ΤΜ M που υπολογίζει τη χ_L.

Παράδειγμα 1.2.18. Η γλώσσα $L = \{0,1\}^*$ είναι αποφάνσιμη καθώς η ΤΜ του Σχήματος 1.2.1 υπολογίζει τη χαρακτηριστική της συνάρτηση (που ταυτίζεται με τη σταθερή συνάρτηση του Παραδείγματος 1.2.3).

Για να ελέγξουμε αν μία λέξη w ανήκει σε μία γλώσσα L (ή αντίστοιχα αν ένα στιγμιότυπο του προβλήματος είναι θετικό στιγμιότυπο) βασική προϋπόθεση είναι η ύπαρξη μιας ΤΜ, έστω M, που υπολογίζει τη χαρακτηριστική συνάρτηση της L. Έτσι, τρέχοντας την M με είσοδο τη w αν ο υπολογισμός επιστρέψει 1 θα έπεται ότι $w \in L$ και αν επιστρέψει 0 ότι $w \notin L$. Όπως θα δούμε αργότερα (Κεφάλαιο 5) υπάρχουν γλώσσες για τις οποίες δεν μπορούμε να έχουμε και τα δύο κομμάτια πληροφορίας (και το «ναι» και το «όχι»). Για τον λόγο αυτό θα ορίσουμε άλλη μία κατηγορία γλωσσών τις *αναγνωρίσιμες* (ή *ημι-αποφάνσιμες*).

Ορισμός 1.2.19. Έστω ΤΜ $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{τέλος}})$. Η γλώσσα που *αναγνωρίζει* (ή *αποδέχεται*) η M είναι η:

$$L(M) = \{w \in \Sigma^* \mid \triangleright\, q_0 w \vdash_M^* \triangleright\, q_{\text{τέλος}} 1\}$$

ή αλλιώς (δες Ορισμό 1.2.13):

$$L(M) = \{w \in \Sigma^* \mid \phi_M(w) = 1\}$$

Παρατήρηση 1.2.20. Παρατηρήστε ότι στον Ορισμό 1.2.19 η M δεν υπολογίζει κατ' ανάγκη τη χαρακτηριστική συνάρτηση της γλώσσας $L(M)$.

Παράδειγμα 1.2.21. Έστω ΤΜ $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{τέλος}})$ με $Q = \{q_0, q_{\text{τέλος}}\}$, $\Sigma = \{0,1\}$, $\Gamma = \{\triangleright, \sqcup, 0, 1\}$ και δ με διάγραμμα καταστάσεων αυτό του Σχήματος 1.2.3. Παρατηρούμε ότι $L(M) = \varnothing$.

Ορισμός 1.2.22. Έστω $L \subseteq \{0,1\}^*$. Η L είναι *αναγνωρίσιμη* (ή *ημι-αποφάνσιμη*) ανν υπάρχει ΤΜ M τέτοια ώστε $L = L(M)$.

[1] Για παράδειγμα το $\{A, B, C\}$ μπορούμε να το κωδικοποιήσουμε ως εξής:

$A \rightsquigarrow 01$
$B \rightsquigarrow 011$
$C \rightsquigarrow 0111$

Άρα η λέξη $ACAB$ θα κωδικοποιείται ως 01011101011. Θα αναφερθούμε πιο αναλυτικά στην κωδικοποίηση λέξεων στην Παράγραφο 1.4.

Παρατηρήστε ότι στον παραπάνω ορισμό ζητάμε κάτι πιο ασθενές από τον Ορισμό 1.2.17, καθώς δεν απαιτούμε από τη ΤΜ να επιστρέφει 0 για τις λέξεις που δεν ανήκουν στη γλώσσα. Η ύπαρξη γλωσσών που είναι ημι-αποφάνισμες και όχι αποφάνσιμες ενδεχομένως να μην γίνεται εύκολα πιστευτή. Για να μπορέσουμε να δείξουμε ότι αυτός ο ισχυρισμός είναι αληθής θα χρειαστεί να χρησιμοποιήσουμε ισχυρά «εργαλεία» της *Θεωρίας Συνόλων* (συγκεκριμένα τη μέθοδο της *Διαγωνιοποίησης* που εφαρμόσαμε στην απόδειξη του Θεωρήματος 0.1.17).

Συνήθως στη βιβλιογραφία αναφέρεται ένας διαφορετικός ορισμός των ΤΜ, όπου χρησιμοποιούνται δύο τερματικές καταστάσεις αντί για μία, η $q_{\text{ναι}}$ και η $q_{\text{όχι}}$. Αυτό είναι ιδιαιτέρως χρήσιμο όταν θέλουμε να ελέγξουμε αν μία λέξη ανήκει σε μια γλώσσα ή όχι. Ας δούμε αυτόν τον εναλλακτικό ορισμό.

Ορισμός 1.2.23. Μηχανή Turing είναι μια επτάδα $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{ναι}}, q_{\text{όχι}})$ όπου Q, Σ, Γ πεπερασμένα σύνολα, και:

1. $q_0, q_{\text{ναι}}, q_{\text{όχι}} \in Q$, με $q_{\text{ναι}} \neq q_{\text{όχι}}$ όπου $q_{\text{ναι}}, q_{\text{όχι}}$ οι τερματικές καταστάσεις
2. $\Sigma \subset \Gamma$
3. $\triangleright, \sqcup \in \Gamma \setminus \Sigma$
4. $\delta : Q \times \Gamma \to Q \times \Gamma \times \{\text{Α}, \Delta\}$ τέτοια ώστε:
   - $\forall a \in \Gamma \ \forall q \in \{q_{\text{ναι}}, q_{\text{όχι}}\}(\delta(q, a) = \bot)$
   - $\forall q \in Q \setminus \{q_{\text{ναι}}, q_{\text{όχι}}\} \forall q' \in Q \ \forall a \in \Gamma(\delta(q, \triangleright) = (q', a, x) \to x = \Delta \wedge a = \triangleright)$

Ορισμός 1.2.24. Έστω ΤΜ $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{ναι}}, q_{\text{όχι}})$ και $w \in \Sigma^*$. Ο υπολογισμός της $M(w)$ τερματίζει ανν υπάρχουν $w_1, w_2 \in \Gamma^*$ τέτοια ώστε

$$\triangleright\, q_0 w \vdash_M^* \triangleright\, w_1 q w_2$$

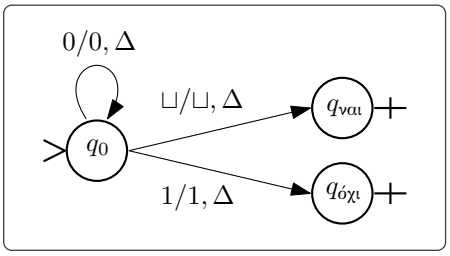
όπου $q \in \{q_{\text{ναι}}, q_{\text{όχι}}\}$.

- Αν $q = q_{\text{ναι}}$ (δηλαδή $M(w) \downarrow_{q_{\text{ναι}}}$) λέμε ότι η M *αποδέχεται την* w.
- Αν $q = q_{\text{όχι}}$ (δηλαδή $M(w) \downarrow_{q_{\text{όχι}}}$) λέμε ότι η M *απορρίπτει την* w.

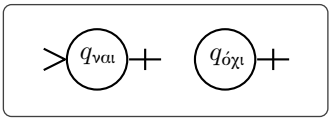
Χρησιμοποιώντας την παραπάνω «παραλλαγή» των ΤΜ μπορούμε να παρακάμψουμε κατά τον υπολογισμό το κομμάτι που προετοιμάζει την «έξοδο» (το 1 ή το 0 ανάλογα με το αν η λέξη ανήκει ή όχι στη γλώσσα) και απλά να μεταβούμε στην κατάλληλη τερματική κατάσταση. Καθώς αυτό διευκολύνει πολύ την παρουσίαση, θα χρησιμοποιήσουμε τον Ορισμό 1.2.23 σε αυτήν την παράγραφο (και σε όποιο άλλο κομμάτι των σημειώσεων ενδιαφερόμαστε για την *αποφανσιμότητα* μίας γλώσσας). Για λόγους πληρότητας θα χρειαστεί να επαναλάβουμε κάποιους από τους ορισμούς.

Ορισμός 1.2.25. Έστω ΤΜ $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{ναι}}, q_{\text{όχι}})$. Η γλώσσα που αναγνωρίζει (ή αποδέχεται) η M είναι η:

$$L(M) = \{w \in \Sigma^* \mid M(w) \downarrow_{q_{\text{ναι}}}\}$$



Σχήμα 1.2.8: *Το διάγραμμα καταστάσεων της ΤΜ του Παραδείγματος 1.2.26.*



Σχήμα 1.2.9: *Το διάγραμμα καταστάσεων της ΤΜ του Παραδείγματος 1.2.27.*

Παράδειγμα 1.2.26. Έστω ΤΜ $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{ναι}}, q_{\text{όχι}})$ με $Q = \{q_0, q_{\text{ναι}}, q_{\text{όχι}}\}$, $\Sigma = \{0, 1\}$, $\Gamma = \{\triangleright, \sqcup, 0, 1\}$ και δ με διάγραμμα καταστάσεων αυτό του Σχήματος 1.2.8. Παρατηρούμε ότι:

$$L(M) = \{w \in \{0,1\}^* \mid w = 0^n, n \in \mathbb{N}\}$$

Παράδειγμα 1.2.27. Έστω ΤΜ $M = (Q, \Sigma, \Gamma, \delta, q_{\text{ναι}}, q_{\text{ναι}}, q_{\text{όχι}})$ με $Q = \{q_{\text{ναι}}, q_{\text{όχι}}\}$, $\Sigma = \{0, 1\}$, $\Gamma = \{\triangleright, \sqcup, 0, 1\}$ και δ με διάγραμμα καταστάσεων αυτό του Σχήματος 1.2.9. Παρατηρούμε ότι $L(M) = \{0, 1\}^*$.

Παρατηρήστε πόσο πιο απλή περιγραφή έχει η ΤΜ του Παραδείγματος 1.2.27 σε σχέση με αυτήν του Παραδείγματος 1.2.18.

Ορισμός 1.2.28. Έστω $L \subseteq \Sigma^*$. Η L είναι αναγνωρίσιμη (ή ημι-αποφάνσιμη) ανν υπάρχει ΤΜ M τέτοια ώστε:

(Α) $w \in L \Leftrightarrow M(w) \downarrow_{q_{\text{ναι}}}$

Ορισμός 1.2.29. Έστω $L \subseteq \Sigma^*$. Η L είναι αποφάνσιμη ανν υπάρχει ΤΜ M τέτοια ώστε:

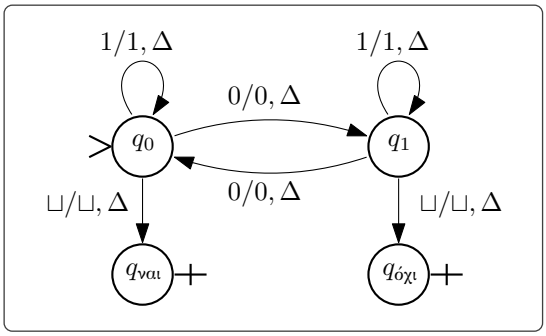
(Α) $w \in L \Leftrightarrow M(w) \downarrow_{q_{\text{ναι}}}$

(Β) $w \notin L \Leftrightarrow M(w) \downarrow_{q_{\text{όχι}}}$

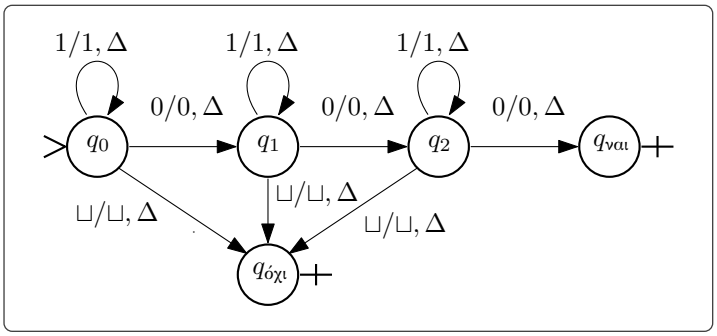
Παράδειγμα 1.2.30. Έστω $L = \{w \in \{0,1\}^* \mid$ το πλήθος των 0 στην w είναι άρτιο$\}$. Η L είναι αποφάνσιμη καθώς για την ΤΜ του Σχήματος 1.2.10 για κάθε $w \in \{0,1\}^*$ ισχύει ότι:

(Α) Το πλήθος των 0 στην w είναι άρτιο ανν $M(w) \downarrow_{q_{\text{ναι}}}$.

(Β) Το πλήθος των 0 στην w είναι περιττό ανν $M(w) \downarrow_{q_{\text{όχι}}}$.



Σχήμα 1.2.10: *Η ΤΜ του Παραδείγματος 1.2.30.*



Σχήμα 1.2.11: *Η ΤΜ του Παραδείγματος 1.2.31.*

Παράδειγμα 1.2.31. Έστω $L = \{w \in \{0,1\}^* \mid$ το πλήθος των 0 στην w είναι $\geq 3\}$. Η L είναι αποφάνσιμη από την ΤΜ του Σχήματος 1.2.11.

Παράδειγμα 1.2.32. Η $L_{\text{Παλίνδρομο}}$ (Παράδειγμα 0.2.18) είναι αποφάνσιμη από την ΤΜ με $Q = \{q_0, q_1, q_2, q_3, q_4, q_5, q_{\text{ναι}}, q_{\text{όχι}}\}$, $\Sigma = \{0,1\}$, $\Gamma = \{\triangleright, \sqcup, 0, 1, \times\}$ και δ με διάγραμμα καταστάσεων αυτό του Σχήματος 1.2.12.

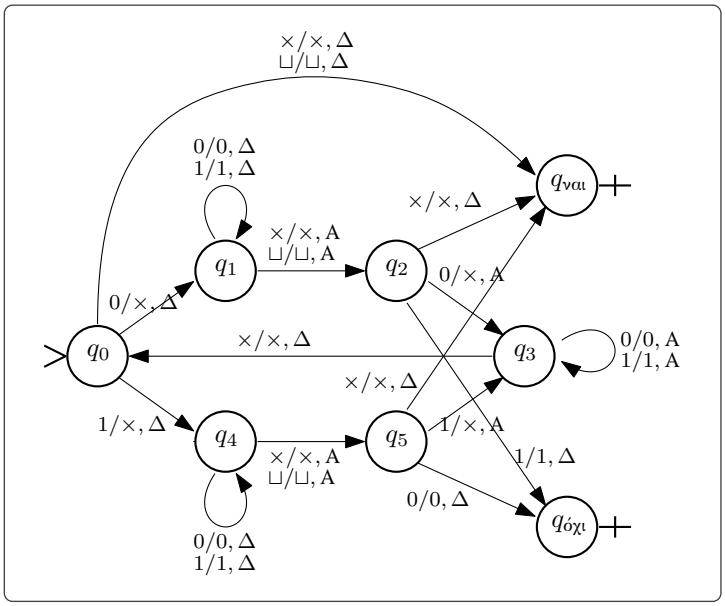
Παρατήρηση 1.2.33. Αν στη ΤΜ του Σχήματος 1.2.12 είχαμε παραλείψει κάποια από τις μεταβάσεις στην κατάσταση $q_{\text{όχι}}$ τότε αυτή η μηχανή θα αναγνώριζε μόνο την $L_{\text{Παλίνδρομο}}$.

Ορισμός 1.2.34. Ορίζουμε τις ακόλουθες κλάσεις [1] γλωσσών:

- $\mathsf{RE} = \{L \subseteq \{0,1\}^* \mid$ υπάρχει ΤΜ που ημι-αποφασίζει την $L\}$
- $\mathsf{REC} = \{L \subseteq \{0,1\}^* \mid$ υπάρχει ΤΜ που αποφασίζει την $L\}$

Προφανώς ισχύει ότι $\mathsf{REC} \subseteq \mathsf{RE} \subseteq 2^{\{0,1\}^*}$ (Σχήμα 1.2.13). Ένας από τους βασικούς σκοπούς μας είναι να ερευνήσουμε κατά πόσον αυτοί οι εγκλεισμοί είναι αυστηροί, δηλαδή να απαντήσουμε στα ερωτήματα:

[1] Είδισται στη Θεωρία Συνόλων τα σύνολα με στοιχεία σύνολα που έχουν κάποια κοινή ιδιότητα να τα αποκαλούμε *κλάσεις*. Έτσι και εδώ τα σύνολα γλωσσών θα τα αποκαλούμε κλάσεις γλωσσών.



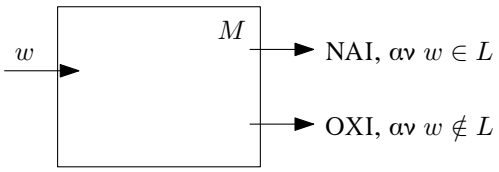
Σχήμα 1.2.12: *Η TM του Παραδείγματος 1.2.32.*

Ερώτημα 1: $\exists L \in \mathsf{RE} \setminus \mathsf{REC}$;

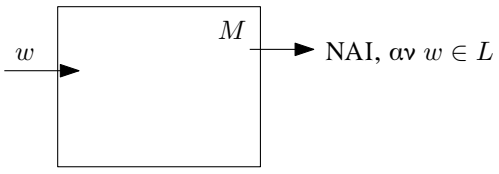
Ερώτημα 2: $\exists L \in 2^{\{0,1\}^*} \setminus \mathsf{RE}$;

Συμβολισμός 1.2.35 (Κουτάκια συνέχεια...).

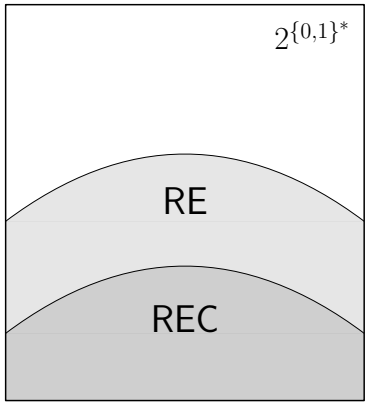
2. Αν $L \in \mathsf{REC}$ και M είναι μία TM που αποφασίζει την L θα γράφουμε:



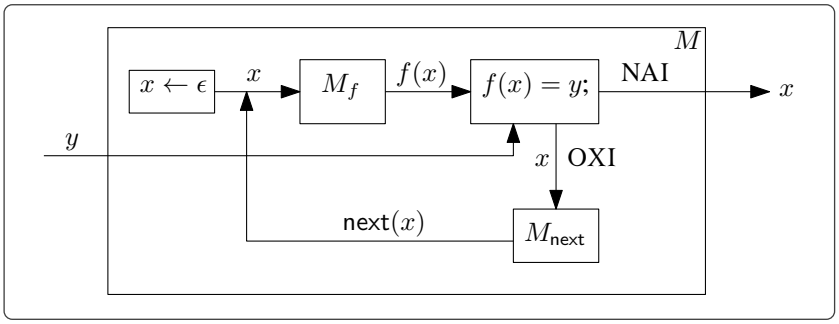
3. Αν $L \in \mathsf{RE}$ και M είναι μία TM που ημι-αποφασίζει την L θα γράφουμε:



Όσο εξοικειωνόμαστε με τις δυνατότητες των TM θα μπορούμε να χρησιμοποιούμε τον συμβολισμό με τα κουτάκια με μεγαλύτερη ελευθερία.



Σχήμα 1.2.13: *Η σχέση εγκλεισμού μεταξύ* REC *και* RE. *Στο Κεφάλαιο 5 θα δούμε ότι ο εγκλεισμός αυτός είναι γνήσιος (δηλαδή ότι* REC $\neq$ RE*).*



Σχήμα 1.2.14: *Η TM που υπολογίζει τη συνάρτηση* f^{-1}.

Παραδείγματα πιο σύνθετων ΤΜ

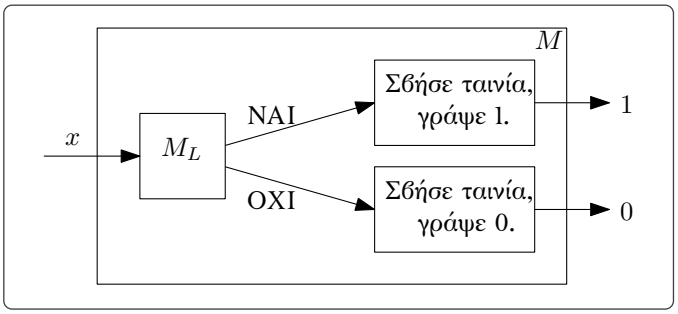
Θα δούμε μερικά παραδείγματα του τρόπου που θα σχεδιάζουμε ΤΜ χρησιμοποιώντας υπορουτίνες-κουτάκια.

Πρόταση 1.2.36. Έστω $f : \{0,1\}^* \to \{0,1\}^*$ πλήρης, 1-1 και επί, υπολογίσιμη συνάρτηση. Η συνάρτηση f^{-1} είναι επίσης υπολογίσιμη.

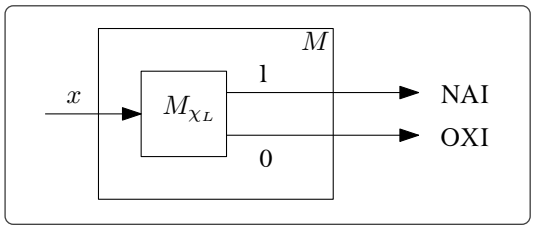
Απόδειξη. Έστω M_f η ΤΜ που υπολογίζει την f. Θα κατασκευάσουμε μία ΤΜ που χρησιμοποιεί σαν υπορουτίνες τις M_f και M_{next} (δες Παράδειγμα 1.2.8), καθώς και μία ΤΜ που αρχικοποιεί έναν μετρητή y στην τιμή ϵ (και επιστρέφει αυτήν την τιμή) [1] και μία ΤΜ που ελέγχει αν δύο λέξεις ταυτίζονται [2]. Η μηχανή αυτή φαίνεται στο Σχήμα 1.2.14. □

[1] Μπορούμε να χρησιμοποιήσουμε μετρητές κατά τον υπολογισμό μίας ΤΜ αποθηκεύοντας την τιμή τους σε συγκεκριμένα μέρη της ταινίας (για παράδειγμα τα πρώτα κελιά της) που θα χωρίζονται μεταξύ τους με κάποιο ειδικό σύμβολο (για παράδειγμα το #). Όποτε χρειαζόμαστε παραπάνω χώρο για κάποιο μετρητή μπορούμε να χρησιμοποιούμε κάποια παραλλαγή της M_{space} (δες Παράδειγμα 1.2.9) για να τον δημιουργήσουμε.

[2] Οι λέξεις αυτές, όπως και πριν, είναι αποθηκευμένες σε ξεχωριστά κομμάτι της ταινίας. Η ΤΜ κινεί την κεφαλή, πότε στην μία λέξη και πότε στην άλλη, και ελέγχει αν οι λέξεις περιέχουν τα ίδια σύμβολα στις ίδιες θέσεις.



Σχήμα 1.2.15: *Η TM που υπολογίζει τη συνάρτηση χ_L όταν $L \in$ REC.*



Σχήμα 1.2.16: *Η TM που αποφασίζει την L όταν η χ_L είναι υπολογίσιμη.*

Παρατήρηση 1.2.37. Η Πρόταση 1.2.36 ισχύει ακόμα και αν η f δεν είναι πλήρης συνάρτηση (δες Άσκηση 1.7).

Για λόγους πληρότητας θα πρέπει να δείξουμε ότι οι δύο ορισμοί των TM που είδαμε είναι *ισοδύναμοι*. Όσον αφορά τον υπολογισμό συναρτήσεων η ύπαρξη μίας επιπλέον τερματικής κατάστασης δεν αλλοιώνει καθόλου τον υπολογισμό (επιλέγουμε μία από αυτές σαν τερματική κατάσταση και σχεδιάζουμε TM που δεν μπορούν να μεταβούν ποτέ στην άλλη). Για την αποφανσιμότητα γλωσσών η ισοδυναμία προκύπτει από τις ακόλουθες προτάσεις.

Πρόταση 1.2.38. Έστω $L \subseteq \{0,1\}^*$. Ισχύει ότι $L \in$ REC ανν η χαρακτηριστική συνάρτηση χ_L της L είναι υπολογίσιμη.

Απόδειξη. ($\Rightarrow$) Έστω ότι $L \in$ REC και έστω M_L μία TM που την αποφασίζει. Η TM του Σχήματος 1.2.15 υπολογίζει την χ_L.

($\Leftarrow$) Έστω ότι η TM M_{χ_L} υπολογίζει την χ_L. Η TM M του Σχήματος 1.2.16 αποφασίζει την L. □

Πρόταση 1.2.39. Έστω $L \subseteq \{0,1\}^*$. Ισχύει ότι $L \in$ RE ανν η συνάρτηση $f : \{0,1\}^* \to \{0,1\}^*$ με $f(x) = \begin{cases} 1 & , \text{αν } x \in L \\ \perp & , \text{αλλιώς} \end{cases}$ είναι υπολογίσιμη.

Η απόδειξη της Πρότασης 1.2.39 αφήνεται ως άσκηση.

1.2.3 Απαρίθμηση γλωσσών

Στο Κεφάλαιο 4 θα δούμε πως μπορούμε να «παράγουμε» τις λέξεις μιας γλώσσας από ένα πεπερασμένο σύνολο κανόνων (κάτι αντίστοιχο με την παραγωγή λέξεων σε μία φυσική γλώσσα, η οποία βασίζεται στους γραμματικούς κανόνες της γλώσσας). Η *παραγωγή* μιας γλώσσας (ή η *απαρίθμηση* όπως την αποκαλούμε σε αυτήν την παράγραφο), παρουσιάζει μεγάλο ενδιαφέρον, όχι μόνο γιατί αποτελεί έναν πεπερασμένο και αυστηρό τρόπο να περιγραφεί ένα άπειρο σύνολο [1], αλλά γιατί στην ουσία μας περιγράφει τη διαδικασία που πρέπει να ακολουθήσουμε για να κατασκευάσουμε τις λέξεις της γλώσσας. Μάλιστα από αυτήν πηγάζουν τα ονόματα – τα ακρωνύμια – των κλάσεων γλωσσών που ορίσαμε πριν [2].

Θα εισάγουμε ακόμα μία παραλλαγή του ορισμού της TM. Ο σκοπός της μηχανής αυτής θα είναι να «τυπώσει» όλες τις λέξεις μιας γλώσσας [3].

Ορισμός 1.2.40. *Απαριθμητής* είναι μια εξάδα $E = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{out}})$ όπου Q, Σ, Γ πεπερασμένα σύνολα, και:

1. Q είναι το *σύνολο των καταστάσεων*
2. $q_0, q_{\text{out}} \in Q$, q_{out} είναι η *κατάσταση εξόδου*
3. Το Q δεν έχει τερματικές καταστάσεις
4. Σ είναι το *αλφάβητο εξόδου*
5. Γ είναι το *αλφάβητο ταινίας*
6. $\Sigma \subset \Gamma$
7. $\triangleright, \sqcup, \# \in \Gamma \setminus \Sigma$, το # χρησιμοποιείται για να χωρίζουμε την ταινία του E σε δύο μέρη: το *πρόχειρο* και την *έξοδο* (δες Σχήμα 1.2.17)
8. $\delta : Q \times \Gamma \to Q \times \Gamma \times \{\text{A}, \Delta\}$ είναι η *συνάρτηση μετάβασης* για την οποία ισχύει ότι:
   - $\forall q, q' \in Q \ \forall a \in \Gamma(\delta(q, \triangleright) = (q', a, x) \to x = \Delta \wedge a = \triangleright)$

Ο E δεν δέχεται σαν είσοδο κάποια λέξη (ξεκινάει με κενή ταινία). Κάνει υπολογισμούς στο πρόχειρο [4] και όταν μεταβεί στην κατάσταση q_{out} λέμε ότι *«τυπώνει»* τη λέξη που βρίσκεται στο κομμάτι της εξόδου (δεξιά από το # δηλαδή). Στο κομμάτι της εξόδου ο E μπορεί να γράψει μόνο σύμβολα από το $\Sigma \cup \{\sqcup\}$ [5]. Στην περίπτωση όπου ο E τυπώνει τη λέξη

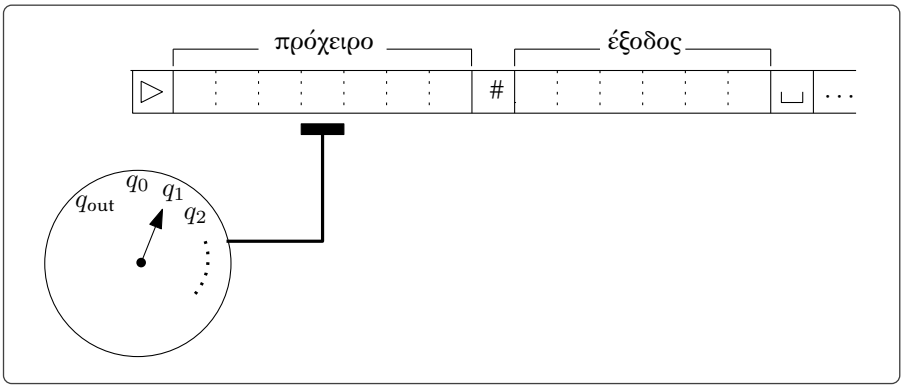
[1] Ειδικά αν φέρουμε στο μυαλό ότι αυτό το σύνολο περιέχει τα θετικά-στιμιότυπα ενός προβλήματος απόφανσης.

[2] Το RE αντιστοιχεί στο Recursive Enumerable και το REC στο Recursive.

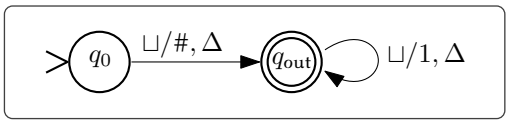
[3] Προφανώς, αν η γλώσσα είναι άπειρη η μηχανή θα πρέπει να δουλεύει για πάντα. Η έννοια του τερματισμού δεν υφίσταται σε αυτού του είδους τον υπολογισμό.

[4] Στην αρχή αυτών των υπολογισμών γράφει το σύμβολο # πάνω στην ταινία, ώστε να χωρίσει το πρόχειρο από το κομμάτι της εξόδου (δες τα Παραδείγματα 1.2.43, 1.2.44).

[5] Τυπικά δεν μπορούμε να επιβάλουμε κάποιον περιορισμό στη συνάρτηση μετάβασης για να το εξασφαλίσουμε αυτό. Αυτό που θα κάνουμε είναι όταν ο E μεταβαίνει στην κατάσταση q_{out} να θεωρούμε σαν λέξη εξόδου το κομμάτι της ταινίας δεξιά από το # και αν τυχαίνει αυτό να περιέχει κάποιο σύμβολα που δεν ανήκουν στο Σ απλά θα τα αγνοούμε. Πρακτικά όμως όταν σχεδιάζουμε έναν απαριθμητή θα φροντίζουμε να ικανοποιείται αυτή η προϋπόθεση.



Σχήμα 1.2.17: *Σχηματική αναπαράσταση ενός απαριθμητή.*



Σχήμα 1.2.18: *Ο απαριθμητής της γλώσσας* $\{1^n \mid n \in \mathbb{N}\}$.

$w \in \Sigma^*$ θα γράφουμε $\mathsf{print}_E(w)$ (ή σκέτο $\mathsf{print}(w)$ αν ο E εννοείται από τα συμφραζόμενα). Ο E δεν τερματίζει ποτέ (ακόμα και αν τυπώσει όλες τις λέξεις μιας πεπερασμένης γλώσσας) και συνεχώς τυπώνει λέξεις.

Ορισμός 1.2.41. Έστω απαριθμητής $E = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{out}})$. Η γλώσσα που *απαριθμεί* ο E είναι η:

$$L(E) = \{w \in \Sigma^* \mid \exists w' \in \Gamma^* (\triangleright\, q_0 \vdash_E^* \triangleright\, q_{\text{out}} w' \# w)\} \ [1]$$

ή αλλιώς:

$$L(E) = \{w \in \Sigma^* \mid \mathsf{print}_E(w)\}$$

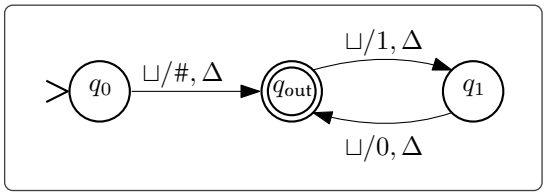
Ορισμός 1.2.42. Μία γλώσσα $L \subseteq \Sigma^*$ καλείται *αναδρομικά απαριθμήσιμη* ανν υπάρχει απαριθμητής $E = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{out}})$ τέτοιος ώστε $L = L(E)$.

Παράδειγμα 1.2.43. Ο απαριθμητής E του Σχήματος 1.2.18 απαριθμεί τη γλώσσα $L(E) = \{1^n \mid n \in \mathbb{N}\}$.

Παράδειγμα 1.2.44. Ο απαριθμητής E του Σχήματος 1.2.19 απαριθμεί τη γλώσσα $L(E) = \{(10)^n \mid n \in \mathbb{N}\}$.

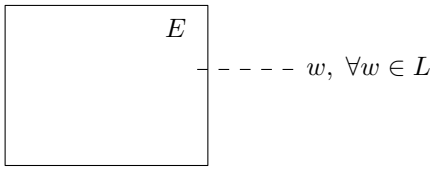
Συμβολισμός 1.2.45 (Κουτάκια συνέχεια...).

[1] Και εδώ η σύμβαση ότι πριν μεταβεί ο E στην q_{out} θα πρέπει να έχει πάει την κεφαλή στην αρχή της ταινίας δεν είναι ουσιαστική. Επίσης, όπως είπαμε, στην w αγνοούμε τυχόν σύμβολα που δεν ανήκουν στο Σ.



Σχήμα 1.2.19: *Ο απαριθμητής της γλώσσας* $\{(10)^n \mid n \in \mathbb{N}\}$.

4. Αν ο απαριθμητής E απαριθμεί τη γλώσσα L θα γράφουμε:



Παρατηρήστε ότι η χρησιμοποίηση ενός απαριθμητή E ως υπορουτίνα σε μία TM M είναι εξ ορισμού προβληματική. Όχι τόσο γιατί ο Ορισμός 1.2.40 διαφέρει από τον Ορισμό 1.1.1 [1], αλλά γιατί στους απαριθμητές δεν υφίσταται τερματισμός. Στην πραγματικότητα αυτό που κάνουμε είναι να προσθέσουμε στην M τις απαραίτητες μεταβάσεις του E για να παραχθούν οι λέξεις της $L(E)$, και όχι να «συνδέουμε» τις δύο μηχανές.

Θεώρημα 1.2.46. Έστω γλώσσα $L \subseteq \{0,1\}^*$. $L \in \mathsf{RE}$ ανν υπάρχει απαριθμητής E τέτοιος ώστε $L(E) = L$.

Απόδειξη. ($\Rightarrow$) Η απόδειξη θα γίνει αργότερα (δες σελίδα 50) καθώς χρειάζεται να εισάγουμε την έννοια της *Καθολικής TM* πρώτα [2].

($\Leftarrow$) Έστω απαριθμητής E που απαριθμεί την L. Η TM M του Σχήματος 1.2.20 ημιαποφασίζει την L [3]. □

Παρατήρηση 1.2.47. Σύμφωνα με το Θεώρημα 1.2.46 μία γλώσσα L είναι αναδρομικά απαριθμήσιμη ανν $L \in \mathsf{RE}$.

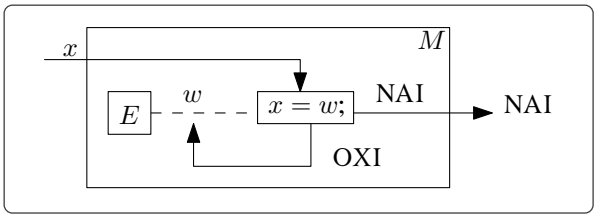
Παρατήρηση 1.2.48. Έστω γλώσσα $L \subseteq \Sigma^*$ και απαριθμητής $E = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{out}})$ που την απαριθμεί. Ο ορισμός που δώσαμε για τον απαριθμητή αφήνει ανοιχτό το ενδεχόμενο ο E να τυπώνει τις λέξεις της L σε οποιαδήποτε σειρά, ακόμα και με επαναλήψεις [4].

[1] Αυτό διορθώνεται εύκολα χρίζοντας κατάσταση εξόδου μία από τις (μη-τερματικές) καταστάσεις της TM.

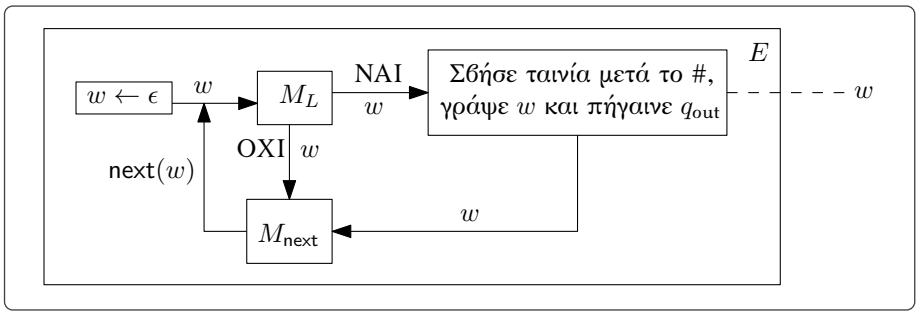
[2] Θα χρειαστεί να κάνουμε «χρονομετρημένη προσομοίωση» της TM που ημιαποφασίζει την L.

[3] Ο τρόπος που χρησιμοποιείται ως υπορουτίνα ο E είναι ο εξής: Ο E παράγει μια λέξη που την τροφοδοτεί στις υπόλοιπες υπορουτίνες της M. Όταν ο υπολογισμός γυρίσει πίσω στον E αυτός παράγει καινούργια λέξη που την τροφοδοτεί ξανά στις υπορουτίνες κ.ο.κ..

[4] Ενδεχομένως να έχουμε και άπειρες επαναλήψεις! Αυτό συμβαίνει π.χ. σε έναν απαριθμητή που απαριθμεί μία πεπερασμένη γλώσσα.



Σχήμα 1.2.20: *Η TM που ημι-αποφασίζει μία γλώσσα όταν υπάρχει απαριθμητής E που την απαριθμεί.*



Σχήμα 1.2.21: *Ο απαριθμητής που απαριθμεί την $L \in$ REC σύμφωνα με τη λεξικογραφική διάταξη (M_{next} είναι η TM του Παραδείγματος 1.2.8).*

Θεώρημα 1.2.49. Έστω γλώσσα $L \subseteq \{0,1\}^*$. $L \in$ REC ανν υπάρχει απαριθμητής E που απαριθμεί τις λέξεις της L σύμφωνα με τη λεξικογραφική διάταξη.

Απόδειξη. ($\Rightarrow$) Έστω ότι $L \in$ REC και ότι η TM M_L την αποφασίζει. Αν η L είναι πεπερασμένη γλώσσα τότε προφανώς υπάρχει απαριθμητής που την απαριθμεί σύμφωνα με τη λεξικογραφική διάταξη [1]. Αν η L είναι άπειρη τότε ο απαριθμητής E του Σχήματος 1.2.21 είναι ο ζητούμενος.

($\Leftarrow$) Αν η L είναι πεπερασμένη γλώσσα, έστω η $\{w_1, w_2, \ldots, w_n\}$, τότε π.χ. η TM του Σχήματος 1.2.22 την αποφασίζει.

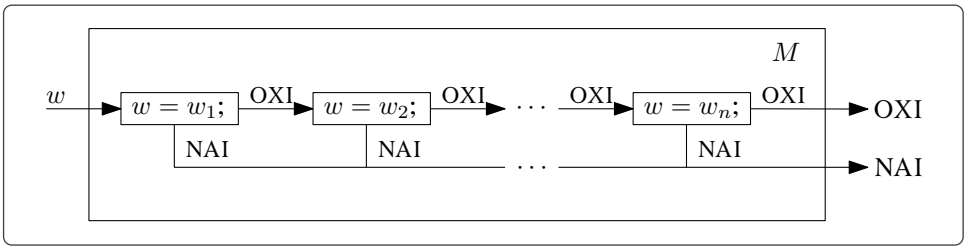
Έστω ότι η L είναι άπειρη γλώσσα και ότι ο απαριθμητής E την απαριθμεί σύμφωνα με τη λεξικογραφική διάταξη. Η TM M του Σχήματος 1.2.23 αποφασίζει την L. □

Ορισμός 1.2.50. Μία γλώσσα L λέγεται *αναδρομική* ανν $L \in$ REC.

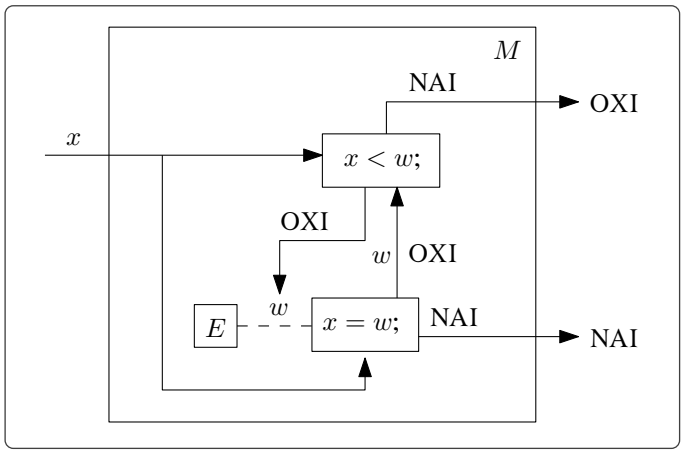
1.3 Επεκτάσεις Μηχανών Turing

Μπορούμε να φανταστούμε πολλούς τρόπου να «βελτιώσουμε» τις TM ούτως ώστε ο υπολογισμός να γίνεται ευκολότερα και γρηγορότερα. Το ενδιαφέρον μας όμως στρέφεται

[1] Έστω ότι $L = \{w_1, w_2, \ldots, w_n\}$, όπου $w_i < w_j$ για $i < j$. Ο απαριθμητής θα τυπώσει τις λέξεις $w_1, w_2, \ldots, w_n$ (σε αυτήν τη σειρά) και μετά θα τυπώνει την w_n για πάντα.



Σχήμα 1.2.22: *Η TM που αποφασίζει την πεπερασμένη γλώσσα* $L = \{w_1, w_2, \dots, w_n\}$.



Σχήμα 1.2.23: *Η TM που αποφασίζει την* L *όταν υπάρχει απαριθμητής* E *που τη απαριθμεί σύμφωνα με την λεξικογραφική διάταξη.*

στο κατά πόσον μία συνάρτηση *είναι* υπολογίσιμη (ή μία γλώσσα *είναι* αναγνωρίσιμη/αποφάνσιμη), χωρίς να ενδιαφερόμαστε για την *Πολυπλοκότητα* του τρόπου που υπολογίζεται (αντίστοιχα αναγνωρίζεται/αποφασίζεται).

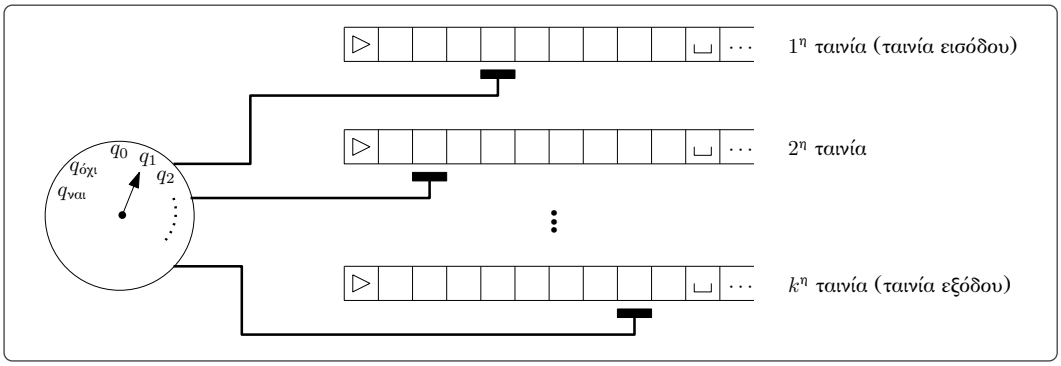
Σε αυτήν την παράγραφο θα δούμε ότι οι πιο εύλογες βελτιώσεις-επεκτάσεις στον ορισμό των TM δεν είναι ικανές να επεκτείνουν το σύνολο των υπολογίσιμων συναρτήσεων (ή των διαγνώσιμων/αποφάνσιμων γλωσσών) [1], πράγμα που καταδεικνύει πως αν θέλουμε απλά να ερευνήσουμε τους ορίζοντες της υπολογισιμότητας η μηχανή του Ορισμού 1.1.1 είναι η μόνη που χρειαζόμαστε.

1.3.1 Πολυταινιακές Μηχανές Turing

Ορισμός 1.3.1. Για κάθε $k \geq 1$ *Μηχανή Turing* k*-ταινιών* είναι μια εξάδα $M_k = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{τέλος}})$ όπου Q, Σ, Γ πεπερασμένα σύνολα, και:

1. Q είναι το *σύνολο των καταστάσεων*

[1] Αποδεικνύεται ότι το ίδιο ισχύει και για όλες τις άλλες (εύλογες) επεκτάσεις TM (δες Σημείωση 1.3.16).



Σχήμα 1.3.1: *Σχηματική αναπαράσταση μίας TM k-ταινιών.*

2. $q_0, q_{\text{τέλος}} \in Q$, $q_{\text{τέλος}}$ η τερματική κατάσταση
3. Σ είναι το *αλφάβητο εισόδου*
4. Γ είναι το *αλφάβητο ταινίας*
5. $\Sigma \subset \Gamma$
6. $\triangleright, \sqcup \in \Gamma \setminus \Sigma$
7. $\delta : Q \times \Gamma^k \to Q \times \Gamma^k \times \{\text{A}, \Delta\}^k$ που ικανοποιεί τους ακόλουθους περιορισμούς:
   - $\forall a_1, \dots, a_k \in \Gamma(\delta(q_{\text{τέλος}}, a_1, \dots, a_k) = \bot)$
   - $\forall i \in [k]\ \forall q' \in Q \setminus \{q_{\text{τέλος}}\}\ \forall q' \in Q\ \forall a_1, \dots, a_k, b_1, \dots, b_k \in \Gamma\ \forall x_1, \dots, x_k \in \{\text{A}, \Delta\}$
     $(\delta(q, a_1, \dots, a_k) = (q', b_1, \dots, b_k, x_1, \dots, x_k) \wedge a_i =\triangleright\to x_i = \Delta \wedge b_i = \triangleright)$

Μπορούμε να φανταστούμε την M_k ως εξής (δες Σχήμα 1.3.1):

> *Η M_k αποτελείται από k-ταινίες, k-κεφαλές (μία για κάθε ταινία) και έναν δείκτη καταστάσεων. Η είσοδος βρίσκεται στην ταινία 1 [1] και η έξοδος βρίσκεται στην ταινία k (οι υπόλοιπες ταινίες χρησιμοποιούνται ως πρόχειρο).*

Το κάθε «βήμα» υπολογισμού, όπως και στις *μονοταινιακές* TM, αποτελείται από μία μετάβαση της συνάρτησης δ. Αυτό σημαίνει ότι το βήμα ολοκληρώνεται όταν έχουν γίνει οι αλλαγές στις k ταινίες και στον ελεγκτή καταστάσεων. Μιλώντας «μηχανιστικά» θα λέγαμε ότι σε κάθε βήμα η πολυταινιακή TM κάνει «παράλληλα» τις αλλαγές στις k ταινίες. Μιλώντας όμως μαθηματικά μπορούμε να ορίσουμε το επόμενο στιγμιότυπο μέσα από τη συνάρτηση μεταβάσεων όπως κάναμε στον Ορισμό 1.1.7 (φτάνει πρώτα να συμφωνήσουμε σε έναν τρόπο να κωδικοποιήσουμε τα στιγμιότυπα λειτουργίας ως λέξεις, δες Σελίδα 15).

[1] Μπορούμε να θεωρήσουμε ότι η M_k δέχεται παραπάνω από μια λέξεις σαν είσοδο, για παράδειγμα $i \in \mathbb{N}$ λέξεις. Στην περίπτωση όπου $i \leq k$, οι λέξεις μπορεί να γραφτούν, η κάθε μία ξεχωριστά, στις i-πρώτες ταινίες. Αν $i > k$ θα πρέπει κάποια ταινία να περιέχει παραπάνω από μία λέξεις, τις οποίες θα χωρίζουμε με κάποιο ειδικό σύμβολο όπως παραδείγματος χάρη το #.

Παράδειγμα 1.3.2. Μπορούμε να ορίσουμε τους απαριθμητές σαν ΤΜ με δύο ταινίες. Η πρώτη ταινία είναι το πρόχειρο και η δεύτερη η ταινία εξόδου [1].

Για να δείξουμε ότι οι πολλαπλές ταινίες (παρόλο που αντικειμενικά διευκολύνουν πολύ τον σχεδιασμό τον ΤΜ και επισπεύδουν τον υπολογισμό) δεν έχουν τη δυνατότητα να υπολογίζουν συναρτήσεις που δεν είναι υπολογίσιμες σύμφωνα με τον Ορισμό 1.2.1, θα δείξουμε ότι για κάθε πολυταινιακή ΤΜ υπάρχει *ισοδύναμη* μονοταινιακή (δες ορισμός 1.2.14).

Θεώρημα 1.3.3. Για κάθε ΤΜ k-ταινιών, $k \in \mathbb{N}$, υπάρχει ισοδύναμη μονοταινιακή ΤΜ.

Απόδειξη. Έστω $M_k = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{τέλος}})$ η ΤΜ k-ταινιών. Θα *προσομοιώσουμε* [2] τη λειτουργία της με μία μονοταινιακή ΤΜ $M = (Q', \Sigma, \Gamma', \delta', q_0, q_{\text{τέλος}})$ όπου

$$\Gamma' = \Gamma \cup \{\#\} \cup \{\dot{a} \mid a \in \Gamma \setminus \{\triangleright\}\} \cup \{\blacktriangleright, \dot{\blacktriangleright}\}$$

Το σύμβολο # χρησιμοποιείται για να χωρίσουμε την ταινία της M σε k-τμήματα που αντιστοιχούν στις k ταινίες της M_k. Τα σύμβολα με κουκκίδα χρησιμοποιούνται για να επισημάνουν τη θέση του συμβόλου που βρίσκεται η κεφαλή σε κάθε ταινία της M_k. Σε κάθε βήμα υπολογισμού της M θα υπάρχουν k-σύμβολα με κουκκίδα στην ταινία της, ένα σε κάθε τμήμα της. Για κάθε κεφαλή που διαβάζει κενό το τμήμα που αντιστοιχεί στην ταινία της θα περιέχει εκτός από τη λέξη και όσα κενά προηγούνται του κενού που διαβάζει (για το οποίο φυσικά θα χρησιμοποιούμε το σύμβολο $\dot{\sqcup}$). Τέλος, το $\blacktriangleright$ παίζει τον ρόλο του αριστερού μαξιλαρακίου σε κάθε τμήμα της ταινίας (δες Σχήμα 1.3.2).

Η συνάρτηση δ' (και το σύνολο καταστάσεων Q') ορίζεται ως εξής [3]:

1. Η M ξεκινάει από το $\triangleright$ και διαβάζει τα σύμβολα που έχουν κουκκίδα σε κάθε τμήμα της ταινίας μέχρι να βρει το πρώτο σύμβολο κενού που ακολουθεί το σύμβολο # (τα σύμβολα αυτά τα «θυμάται» χρησιμοποιώντας επιπλέον καταστάσεις).

2. Επιστρέφει στην αρχή της ταινίας.

3. Διασχίζει πάλι την ταινία (από τα αριστερά προς τα δεξιά) και κάνει τις αλλαγές στα σύμβολα με την κουκκίδα, σε κάθε τμήμα, σύμφωνα με τη δ (γράφοντας σύμβολα χωρίς κουκκίδα). Στο ίδιο πέρασμα αλλάζει το σύμβολο αριστερά ή δεξιά από τα σύμβολα αυτά, γράφοντας το αντίστοιχο σύμβολο με κουκκίδα, ανάλογα με το αν η κεφαλή στην εν λόγω ταινία της M_k κινείται αριστερά ή δεξιά.

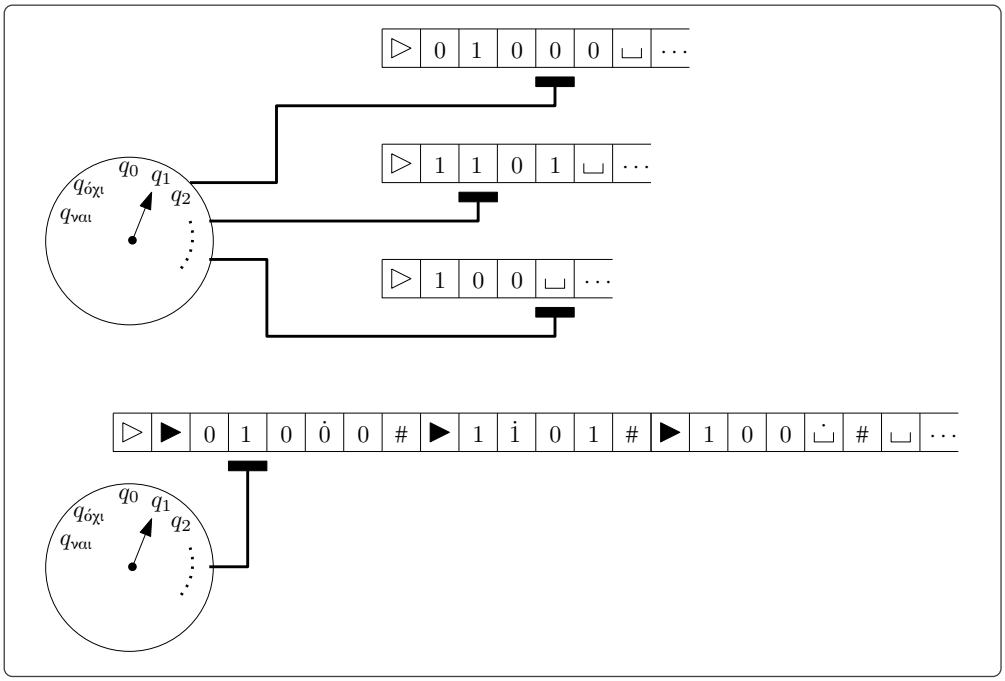
[1] Παρατηρήστε ότι με αυτόν τον τρόπο μπορούμε να εξασφαλίσουμε ότι ο απαριθμητής θα γράφει στο πρόχειρο μόνο σύμβολα του $\Sigma \cup \{\sqcup\}$, απλά απαιτώντας η συνάρτηση μεταβάσεων να είναι συνάρτηση:

$$\delta : Q \times \Gamma \times \Sigma \cup \{\sqcup\} \to Q \times \Gamma \times \Sigma \cup \{\sqcup\} \times \{\mathrm{A}, \Delta\} \times \{\mathrm{A}, \Delta\}$$

(δες Υποσημείωση 5 στη Σελίδα 31).

[2] Για κάθε μετάβαση της M_k θα ορίσουμε (περιγραφικά και όχι τυπικά) μία ακολουθία μεταβάσεων της M που καταλήγει στο ίδιο (ή, πιο σωστά, σε αντίστοιχο) στιγμιότυπο.

[3] Δεν θα δώσουμε αναλυτική περιγραφή της δ' και του Q'. Αντ'αυτού θα περιγράψουμε τη λειτουργία της M. Ο σχεδιασμός συνάρτησης μεταβάσεων που να υλοποιεί αυτήν τη λειτουργία επαφίεται στον λεπτολόγο αναγνώστη.

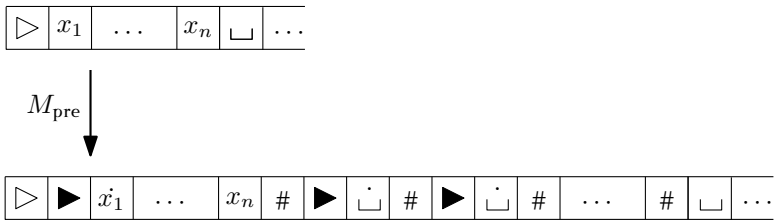


Σχήμα 1.3.2: *Παράδειγμα προσομοίωσης TM k-ταινιών από μονοταινιακή TM.*

Αν χρειαστεί να γράψει πάνω στο # σε κάποιο κομμάτι της ταινίας [1], μεταφέρει το περιεχόμενο της ταινίας που ακολουθεί το εν λόγω # ένα κελί δεξιά (χρησιμοποιώντας παραδείγματος χάρη κάποια παραλλαγή της M_{space} του Παραδείγματος 1.2.9), κάνει την αλλαγή που πρέπει και μετά γράφει # στο «κενό» κελί (που θα περιέχει π.χ. το σύμβολο _ αν χρησιμοποιήσουμε την M_{space}).

4. Επιστρέφει στην αρχή της ταινίας και αλλάξει την κατάσταση στον ελεγκτή σύμφωνα με τη δ.

Τέλος, πριν ξεκινήσει τη λειτουργία της η M με είσοδο τη λέξη $w = x_1 \cdots x_n \in \Sigma^*$, η M τρέχει μία υπορουτίνα, έστω M_{pre}, που τροποποιεί την ταινία της ως εξής:

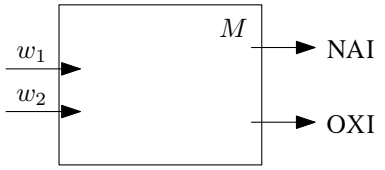


□

Συμβολισμός 1.3.4 (Κουτάκια συνέχεια...).

[1] Για παράδειγμα αν η M_k πρέπει να προσθέσει κάποιο σύμβολο στο τέλος της λέξης που περιέχει μία ταινία.

5. Πολλές φορές στη συνέχεια, όταν σχεδιάζουμε μία ΤΜ M, θα γράφουμε (παραδείγματος χάρη):



εννοώντας ότι η M είναι ΤΜ δύο ταινιών, όπου η πρώτη ταινία γράφει την είσοδο w_1 και η δεύτερη την είσοδο w_2 [1].

1.3.2 Μη-ντετερμινιστικές Μηχανές Turing

Από τη *Θεωρία Υπολογιστικής Πολυπλοκότητας* γνωρίζουμε ότι η προσθήκη επιπλέον ταινιών σε μία ΤΜ δεν βελτιώνει ουσιαστικά τον χρόνο του υπολογισμού. Από την άλλη πλευρά, αν προσθέσουμε στη ΤΜ τη δυνατότητα να κάνει και *μη-ντετερμινιστικά βήματα* τότε η βελτίωση στον χρόνο είναι ουσιαστική [2]. Όμως όσον αφορά τη Θεωρία Υπολογισμού που μελετάμε εδώ, βελτιώσεις στη *χρονική πολυπλοκότητα* δεν λαμβάνονται υπόψιν καθώς ενδιαφερόμαστε αποκλειστικά και μόνο για το αν μία συνάρτηση είναι υπολογίσιμη ή όχι.

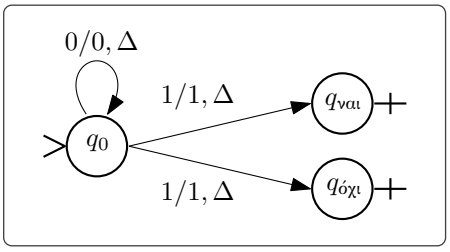
Για τον ορισμό της *Μη-ντετερμινιστικής ΤΜ* θα χρησιμοποιήσουμε την παραλλαγή με τις δύο τερματικές καταστάσεις.

Ορισμός 1.3.5. *Μη-ντετερμινιστική Μηχανή Turing (NTM)* είναι μια επτάδα $N = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{ναι}}, q_{\text{όχι}})$ όπου Q, Σ, Γ πεπερασμένα σύνολα, και:

1. Q είναι το *σύνολο των καταστάσεων*
2. $q_0, q_{\text{ναι}}, q_{\text{όχι}} \in Q$, με $q_{\text{ναι}} \neq q_{\text{όχι}}$ όπου $q_{\text{ναι}}, q_{\text{όχι}}$ οι τερματικές καταστάσεις
3. Σ είναι το *αλφάβητο εισόδου*
4. Γ είναι το *αλφάβητο ταινίας*
5. $\Sigma \subset \Gamma$
6. $\triangleright, \sqcup \in \Gamma \setminus \Sigma$
7. $\delta \subseteq Q \times \Gamma \times Q \times \Gamma \times \{\text{Α}, \Delta\}$ είναι η *σχέση μετάβασης* που ικανοποιεί τους ακόλουθους περιορισμούς:

[1] Γνωρίζοντας (από το Θεώρημα 1.3.3) ότι υπάρχει ισοδύναμη μονοταινιακή ΤΜ θα θεωρούμε καταχρηστικά ότι και η μηχανή που χρησιμοποιεί την M ως υπορουτίνα είναι μονοταινιακή.

[2] Για παράδειγμα αν θέλουμε να βρούμε τη θέση ενός στοιχείου x σε έναν πίνακα A με n στοιχεία, μη-ντετερμινιστικά μπορούμε να πάρουμε την απάντηση σε ένα μόνο βήμα (ελέγχουμε μη-ντετερμινιστικά αν το στοιχείο $A[i],\ i = 1, \ldots, n$, ταυτίζεται με το x. Ντετερμινιστικά όμως, στη χειρότερη περίπτωση, θα πρέπει να επισκεφτούμε όλα τα κελιά του A για να βρούμε την απάντηση (εκτός βέβαια αν ο A είναι ταξινομημένος, όπου και πάλι θα χρειαστεί να ελέγξουμε $\log n$ κελιά).



Σχήμα 1.3.3: *Παράδειγμα μη-ντετερμινιστικής ΤΜ.*

- $\forall a, b \in \Gamma\ \forall q \in Q\ \forall x \in \{\text{Α}, \Delta\}((q_{\text{ναι}}, a, q, b, x) \notin \delta \wedge (q_{\text{όχι}}, a, q, b, x) \notin \delta)$
- $\forall q \in Q \setminus \{q_{\text{ναι}}, q_{\text{όχι}}\}\ \forall q' \in Q\ \forall a \in \Gamma((q, \triangleright, q', a, x) \in \delta \rightarrow x = \Delta \wedge a = \triangleright)$

Ο υπολογισμός της N κάθε φορά που η δ έχει παραπάνω από μία επιλογές για το επόμενο στιγμιότυπο λειτουργίας (*μη-ντετερμινιστικό βήμα*) χωρίζεται σε δύο ή περισσότερα *υπολογιστικά σενάρια*. Συνεπώς, αντί να έχουμε ένα μονοπάτι υπολογισμού, όπως στην περίπτωση των ντετερμινιστικών ΤΜ, έχουμε ένα *δέντρο υπολογισμού*, που πιθανόν να έχει «κλαδιά» με άπειρο μήκος.

Παράδειγμα 1.3.6. Η ΤΜ N του Σχήματος 1.3.3 είναι μία μη-ντετερμινιστική ΤΜ. Παρατηρήστε ότι ο υπολογισμός της N με είσοδο 0010 αποτελείται από δύο υπολογιστικά σενάρια:

$1^ο$ σενάριο: $\triangleright\, q_0 0010 \vdash_N \triangleright\, 0 q_0 010 \vdash_N \triangleright\, 00 q_0 10 \vdash_N \triangleright\, 001 q_{\text{ναι}} 0$

$2^ο$ σενάριο: $\triangleright\, q_0 0010 \vdash_N \triangleright\, 0 q_0 010 \vdash_N \triangleright\, 00 q_0 10 \vdash_N \triangleright\, 001 q_{\text{όχι}} 0$

Ορισμός 1.3.7. Έστω συνάρτηση $f : \Sigma^* \rightarrow \Sigma^*$ και ΝΤΜ N. Η N *υπολογίζει* την f αν για κάθε $w \in \Sigma^*$:

- αν $w \in \mathsf{dom}(f)$, τότε κάθε υπολογιστικό σενάριο της $N(w)$ τερματίζει σε στιγμιότυπο της μορφής $\triangleright\, q f(w)$, όπου $q \in \{q_{\text{ναι}}, q_{\text{όχι}}\}$,
- αν $w \notin \mathsf{dom}(f)$, τότε υπάρχει υπολογιστικό σενάριο της $N(w)$ που δεν τερματίζει.

Ορισμός 1.3.8. Έστω ΝΤΜ $N = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{ναι}}, q_{\text{όχι}})$. Η γλώσσα που *αναγνωρίζει* (ή *αποδέχεται*) η N είναι η:

$$L(N) = \{w \in \Sigma^* \mid \exists w_1, w_2 \in \Gamma^*(\triangleright\, q_0 w \vdash_N^* \triangleright\, w_1 q_{\text{ναι}} w_2)\}$$

δηλαδή υπάρχει υπολογιστικό σενάριο στο οποίο εμφανίζεται η $q_{\text{ναι}}$ [1].

Ορισμός 1.3.9. Έστω $L \subseteq \Sigma^*$ και ΝΤΜ N. Η N *ημι-αποφασίζει* την L αν:

(Α) $L = L(N)$

[1] Δεν έχει σημασία αν στα υπόλοιπα σενάρια η N κολλάει ή απορρίπτει.

Ορισμός 1.3.10. Έστω $L \subseteq \Sigma^*$ και NTM N. Η N *αποφασίζει* την L ανν:

(Α) $L = L(N)$

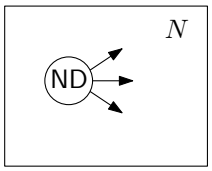
(Β) Για κάθε $w \in \Sigma^*$, κάθε υπολογιστικό σενάριο της $N(w)$ τερματίζει.

Παρατήρηση 1.3.11. Μία NTM απορρίπτει την είσοδο της ανν κάθε υπολογιστικό σενάριο τερματίζει στην $q_{\text{όχι}}$.

Παράδειγμα 1.3.12. Η NTM του Παραδείγματος 1.3.6 ημι-αποφασίζει τη γλώσσα $L = \{w \in \{0,1\}^* \mid \text{η } w \text{ περιέχει τουλάχιστον ένα } 1\}$ [1].

Συμβολισμός 1.3.13 (Κουτάκια συνέχεια...).

6. Όταν σχεδιάζουμε μία N.T.M N θα σημειώνουμε τα μη-ντετερμινιστικά βήματα ως εξής (παραδείγματος χάρη αν έχουμε τρεις μη-ντετερμινιστικές επιλογές):



Θεώρημα 1.3.14. Για κάθε NTM υπάρχει ισοδύναμη TM.

Απόδειξη. [2] Έστω NTM $N = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{ναι}}, q_{\text{όχι}})$. Θα δείξουμε ότι υπάρχει TM M (με τρεις ταινίες σε πρώτη φάση) τέτοια ώστε:

$$\forall w \in \Sigma^* (w \in L(N) \leftrightarrow w \in L(M))$$

Η ιδέα της απόδειξης είναι η ακόλουθη:

> *Δοσμένης μίας λέξης $w \in \Sigma^*$ «ακολουθούμε» όλα τα υπολογιστικά σενάρια στο δέντρο υπολογισμού της $N(w)$ για πεπερασμένο αριθμό βημάτων, έστω $k \in \mathbb{N}$. Ελέγχουμε αν κάποιο από αυτά τερματίζει στην $q_{\text{ναι}}$. Αν υπάρχει τέτοιο σενάριο, η $M(w)$ τερματίζει και επιστρέφει ΝΑΙ, αλλιώς αυξάνουμε το k και επαναλαμβάνουμε τον έλεγχο.*

Παρατηρούμε ότι για κάθε $w \in \Sigma^*$:

- Αν $w \in L(N)$ τότε υπάρχει $k_0 \in \mathbb{N}$ τέτοιο ώστε κάποιο υπολογιστικό σενάριο της $N(w)$ τερματίζει στην $q_{\text{ναι}}$. Συνεπώς, όταν ακολουθούμε τα υπολογιστικά σενάρια της $N(w)$ για k_0 βήματα, η $M(w)$ θα τερματίσει στην $q_{\text{ναι}}$. Άρα $w \in L(M)$.

[1] Δεν την αποφασίζει γιατί, παραδείγματος χάρη, για την ϵ υπάρχουν σενάρια στο υπολογιστικό δέντρο της $N(\epsilon)$ που δεν τερματίζουν (όλα για την ακρίβεια).

[2] Θα δείξουμε μόνο την (πιο εύκολη) περίπτωση όπου η NTM ημι-αποφασίζει μία γλώσσα (η κεντρική ιδέα είναι ίδια και για την περίπτωση όπου η NTM αποφασίζει μία γλώσσα ή υπολογίζει μία συνάρτηση).

- Αν $w \notin L(N)$ τότε για κάθε $k \in \mathbb{N}$ δεν υπάρχει υπολογιστικό σενάριο της $N(w)$ που τερματίζει στην $q_{\text{ναι}}$. Συνεπώς, η $M(w)$ δεν τερματίζει ποτέ. Άρα $w \notin L(M)$.

Για να διευκολύνουμε την παρουσίαση θα θεωρήσουμε χωρίς βλάβη της γενικότητας ότι κάθε βήμα της $N(w)$ είναι μη-ντετερμινιστικό. Για ένα ζεύγος (q, a), όπου $q \in Q$ και $a \in \Gamma$ υπάρχουν το πολύ $r = |Q| \cdot |\Gamma| \cdot 2$ διαφορετικές δυνατές τιμές για το (q, a, p, b, x) όπου $p \in Q$, $b \in \Gamma$ και $x \in \{\text{A}, \Delta\}$. Συνεπώς σε κάθε βήμα της $N(w)$ υπάρχουν το πολύ r μη-ντετερμινιστικές επιλογές. Θεωρώντας μία αρίθμηση των r αυτών επιλογών παρατηρούμε ότι σε κάθε υπολογιστικό σενάριο το επόμενο στιγμιότυπο προκύπτει από έναν αριθμό στο $[r]$ (τη μη-ντετερμινιστική επιλογή δηλαδή που θα εκτελέσει η $N(w)$). Συνεπώς ένα υπολογιστικό σενάριο k-βημάτων, $k \in \mathbb{N}$, μπορεί να χαρακτηρισθεί από μία λέξη $c \in \{1, \dots, r\}^*$ με μήκος k [1].

Θεωρούμε την TM N_D του Σχήματος 1.3.4 η οποία δέχεται σαν είσοδο τη w και μία λέξη $c \in \{1, \dots, r\}^*$ και «τρέχει», με ντετερμινιστικό τρόπο, την $N(w)$ ως εξής: Σε κάθε βήμα της η $N_D(w, c)$ διαβάζει ένα σύμβολο από τη δεύτερη ταινία (που περιέχει τη c), δηλαδή έναν αριθμό, έστω c_0, στο $[r]$, και κάνει ότι θα έκανε η $N(w)$ εφαρμόζοντας τη c_0-οστή μη-ντετερμινιστική επιλογή [2].

- Αν η $N(w)$, κάνοντας τις επιλογές της c, φτάσει στην $q_{\text{ναι}}$ τότε η $N_D(w, c)$ επιστρέφει NAI.

- Αν η δεύτερη κεφαλή διαβάσει $\sqcup$ (δηλαδή τελείωσαν οι επιλογές της c) η $N_D(w, c)$ θα πάει σε μία ειδική κατάσταση, έστω την q_{next}.

- Αν για κάποιο $i \in [|c|]$ η c_i-οστή μη-ντετερμινιστική επιλογή δεν αποτελεί επιλογή για την N, η $N_D(w, c)$ θα πάει στην q_{next}.

Θεωρούμε επίσης την TM M_{next} που δέχεται σαν είσοδο μία λέξη $w \in \{1, \dots, r\}^*$ και επιστρέφει την επόμενη λέξη $\mathsf{next}(w)$(σύμφωνα με την λεξικογραφική διάταξη του $\{1, \dots, r\}^*$).

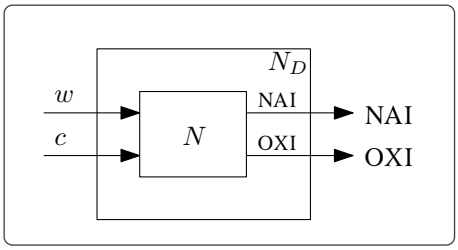
Τέλος, κατασκευάζουμε την TM M του Σχήματος 1.3.5, της οποίας η πρώτη ταινία περιέχει την w και δεν αλλάξει ποτέ, και οι άλλες δύο χρησιμοποιούνται από την N_D.

Από το Θεώρημα 1.3.3 γνωρίζουμε ότι υπάρχει μονοταινιακή TM M' που είναι ισοδύναμη με την M. Η M' είναι η ζητούμενη TM. □

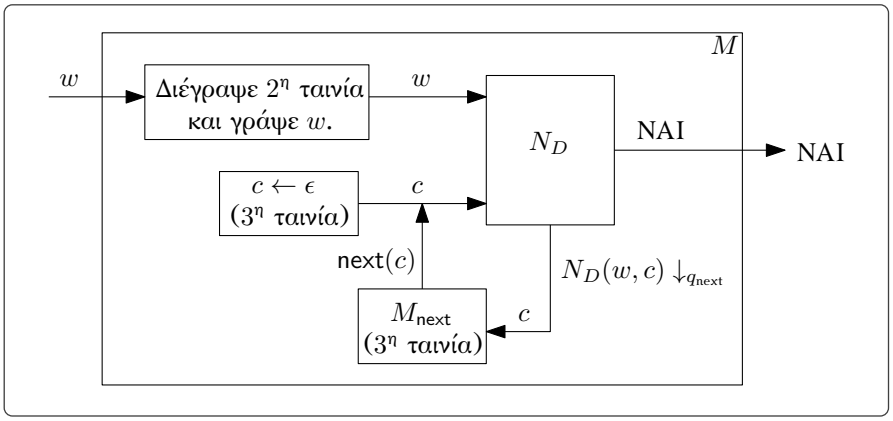
Παρατήρηση 1.3.15. Σύμφωνα με το Θεώρημα 1.3.14 ούτε οι NTM είναι ικανές να επεκτείνουν το σύνολο των υπολογίσιμων συναρτήσεων (ή των διαγνώσιμων/αποφάνσιμων γλωσσών).

[1] Για παράδειγμα η λέξη $c_1 \cdots c_k$ (ή πιο σωστά $c_1\#\cdots\#c_k$, όπου το σύμβολο # χρησιμοποιείτε για να διαχωρίσουμε τους αριθμούς μεταξύ τους, οπότε είναι λέξη μήκους $2k-1$ από το αλφάβητο $\{1, \dots, r, \#\}$) είναι ένα υπολογιστικό σενάριο k-βημάτων, που στο πρώτο μη-ντετερμινιστικό βήμα κάνουμε την επιλογή c_1, στο δεύτερο τη c_2 κ.ο.κ.. Τυπικά θα θεωρήσουμε ότι αν σε κάποιο βήμα υπολογισμού η επιλογή c_i, $i \leq k$, δεν υπάρχει στη σχέση δ θα την αγνοούμε και θα πηγαίνουμε στην επόμενη επιλογή.

[2] Αυτό γίνεται προσθέτοντας ξεχωριστές καταστάσεις για κάθε ένα από τα μη-ντετερμινιστικά βήματα και αφού μεταβούμε στην κατάλληλη κατάσταση, συνεχίζουμε τον υπολογισμό όπως επιβάλει η σχέση μεταβάσεων της NTM.



Σχήμα 1.3.4: *Η TM N_D στην απόδειξη του Θεωρήματος 1.3.14.*



Σχήμα 1.3.5: *Η TM M στην απόδειξη του Θεωρήματος 1.3.14.*

Σημείωση 1.3.16. Μπορούμε να ορίσουμε πολλές ακόμα παραλλαγές ΤΜ, όπως για παράδειγμα ΤΜ με άπειρη ταινία και από τις δύο μεριές ή ΤΜ με άπειρο πίνακα αντί για ταινία, όπως επίσης και συνδυασμούς παραλλαγών ΤΜ, για παράδειγμα πολυταινιακές μηντετερμινιστικές ΤΜ (δες την απόδειξη του Θεωρήματος 4.1.9). Όλες αυτές οι παραλλαγές αποδεικνύεται ότι είναι ισοδύναμες με την απλή ΤΜ (δες Ασκήσεις 1.2 και 1.3).

Εκτός από τις επεκτάσεις των ΤΜ, για να διευκολύνουμε την παρουσίαση των αποδείξεων συχνά θα υποθέτουμε ότι μία δοσμένη ΤΜ ικανοποιεί κάποιους περιορισμούς, που δεν θα βλάπτουν όμως τη γενικότητα (για παράδειγμα δες τις αποδείξεις των Θεωρημάτων 2.5.1 και 4.1.9).

1.4 Καθολική Μηχανή Turing

Ο φορμαλισμός που εισήγαγε ο Alan Turing έχει επικρατήσει έναντι των υπόλοιπων φορμαλισμών (ιδιαιτέρως μετά την έλευση του Η/Υ), και πλέον είναι ο βασικός φορμαλισμός που χρησιμοποιείται τόσο σε μαθήματα Υπολογιστικής Πολυπλοκότητας όσο και σε μαθήματα Θεωρίας Υπολογισμού. Ο κύριος λόγος είναι το γεγονός ότι μπορούμε να διακρίνουμε πολλές πτυχές της λειτουργίας των σημερινών υπολογιστών στις ΤΜ (σε πολύ πιο στοιχειώδη μορφή φυσικά). Μία από αυτές τις λειτουργίες – ίσως η πιο ουσιαστική σε έναν

Η/Υ – είναι η δυνατότητά τους να «προγραμματίζονται», δηλαδή να εισάγουμε σε αυτούς κάποιες απλές οδηγίες και αυτοί με τις σειρά τους να τις διεκπεραιώνουν. Σε πρώτη ανάγνωση, ο προγραμματισμός μπορεί να μην μοιάζει και τόσο σημαντικός, σκεφτείτε όμως ότι οι πρώτοι υπολογιστές που κατασκευάστηκαν είχαν μία και μοναδική λειτουργία (ή, έστω, ένα πολύ περιορισμένο σύνολο λειτουργιών [1]), πράγμα που μείωνε δραματικά το εύρος εφαρμογών τους.

Μέχρι τώρα είδαμε ότι η ΤΜ μπορεί να θεωρηθεί το πρόγραμμα που υπολογίζει μία (και μόνο μία) συνάρτηση (ή αποφασίζει/ημι-αποφασίζει μία και μόνο μία γλώσσα). Σε αυτήν την παράγραφο θα ορίσουμε μία ΤΜ που δέχεται σαν είσοδο την *κωδικοποίηση* μίας άλλης ΤΜ, μαζί με μία λέξη εισόδου, και φέρει «εις πέρας» τον υπολογισμό της δεύτερης. Έτσι, στην ουσία, οι ΤΜ μπορούν να προγραμματίζονται όπως ακριβώς και ο Η/Υ μας!

Καθώς θα χρησιμοποιούμε συνεχώς παραλλαγές αυτής της μηχανή θα της δώσουμε ένα ξεχωριστό όνομα, θα την αποκαλούμε *Καθολική Μηχανή Turing*. Πριν περάσουμε όμως στον ορισμό της θα πρέπει να συμφωνήσουμε σε μία κωδικοποίηση των ΤΜ.

Κωδικοποίηση Μηχανών Turing στο αλφάβητο $\{0,1\}$

Συμβολισμός 1.4.1. Έστω αλφάβητο Σ. Θα χρησιμοποιούμε τον συμβολισμό $\langle * \rangle_\Sigma$ για να δηλώσουμε το γεγονός ότι το $*$ είναι κωδικοποιημένο στο αλφάβητο Σ [2].

Έστω ΤΜ $M = (Q, \{0,1\}, \{\triangleright, \sqcup, 0, 1\}, \delta, q_0, q_{\text{ναι}}, q_{\text{όχι}})$. Φυσικά μπορούμε να κωδικοποιήσουμε και τις ΤΜ που έχουν περισσότερα από τέσσερα σύμβολα στο αλφάβητο ταινίας τους. Θα κρατήσουμε όμως το μέγεθος του Γ στο ελάχιστο δυνατό για να διευκολύνουμε την παρουσίαση.

Αναφέραμε στο παρελθόν ότι η δ περιέχει όλη την πληροφορία που χαρακτηρίζει την M. Θα ήταν πιο σωστό να πούμε ότι περιέχει όλη την «ουσιαστική» πληροφορία της M. Κάτι που δεν γίνεται με την πρώτη ματιά ορατό είναι ότι αν η M περιέχει καταστάσεις που είναι μη προσβάσιμες (δηλαδή για οποιαδήποτε λέξη w η $M(w)$ δεν μεταβαίνει ποτέ σε αυτές) τότε αυτές δεν θα εμφανίζονται στις μεταβάσεις της δ. Το ίδιο συμβαίνει επίσης αν το Γ περιέχει σύμβολα που δεν χρησιμοποιούνται ποτέ.

Συνεπώς θα πρέπει, ναι μεν να κωδικοποιήσουμε τη δ, αλλά με τρόπο ώστε να αποτυπώνεται και η πληροφορία που ενδεχομένως της διαφεύγει. Για λόγους που θα φανούν στη συνέχεια, θέλουμε η κωδικοποίηση μιας ΤΜ να είναι μονοσύμαντη (Πρόταση 1.4.6). Αυτό δεν θα μπορούσε να γίνει εφικτό αν δεν καταγράφαμε στην κωδικοποίηση το πλήθος μη προσβάσιμων καταστάσεων ή μη χρησιμοποιούμενων συμβόλων.

Θα ξεκινήσουμε σε πρώτη φάση κωδικοποιώντας τη δ σε μία λέξη του αλφαβήτου $\Sigma = \{0, 1, q, s, d, \#\}$:

- Κάθε κατάσταση του Q κωδικοποιείται από το q ακολουθούμενο από μία λέξη του

[1] Όπως για παράδειγμα η *Διαφορική Μηχανή* και η *Αναλυτική Μηχανή* (που υποστήριξε αρκετές στοιχειώδεις υπολογιστικές λειτουργίες και χρησιμοποιούσε διάτρητες κάρτες για την επιλογή μεταξύ τους), που σχεδίασε ο *Charles Babbage* στις αρχές του $19^{ου}$ αιώνα.

[2] Όπως θα δούμε λίαν συντόμως, το $*$ μπορεί να είναι σύμβολο, λέξη, συνάρτηση ακόμα και ΤΜ.

$\{0,1\}$ μήκους $|Q|-1$ [1]:

$$\begin{aligned} & & & \overbrace{\qquad}^{|Q|-1\text{-φορές}} \\ \langle q_0\rangle_\Sigma &= q\overbrace{00\cdots00} \\ \langle q_1\rangle_\Sigma &= q00\cdots01 \\ \langle q_2\rangle_\Sigma &= q00\cdots11 \\ &\vdots \\ \langle q_{\text{ναι}}\rangle_\Sigma &= q01\cdots11 \\ \langle q_{\text{όχι}}\rangle_\Sigma &= q11\cdots11 \end{aligned}$$

- Κωδικοποιούμε τα σύμβολα του $\{\triangleright, \sqcup, 0, 1\}$ ως εξής [2]:

$$\begin{aligned} \langle \triangleright\rangle_\Sigma &= s000 \\ \langle \sqcup\rangle_\Sigma &= s001 \\ \langle 0\rangle_\Sigma &= s011 \\ \langle 1\rangle_\Sigma &= s111 \end{aligned}$$

- Κωδικοποιούμε τα A, Δ ως εξής:

$$\begin{aligned} \langle \mathrm{A}\rangle_\Sigma &= d0 \\ \langle \Delta\rangle_\Sigma &= d1 \end{aligned}$$

- Κωδικοποιούμε κάθε μετάβαση $(q,a,p,b,x) \in \delta$, όπου $a,b \in \{\triangleright, \sqcup, 0, 1\}$, $q,p \in Q$ και $x \in \{\mathrm{A}, \Delta\}$ ως εξής:

$$\langle (q,a,p,b,x)\rangle_\Sigma = \langle q\rangle_\Sigma\langle a\rangle_\Sigma\langle p\rangle_\Sigma\langle b\rangle_\Sigma\langle x\rangle_\Sigma$$

- Τέλος, έστω $\delta = \{\delta_1, \delta_2, \ldots, \delta_k\}$, κωδικοποιούμε τη δ ως εξής:

$$\langle \delta\rangle_\Sigma = \langle \delta_1\rangle_\Sigma\#\langle \delta_2\rangle_\Sigma\#\cdots\#\langle \delta_k\rangle_\Sigma$$

Παράδειγμα 1.4.2. Η συνάρτηση μετάβασης της TM του Παραδείγματος 1.2.26 (δες Σχήμα 1.2.8) κωδικοποιείται στη λέξη του $\{0,1,q,s,d,\#\}^*$:

$$q00s011q00s011d1\#q00s001q01s001d1\#q00s111q11s111d1$$

[1] Ένας λόγος που θέλουμε να έχουμε το ίδιο πλήθος συμβόλων στην κωδικοποίηση όλων των καταστάσεων είναι ότι μας βολεύει κατά τη λειτουργία της καθολικής TM. Ο σημαντικότερος όμως λόγος είναι ότι με αυτόν τον τρόπο μπορούμε να ελέγξουμε αν υπάρχουν μη προσβάσιμες καταστάσεις: Μετράμε το πλήθος ψηφίων που ακολουθούν το σύμβολο q και προσθέτουμε ένα για να βρούμε το $|Q|$.Έπειτα αφαιρούμε από το $|Q|$ το πλήθος των διαφορετικών καταστάσεων που εμφανίζονται στην κωδικοποίηση της δ.

[2] Αν το Γ είχε περισσότερα σύμβολα θα τα κωδικοποιούσαμε κατά τον ίδιο τρόπο. Πάλι, μετρώντας το πλήθος ψηφίων που ακολουθούν το σύμβολο s μπορούμε να βρούμε το $|\Gamma|$.

Παρατηρήστε ότι με τον τρόπο που κωδικοποιήσαμε το σύνολο καταστάσεων και το αλφάβητο ταινίας καταφέραμε να αποτυπώσουμε και τον πληθάριθμο των δύο συνόλων. Αυτό είναι απαραίτητο έτσι ώστε ΤΜ με την ίδια συνάρτηση μεταβάσεων αλλά με μη προσβάσιμες καταστάσεις ή μη χρησιμοποιούμενα σύμβολα να έχουν διαφορετική κωδικοποίηση. Μία ακόμα περίπτωση που θα πρέπει να λάβουμε υπόψιν μας είναι η περίπτωση που $\delta = \varnothing$ (όταν έχουμε δηλαδή ΤΜ που υπολογίζει την ταυτοτική συνάρτηση, Παράδειγμα 1.2.2). Σε αυτήν την περίπτωση η κωδικοποίηση που αναφέραμε παραπάνω αποτυγχάνει! Θα διορθώσουμε το πρόβλημα προσθέτωντας πριν από την $\langle \delta \rangle_\Sigma$ τη δυαδική αναπαράσταση των αριθμών $|Q|$ και $|\Gamma|$. Άρα τελικά:

$$\langle M \rangle_\Sigma = \langle |Q| \rangle_{\{0,1\}} \# \langle |\Gamma| \rangle_{\{0,1\}} \# \langle \delta \rangle_\Sigma$$

Με αυτόν τον τρόπο μπορούμε να κωδικοποιήσουμε και ΤΜ με κενή συνάρτηση μεταβάσεων.

Παράδειγμα 1.4.3. Η ΤΜ του Παραδείγματος 1.2.26 (δες Σχήμα 1.2.8) κωδικοποιείται στη λέξη του $\{0, 1, q, s, d, \#\}^*$:

$$10\#100\#q00s011q00s011d1\#q00s001q01s001d1\#q00s111q11s111d1$$

Παρατήρηση 1.4.4. Μπορούμε περαιτέρω να κωδικοποιήσουμε τα σύμβολα του $\{0, 1, q, s, d, \#\}$ στο $\{0, 1\}$, όπως για παράδειγμα:

$$\begin{aligned}
\langle 0 \rangle_{\{0,1\}} &= 001 \\
\langle 1 \rangle_{\{0,1\}} &= 010 \\
\langle q \rangle_{\{0,1\}} &= 011 \\
\langle s \rangle_{\{0,1\}} &= 100 \\
\langle d \rangle_{\{0,1\}} &= 101 \\
\langle \# \rangle_{\{0,1\}} &= 110
\end{aligned}$$

Παράδειγμα 1.4.5. Η ΤΜ του Παραδείγματος 1.2.26 (Σχήμα 1.2.8) κωδικοποιείται στη λέξη του $\{0, 1\}^*$:

010 010 110

010 001 001 110

011 001 001 100 001 001 010 011 001 010 100 001 001 010 101 010 110

011 001 001 100 001 010 010 011 001 001 100 001 010 010 101 010 110

011 001 001 100 010 010 010 011 010 010 100 010 010 010 101 010

(Η γραμμή αλλάζει μετά από κάθε # [1].)

Συνεπώς καταλήγουμε στην ακόλουθη Πρόταση.

Πρόταση 1.4.6. Κάθε ΤΜ κωδικοποιείται μονοσήμαντα [2] σε μία λέξη του $\{0, 1\}^*$.

[1] Παρατηρήστε ότι οι κωδικοποιήσεις των μεταβάσεων έχουν τοποθετηθεί ακολουθώντας τη λεξικογραφική διάταξη των επιμέρους κωδικοποιήσεων τους. Ο λόγος που αυτό είναι απαραίτητο φαίνεται στην Πρόταση που ακολουθεί (Πρόταση 1.4.6).

[2] Αυτό δεν είναι απολύτως ακριβές, καθώς η κωδικοποίηση που παρουσιάσαμε εξαρτάται από τη σειρά που έχουμε επιλέξει για τις πεντάδες της συνάρτησης μετάβασης δ. Για να έχουμε μονοσήμαντη κωδικοποίηση θα πρέπει να συμφωνήσουμε και σε μία συγκεκριμένη σειρά. Θα μπορούσαμε παραδείγματος χάρη να ακολουθήσουμε τη σειρά που έχει μία πεντάδα στη λεξικογραφική διάταξη όταν κωδικοποιηθεί σε λέξη του $\{0, 1\}^*$.

Παρατήρηση 1.4.7. Ακολουθώντας την «αντίστροφη» διαδικασία από αυτήν που ακολουθήσαμε στην κωδικοποίηση των TM μπορούμε, πρώτον να ελέγξουμε αν μια λέξη του $\{0,1\}^*$ αποτελεί κωδικοποίηση TM και, δεύτερον, αν όντως αποτελεί κωδικοποίηση, να δούμε τις μεταβάσεις της. Αυτή η διαδικασία καλείται *αποκωδικοποίηση*.

Σημείωση 1.4.8. Υπάρχουν πολύ πιο «αποδοτικοί» τρόποι να κωδικοποιήσουμε τις TM από αυτόν που είδαμε [1], όμως το επίθετο *αποδοτικός* σε αυτές τις σημειώσεις χρησιμοποιείται μόνο όπου θέλουμε να τονίσουμε ότι δεν ενδιαφερόμαστε στο να κάνουμε τον υπολογισμό πιο αποδοτικό κατ' οποιονδήποτε τρόπο.

Σύμβαση 1.4.9. Όταν το αλφάβητο στο οποίο έχουμε κωδικοποιήσει μία TM εννοείται από τα συμφραζόμενα θα χρησιμοποιούμε τον απλουστευμένο συμβολισμό $\langle M \rangle$.

Ορισμός 1.4.10. Θεωρούμε το σύνολο $\mathcal{G} = \{w \in \{0,1\}^* \mid \text{Υπάρχει TM } M \text{ τέτοια ώστε } w = \langle M \rangle\}$ [2]. Μπορούμε να διατάξουμε τις λέξεις του $\mathcal{G}$ σύμφωνα με τη λεξικογραφική διάταξη του $\{0,1\}^*$, ορίζοντας έτσι μία συνάρτηση $\text{Gödel} : \mathcal{G} \to \mathbb{N}$, όπου:

$$\text{Gödel}(M) = \text{«Η σειρά εμφάνισης της } \langle M \rangle \text{ στο } \mathcal{G} \text{ σύμφωνα με τη λεξικογραφική διάταξη του } \{0,1\}^*\text{»} \text{ [3]}$$

Το $\text{Gödel}(M)$ καλείται *αριθμός Gödel* της M.

Παρατήρηση 1.4.11. Ισχύει ότι $\mathcal{G} \in \text{REC}$ και ότι η συνάρτηση Gödel είναι υπολογίσιμη, 1-1 και επί [4].

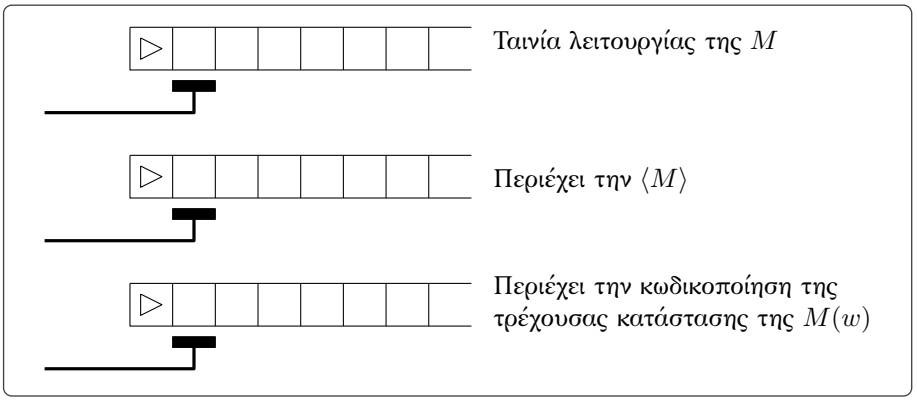
Χρησιμοποιώντας τη συνάρτηση Gödel μπορούμε να δείξουμε (μη-κατασκευαστικά) ότι η απάντηση στο Ερώτημα 2 (σελίδα 28) είναι καταφατική.

Θεώρημα 1.4.12. Υπάρχει γλώσσα $L \in 2^{\{0,1\}^*} \setminus \text{RE}$.

Απόδειξη. Αφού η Gödel είναι μια 1-1 και επί συνάρτηση από το $\mathcal{G}$ στο $\mathbb{N}$ έπεται ότι $|\mathcal{G}| = \aleph_0$. Από την Παρατήρηση 0.2.16 και το Θεώρημα 0.1.17 προκύπτει ότι $|2^{\{0,1\}^*}| > \aleph_0$. Ως συνέπεια δεν μπορεί να υπάρχει 1-1 και επί συνάρτηση από το $2^{\{0,1\}^*}$ στο $\mathcal{G}$. Οπότε υπάρχει γλώσσα $L \in 2^{\{0,1\}^*}$ για την οποία δεν υπάρχει TM M με $L(M) = L$ [5]. □

Παρατήρηση 1.4.13. Αφού το σύνολο των συναρτήσεων από το $\{0,1\}^*$ στο $\{0,1\}^*$ έχει πληθάριθμο τουλάχιστον τον πληθάριθμο του $2^{\{0,1\}^*}$ [6], έπεται επίσης ότι υπάρχουν μη-υπολογίσιμες συναρτήσεις.

[1] Που θα παρήγαγαν για παράδειγμα κωδικοποιήσεις με πολύ μικρότερο μήκος.
[2] Χάριν απλότητας θα γράφαμε $\mathcal{G} = \{\langle M \rangle \in \{0,1\}^* \mid \text{Η } M \text{ είναι TM}\}$.
[3] Για να απλοποιήσουμε λίγο τον συμβολισμό γράφουμε $\text{Gödel}(M)$ και όχι $\text{Gödel}(\langle M \rangle)$.
[4] Οι λεπτομέρειες της απόδειξης αυτής της παρατήρησης αφήνονται ως άσκηση (Άσκηση 1.4).
[5] Για λόγους πληρότητας πρέπει να τονίσουμε, μία ακόμα φορά, ότι κάθε TM κωδικοποιείται μονοσήμαντα στο $\{0,1\}$ και ότι αναγνωρίζει ακριβώς μία γλώσσα.
[6] Το σύνολο αυτό περιέχει για κάθε στοιχείο $L \in 2^{\{0,1\}^*}$ και μία συνάρτηση, τη χ_L.



Σχήμα 1.4.1: *Οι τρεις ταινίες μίας Καθολικής ΤΜ.*

Ορισμός Καθολικής Μηχανής Turing

Ορισμός 1.4.14. *Καθολική Μηχανή Turing* (συμβολισμός $\mathbb{M}$) είναι μία ΤΜ τριών ταινιών (Σχήμα 1.4.1) με αλφάβητο εισόδου το $\{0,1\}$, που δέχεται ως είσοδο την κωδικοποίηση μίας ΤΜ $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{ναι}}, q_{\text{όχι}})$ και μίας λέξης w (την είσοδο για την M) στο $\{0,1\}^*$, συμβολισμός $\langle M, w \rangle$ [1], και μπορεί να προσομοιώσει την $M(w)$. Η 1^{η} ταινία της $\mathbb{M}$ περιέχει την είσοδό της. Στην αρχή του υπολογισμού $\mathbb{M}(\langle M, w \rangle)$ η $\mathbb{M}$ κάνει τα ακόλουθα:

1. Αντιγράφει την $\langle M \rangle$ στην 2^{η} ταινία της και αφήνει την $\langle w \rangle$ στην 1^{η}.
2. Γράφει $\langle q_0 \rangle$ στην 3^{η} ταινία της.

Έπειτα, σε κάθε βήμα προσομοίωσης (ενός βήματος της $M(w)$) η $\mathbb{M}(\langle M, w \rangle)$ κάνει τα ακόλουθα:

1. Διαβάζει την κατάσταση που γράφει η 3^{η} ταινία και το (κωδικοποιημένο) σύμβολο της $1^{\eta\varsigma}$ ταινίας (προσπελάσει δηλαδή όλα τα κελιά της $1^{\eta\varsigma}$ ταινίας που αποτελούν την κωδικοποίηση του συμβόλου που διαβάζει η M).
2. Ψάχνει μετάβαση της M στην 2^{η} ταινία που να ξεκινάει με τον συνδυασμό κατάστασης και συμβόλου που διάβασε.
3. - Αν βρει τέτοια μετάβαση:
   (α΄) γράφει την κωδικοποίηση της καινούριας κατάσταση στην 3^{η} ταινία,
   (β΄) γράφει την κωδικοποίηση του καινούριο συμβόλου στη θέση της κωδικοποίησης του παλιού [2] και

[1] Γράφουμε $\langle M, w \rangle$ βάζοντας «κάτω από το χαλί» τις λεπτομέρειες που αποκρύπτει αυτός ο συμβολισμός.

[2] Παρατηρήστε ότι δεν θα χρειαστεί ποτέ να δημιουργήσουμε (ή να μειώσουμε) χώρο στην ταινία για να φέρουμε εις πέρας αυτήν την εργασία, καθώς οι κωδικοποιήσεις όλων των συμβόλων του αλφαβήτου ταινίας έχουν το ίδιο μήκος.

	0	1	2	3	4	⋯
ϵ	$(\epsilon, 0)$	$(\epsilon, 1)$	$(\epsilon, 2)$	$(\epsilon, 3)$	$(\epsilon, 4)$	⋯
0	$(0, 0)$	$(0, 1)$	$(0, 2)$	$(0, 3)$	$(0, 4)$	⋯
1	$(1, 0)$	$(1, 1)$	$(1, 2)$	$(1, 3)$	$(1, 4)$	⋯
00	$(00, 0)$	$(00, 1)$	$(00, 2)$	$(00, 3)$	$(00, 4)$	⋯
01	$(01, 0)$	$(01, 1)$	$(01, 2)$	$(01, 3)$	$(01, 4)$	⋯
⋮	⋮	⋮	⋮	⋮	⋮	⋱

Σχήμα 1.4.2: *Η σειρά με την οποία επιστρέφει η* np *τα ζευγάρια του* $\{0,1\}^* \times \mathbb{N}$.

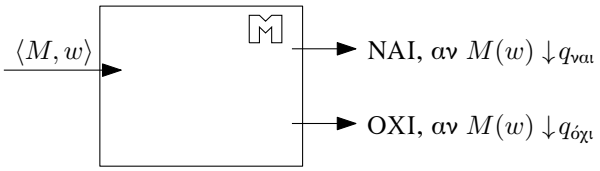
(γ΄) κινεί την κεφαλή της $1^{\eta\varsigma}$ ταινίας είτε στο προηγούμενο σύμβολο της $1^{\eta\varsigma}$ ταινίας (όχι κατ' ανάγκη στο προηγούμενο κελί) είτε στο επόμενο, ανάλογα μα το αν η μετάβαση είχε Α ή Δ.

- Αν δεν βρει τέτοιο συνδυασμό και η κατάσταση της $3^{\eta\varsigma}$ ταινίας είναι τερματική, πάει στην $q_{\text{ναι}}$ αν η 3^{η} ταινία περιέχει την $\langle q_{\text{ναι}} \rangle$ και στην $q_{\text{όχι}}$ αν περιέχει την $\langle q_{\text{όχι}} \rangle$. Σε αντίθετη περίπτωση κολλάει.

4. Γυρίζει τις κεφαλές της $2^{\eta\varsigma}$ και $3^{\eta\varsigma}$ ταινίας στο $\triangleright$.

Συμβολισμός 1.4.15 (Κουτάκια συνέχεια...).

7. Έστω TM M και $w \in \Sigma^*$. Θα γράφουμε:

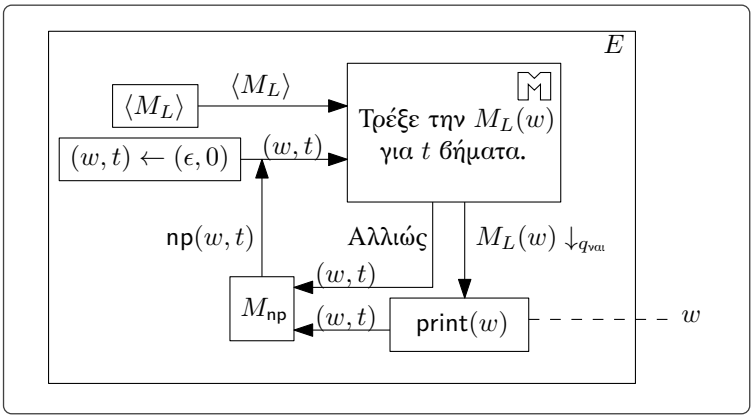


Εφαρμογή Καθολικής Μηχανής Turing

Μπορούμε να χρησιμοποιήσουμε την καθολική TM (ή παραλλαγές αυτής) για να κάνουμε διάφορους ελέγχους όσον αφορά τον υπολογισμό μίας TM M με κάποια είσοδο w. Για παράδειγμα μπορούμε να ελέγξουμε σε πόσα βήματα η $M(w)$ θα τερματίσει (εφόσον τερματίσει) ή να τρέξουμε την $M(w)$ για κάποιο συγκεκριμένο αριθμό βημάτων t και να ελέγξουμε αν θα τερματίσει σε το πολύ t βήματα. Σε αυτήν την περίπτωση θα αναφέρουμε τον έλεγχο που κάνει η $\boxed{M}$ μέσα στο «κουτάκι» της.

Σύμβαση 1.4.16. Όπως φαίνεται στον Συμβολισμό 1.4.15, χάριν απλότητας θα γράφουμε ότι η είσοδος της $\boxed{M}$ είναι πάντα κωδικοποίηση TM και λέξης. Αν θέλουμε να είμαστε πιο τυπικοί η $\boxed{M}$ θα πρέπει πρώτα να ελέγξει ότι η είσοδός της έχει αυτήν τη μορφή.

Ορισμός 1.4.17. Θεωρούμε τη συνάρτηση $\text{np} : \{0,1\}^* \times \mathbb{N} \to \{0,1\}^* \times \mathbb{N}$ που επιστρέφει το επόμενο ζευγάρι λέξης και φυσικού αριθμού σύμφωνα με τον πίνακα του Σχήματος 1.4.2.



Σχήμα 1.4.3: *Ο απαριθμητής E που απαριθμεί την L όταν η ΤΜ M_L την ημι-αποφασίζει.*

Παρατήρηση 1.4.18. Η np είναι υπολογίσιμη, έστω από την ΤΜ M_{np} (Άσκηση 1.5).

Ένα παράδειγμα εφαρμογής της Μ είναι η απόδειξη της κατεύθυνσης ($\Rightarrow$) του Θεωρήματος 1.2.46.

Απόδειξη Θεωρήματος 1.2.46. ($\Rightarrow$) Έστω M_L η ΤΜ που ημι-αποφασίζει την L και M_{np} η ΤΜ της Παρατήρησης 1.4.18. Κατασκευάζουμε [1] τον απαριθμητή E του Σχήματος 1.4.3 και παρατηρούμε ότι:

- Για κάθε λέξη $x \in L$ υπάρχει $t_x \in \mathbb{N}$ τέτοιο ώστε $M_L(x) \downarrow^{t_x}_{q_{\text{ναι}}}$. Το ζευγάρι (w, t) κάποια στιγμή θα γίνει (x, t_x), άρα ο έλεγχος της Μ θα είναι τελικά επιτυχής για την x και ο E θα την τυπώσει.

- Έστω $x \notin L$. Αφού ο E τυπώνει μόνο λέξεις που αποδέχεται η M_L (και η M_L αναγνωρίζει την L), ο E δεν θα τυπώσει ποτέ την x.

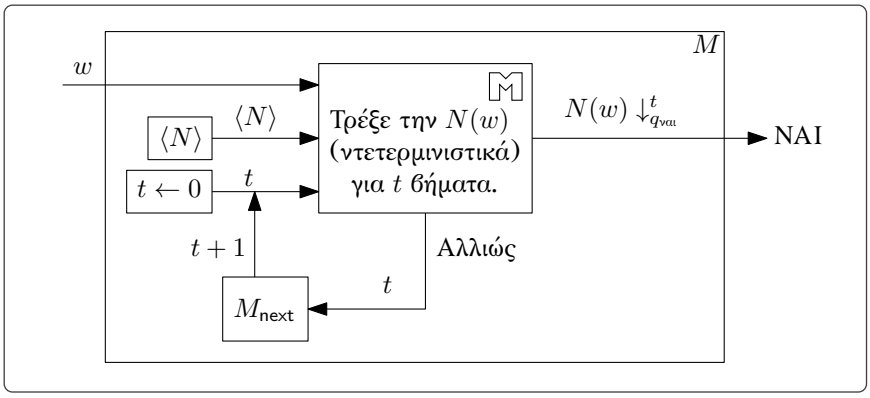
Συνεπώς ο E απαριθμεί την L. □

Μια άλλη εφαρμογή της Μ είναι η απόδειξη της ισοδυναμίας μη-ντετερμινιστικών και ντετερμινιστικών ΤΜ. Παρατηρήστε ότι για να κωδικοποιήσουμε μία μη-ντετερμινιστική ΤΜ μπορούμε να ακολουθήσουμε ακριβώς τα βήματα που κάναμε για τις ντετερμινιστικές ΤΜ.

Απόδειξη Θεωρήματος 1.3.14. [2] Έστω ΝΤΜ $N = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{ναι}}, q_{\text{όχι}})$. Η ΤΜ M του Σχήματος 1.4.4 αναγνωρίζει την $L(N)$. Στην «προσομοίωση» της N με την καθολική μηχανή

[1] Ο όρος «κατασκευάζουμε» εδώ είναι ιδιαίτερα παραπλανητικός. Για να κατασκευάσουμε τον E πρέπει πρώτα να έχουμε στα χέρια μας την M_L. Είναι προφανές ότι δοσμένης μιας αναγνωρίσιμης γλώσσας δεν υπάρχει τρόπος να κατασκευάσουμε μία ΤΜ που να την ημι-αποφασίζει (ξέρουμε ότι υπάρχει τουλάχιστον μία αλλά δεν είναι δυνατό να την κατασκευάσουμε). Ο κυριότερος όγκος των «μαθηματικών» που περιέχουν αυτές οι σημειώσεις είναι μη-κατασκευαστικά. Θα μπορούσαμε να πούμε ότι μοιάζουν περισσότερο με την *Ανάλυση* και όχι με τα *Διακριτά Μαθηματικά* (όπως θα περίμενε κάποιος σε σημειώσεις που προσπαθούν – υπό μία ερμηνεία – να οριοθετήσουν την υπολογιστική δυνατότητα των Η/Υ).

[2] Πάλι θα δείξουμε την περίπτωση όπου η ΝΤΜ ημι-αποφασίζει μία γλώσσα.



Σχήμα 1.4.4: *Η ντετερμινιστική TM που αποφασίζει την $L(N)$. Εδώ η M_{next} δέχεται ως είσοδο τη δυαδική αναπαράσταση ενός φυσικού αριθμού και επιστρέφει (τη δυαδική αναπαράσταση) του επόμενου φυσικού αριθμού (από εδώ και στο εξής θα γράφουμε πιο απλά: $t \leftarrow t+1$).*

ελέγχονται όλοι οι κλάδοι μη ντετερμινισμού [1], για ένα πεπερασμένο πλήθος βημάτων (το πολύ t) κάθε φορά. □

1.5 Κλειστότητα REC και RE

Τα ακόλουθα θεωρήματα βρίσκουν μεγάλη εφαρμογή στις προτάσεις και στις ασκήσεις αυτών των σημειώσεων.

Θεώρημα 1.5.1. Έστω $L_1, L_2 \subseteq \{0,1\}^*$.

i. Αν $L_1, L_2 \in$ REC τότε $L_1 \cap L_2 \in$ REC.

ii. Αν $L_1, L_2 \in$ RE τότε $L_1 \cap L_2 \in$ RE.

Απόδειξη. i. - ii. [2] Έστω M_1, M_2 οι TM που αποφασίζουν (ημι-αποφασίζουν) τις L_1, L_2 αντίστοιχα. Η TM M του Σχήματος 1.5.1 αποφασίζει (ημι-αποφασίζει) την $L_1 \cap L_2$. □

Θεώρημα 1.5.2. Έστω $L_1, L_2 \subseteq \{0,1\}^*$.

i. Αν $L_1, L_2 \in$ REC τότε $L_1 \cup L_2 \in$ REC.

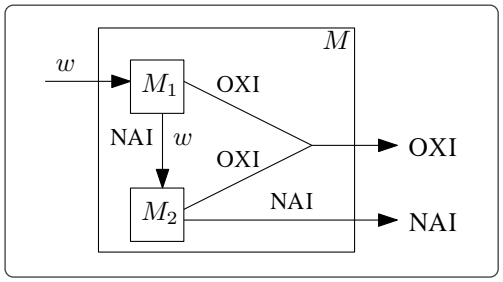
ii. Αν $L_1, L_2 \in$ RE τότε $L_1 \cup L_2 \in$ RE.

Απόδειξη. i. Έστω M_1, M_2 οι TM που αποφασίζουν τις L_1, L_2 αντίστοιχα. Η TM M του Σχήματος 1.5.2 αποφασίζει την $L_1 \cup L_2$.

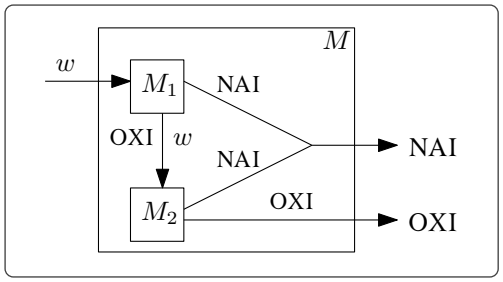
ii. Έστω M_1, M_2 οι TM που ημι-αποφασίζουν τις L_1, L_2 αντίστοιχα. Η TM M του Σχήματος 1.5.3 ημι-αποφασίζει την $L_1 \cup L_2$. □

[1] Η σειρά με την οποία ελέγχονται οι μη-ντετερμινιστικοί κλάδοι είναι μια λεπτομέρεια που δεν μας απασχολεί ιδιαίτερα. Θα την βάλουμε και αυτή «κάτω από το χαλί» όπως και τόσες άλλες.

[2] Η απόδειξη είναι ίδια και για τους δύο ισχυρισμούς.



Σχήμα 1.5.1: *Η TM M που αποφασίζει (ημι-αποφασίζει) την $L_1 \cap L_2$.*



Σχήμα 1.5.2: *Η TM M που αποφασίζει την $L_1 \cup L_2$.*

Θεώρημα 1.5.3. Έστω $L \subseteq \{0,1\}^*$. $L \in$ REC ανν $\overline{L} \in$ REC [1].

Απόδειξη. ($\Leftrightarrow$) Έστω M_L η TM που αποφασίζει την L. Η TM $M_{\overline{L}}$ του Σχήματος 1.5.4 αποφασίζει την $\overline{L}$. □

Οι αποδείξεις των ακόλουθων Θεωρημάτων αφήνονται ως άσκηση (Άσκηση 1.6).

Θεώρημα 1.5.4. Έστω $L \subseteq \{0,1\}^*$. Αν $L \in$ RE και $\overline{L} \in$ RE τότε $L \in$ REC .

Θεώρημα 1.5.5. Έστω $L_1, L_2 \subseteq \{0,1\}^*$.

i. Αν $L_1, L_2 \in$ REC τότε $L_1 L_2 \in$ REC.

ii. Αν $L_1, L_2 \in$ RE τότε $L_1 L_2 \in$ RE.

Θεώρημα 1.5.6. Έστω $L \subseteq \{0,1\}^*$.

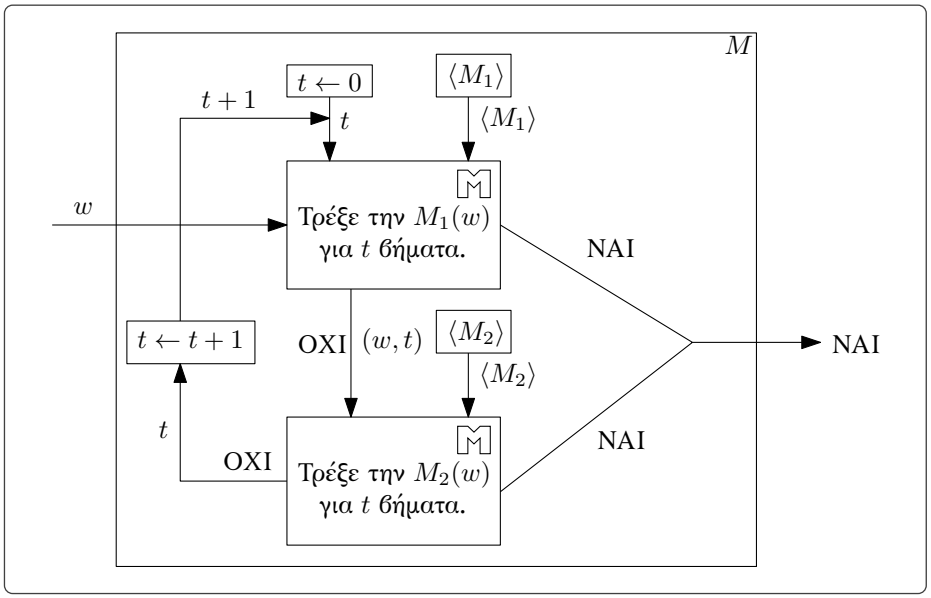
i. Αν $L \in$ REC τότε $L^* \in$ REC.

ii. Αν $L \in$ RE τότε $L^* \in$ RE.

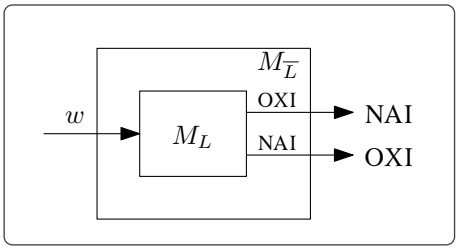
Θεώρημα 1.5.7. Έστω $L \subseteq \{0,1\}^*$ και $L^R = \{w \in \{0,1\}^* \mid w^R \in L\}$.

i. Αν $L \in$ REC τότε $L^R \in$ REC.

[1] Ένα ενδιαφέρον ερώτημα είναι το αν ισχύει το ίδιο και για το RE, δηλαδή $L \in$ RE ανν $\overline{L} \in$ RE. Θα δούμε στη συνέχεια ότι αυτό ισχύει μόνο αν $L \in$ REC.



Σχήμα 1.5.3: *Η TM M που ημι-αποφασίζει την $L_1 \cup L_2$.*



Σχήμα 1.5.4: *Η TM $M_{\overline{L}}$ που αποφασίζει την $\overline{L}$.*

ii. Αν $L \in \mathsf{RE}$ τότε $L^R \in \mathsf{RE}$.

Θεώρημα 1.5.8. Έστω $L \subseteq \{0,1\}^*$ και $L^p = \{w \in L \mid w = w^R\}$.

i. Αν $L \in \mathsf{REC}$ τότε $L^p \in \mathsf{REC}$.

ii. Αν $L \in \mathsf{RE}$ τότε $L^p \in \mathsf{RE}$.

Ασκήσεις

1.1 (☆☆☆). Αποδείξτε την Πρόταση 1.2.39.

1.2 (★☆☆). Θεωρήστε TM που πέρα από τις κατεύθυνσης αριστερά και δεξιά η

κεφαλή μπορεί να μείνει και στάσιμη σε ένα βήμα υπολογισμού. Δείξτε ότι για κάθε TM με αυτή την περιγραφή υπάρχει ισοδύναμη μονοταινιακή TM.

1.3 (★★☆). Θεωρήστε TM που η ταινία τους είναι άπειρη και από τις δύο πλευρές, δεν υπάρχει το μαξιλαράκι και φυσικά δεν υπάρχει ο περιορισμός ότι δεν μπορούμε να κινηθούμε αριστερότερα από αυτό. Δείξτε ότι για κάθε TM με αυτή την περιγραφή υπάρχει ισοδύναμη μονοταινιακή TM.

1.4 (☆☆☆). Αποδείξτε την Πρόταση 1.4.11.

1.5 (☆☆☆). Αποδείξτε την Παρατήρηση 1.4.18.

1.6 (★☆☆). Αποδείξτε τα Θεωρήματα 1.5.4, 1.5.5, 1.5.6, 1.5.7 και 1.5.8.

1.7 (★☆☆). Έστω $f : \{0,1\}^* \to \{0,1\}^*$ 1-1, επί, υπολογίσιμη συνάρτηση. Δείξτε ότι η f^{-1} είναι υπολογίσιμη.

1.8 (★☆☆). Έστω $f : \{0,1\}^* \to \{0,1\}^*$ υπολογίσιμη συνάρτηση. Κατασκευάστε απαριθμητή που απαριθμεί το σύνολο $\mathsf{dom}(f)$.

1.9 (★☆☆). Έστω $L \in \{0,1\}^*$. Δείξτε ότι $L \in \mathsf{RE}$ αν και μόνο αν $L = \{x \in \{0,1\}^* \mid \exists y \in \{0,1\}^*(\langle x, y\rangle \in B)\}$, όπου $B \in \mathsf{REC}$.

1.10 (★★☆). Θεωρήστε τη γλώσσα:

$$L = \{\langle M\rangle \in \{0,1\}^* \mid \text{Υπάρχει λέξη } w \in \{0,1\}^* \text{ για την οποία η } M(w) \text{ τερματίζει σε το πολύ } |\langle M\rangle| \text{-βήματα}\}$$

Δείξτε ότι $L \in \mathsf{REC}$.

1.11 (★★☆). Δείξτε ότι:

1. Κάθε άπειρη αναδρομική γλώσσα είναι η ξένη ένωση δύο άπειρων αναδρομικών γλωσσών.
2. Κάθε άπειρη αναδρομικά απαριθμήσιμη γλώσσα είναι η ξένη ένωση δύο άπειρων αναδρομικά απαριθμήσιμων γλωσσών.

1.12 (★★☆). Έστω $A, B, C \subseteq \{0,1\}^*$. Λέμε ότι η C *διαχωρίζει* τις A και B αν $A \subseteq C$ και $B \subseteq \overline{C}$.

1. Βρείτε $A, B \in \mathsf{RE}$ με $A \cap B = \varnothing$ για τις οποίες δεν υπάρχει $C \in \mathsf{REC}$ που τις διαχωρίζει.

2. Έστω $A, B \subseteq \{0,1\}^*$ με $A \cap B = \varnothing$ και $\overline{A}, \overline{B} \in \mathsf{RE}$. Δείξτε ότι υπάρχει $C \in \mathsf{REC}$ που τις διαχωρίζει.

1.13 (★☆☆). Θεωρήστε τη γλώσσα:

$$L = \{\langle M, w, n\rangle \in \{0,1\}^* \mid n \geq 1 \text{ και κατά τον υπολογισμό } M(w) \text{ η κεφαλή επισκέπτεται τη } n\text{-οστή θέση της ταινίας}\}$$

Δείξτε ότι $L \in \mathsf{REC}$.

1.14 (★★★). Δείξτε ότι αν ένα σύνολο $A \subseteq \mathcal{G}$ δεν περιέχει κωδικοποιήσεις ισοδύναμων TM και είναι αναδρομικά απαριθμήσιμο, τότε υπάρχει $B \subseteq \mathcal{G}$ τέτοιο ώστε:

- για κάθε $\langle M\rangle \in A$ υπάρχει μοναδική TM M' ισοδύναμη της M με $\langle M'\rangle \in B$,
- η B είναι αναδρομική γλώσσα.

1.15 (★★★). Δείξτε ότι υπάρχουν άπειρες το πλήθος αναδρομικά απαριθμήσιμες γλώσσες $L \subseteq \Sigma^*$ τέτοιες ώστε η $\bar{L}$ να είναι άπειρη γλώσσα αλλά κάθε αναδρομικά απαριθμήσιμο υποσύνολο της $\bar{L}$ να είναι πεπερασμένο.

1.16 (★★☆). Θεωρήστε τα σύνολα

$$K = \{w \in \{0,1\}^* \mid w \text{ δυαδική αναπαράσταση του αριθμού } n \text{ και } M_n(w)\downarrow\}$$
$$R = \{w \in \{0,1\}^* \mid w \text{ δυαδική αναπαράσταση του αριθμού } n \text{ και } \mathsf{dom}(\phi_{M_n}) \in \mathsf{REC}\}$$

όπου με M_n συμβολίζουμε την TM με αριθμό Gödel n και με ϕ_{M_n} τη συνάρτηση που υπολογίζει η M_n (δες Ορισμό 1.2.13). Εξετάστε αν ισχύουν τα ακόλουθα:

1. $R \subseteq K$.
2. $R \cap K = \varnothing$.
3. Υπάρχει 1-1 και επί συνάρτηση $f : K \to \overline{K}$.

1.17 (★☆☆). Δείξτε ότι η συνάρτηση $f : \{0,1\}^* \to \{0,1\}^*$ με:

$$f(x) = \begin{cases} 1 \text{ , αν } x \text{ δυαδική αναπαράσταση του αριθμού } n \text{ και υπάρχει } w \in \{0,1\}^* \\ \quad \text{τέτοιο ώστε } M_n(w)\downarrow \\ \perp \text{ , αλλιώς} \end{cases}$$

όπου M_n είναι η TM με αριθμό Gödel n, είναι υπολογίσιμη.

1.18 (★☆☆). Δείξτε ότι η συνάρτηση $f : \{0,1\}^* \to \{0,1\}^*$ με:

$$f(x) = \begin{cases} x \text{ , αν } x \text{ δυαδική αναπαράσταση του αριθμού } n \text{ και } |L(M_n)| \geq n \\ \perp \text{ , αλλιώς} \end{cases}$$

όπου M_n είναι η TM με αριθμό Gödel n, είναι υπολογίσιμη.

1.19 (★☆☆). Έστω $f : \{0,1\}^* \to \{0,1\}^*$ η οποία είναι υπολογίσιμη και φθίνουσα (ως προς τη λεξικογραφική διάταξη του $\{0,1\}$) στο $\mathsf{dom}(f)$. Δείξτε ότι $\mathsf{im}(f) \in \mathsf{REC}$. Επιπλέον δείξτε ότι για κάθε γλώσσα $L \subseteq \{0,1\}^*$, ισχύει ότι $f(L) \in \mathsf{REC}$.

ΚΕΦΑΛΑΙΟ 2

ΑΝΑΔΡΟΜΙΚΕΣ ΣΥΝΑΡΤΗΣΕΙΣ

Σε αυτό το κεφάλαιο θα ασχοληθούμε αποκλειστικά με συναρτήσεις φυσικών αριθμών. Σύμφωνα με την Παρατήρηση 1.2.16 μπορούμε να θεωρήσουμε ότι τα «αντικείμενα του υπολογισμού» είναι οι λέξεις του $\{0,1\}^*$. Μπορούμε περαιτέρω να αντιστοιχίσουμε κάθε λέξη $w \in \{0,1\}^*$ σε έναν φυσικό αριθμό (για παράδειγμα στον αριθμό που αντιστοιχεί στη «σειρά» εμφάνισης της w στη λεξικογραφική διάταξη) και έτσι να υποθέσουμε ότι τα «αντικείμενα υπολογισμού» είναι οι φυσικοί αριθμοί, οπότε οι γλώσσες του $2^{\{0,1\}^*}$ θα αποτελούν στην ουσία σύνολα φυσικών αριθμών και οι συναρτήσεις από το $\{0,1\}^*$ στο $\{0,1\}^*$ θα είναι αριθμητικές συναρτήσεις από το $\mathbb{N}$ στο $\mathbb{N}$. Πηγαίνοντας τον συλογισμό ένα βήμα παραπέρα (και χρησιμοποιώντας τον Ορισμό 1.2.13) μπορούμε να αφοσιωθούμε μόνο στον υπολογισμός συναρτήσεων φυσικών αριθμών.

Στόχος μας είναι να κατατάξουμε (μερικές από) τις αριθμητικές συναρτήσεις σε δύο κλάσεις, σύμφωνα με τον «τρόπο που ορίζονται»: τις *πρωτογενώς αναδρομικές* συναρτήσεις και τις *ελαχιστικά αναδρομικές* συναρτήσεις. Η δεύτερη και γενικότερη κλάση ταυτίζεται με την κλάση των υπολογίσιμων (κατά Turing) συναρτήσεων που είδαμε στο προηγούμενο κεφάλαιο.

Θα δούμε λοιπόν έναν δεύτερο – και εντελώς ανεξάρτητο από τον πρώτο – ορισμό των υπολογίσιμων συναρτήσεων. Αυτό όπως είναι φυσικό μας οδηγεί σε μια δεύτερη προσέγγιση της έννοιας του αλγορίθμου, που σε αντίθεση με τις TM δεν έχει μηχανιστική υφή: *Ο αλγόριθμος που υπολογίζει μία πρωτογενώς ή ελαχιστικά αναδρομική συνάρτηση είναι ο ίδιος ο τρόπος ορισμού της* [1]*!*

Πέρα από την παρουσίαση ενός διαφορετικού φορμαλισμού της Θεωρίας Αναδρομής, θέλουμε να καλλιεργήσουμε στον αναγνώστη την προδιάθεση ότι η *Θέση Church-Turing* (σελίδα 115) αποτελεί μία εύλογη παραδοχή. Μόνον εφόσον πεισθούμε ότι η Θέση Church-Turing μας δίνει μία επαρκή προσέγγιση της έννοιας του Αλγορίθμου, θα μπορέσουμε να

[1] Αυτό δεν θα έπρεπε να σας φανεί περίεργο καθώς αυτό ακριβώς κάνουν οι συναρτησιακές γλώσσες προγραμματισμού.

προχωρήσουμε στη θεωρία μας και τελικά να διαπιστώσουμε τα όρια της *Αλγοριθμικής Υπολογισιμότητας*.

2.1 Πρωτογενώς αναδρομικές συναρτήσεις

Ορισμός 2.1.1. Μία συνάρτηση $f : \mathbb{N}^m \to \mathbb{N}$, $m \geq 1$ είναι *πρωτογενώς αναδρομική* ανν είναι μία εκ των

(a) $\mathsf{s}(x) = x + 1$ (η *συνάρτηση του επόμενου*) [1]

(b) $\mathsf{z}^m(x_1, \dots, x_m) = 0$ (η *σταθερή συνάρτηση ίση με μηδέν* m μεταβλητών)

(c) $\mathsf{p}_i^m(x_1, \dots, x_m) = x_i$, όπου $i \in [m]$ (η *προβολή στην* i*-οστή μεταβλητή*) [2]

ή προκύπτει από τις πρωτογενώς αναδρομικές συναρτήσεις

(1) $\mathsf{g} : \mathbb{N}^n \to \mathbb{N}$ και $\mathsf{h}_i : \mathbb{N}^m \to \mathbb{N}$, $i \in [n]$ ως εξής:

$$f(x_1, \dots, x_m) = \mathsf{g}(\mathsf{h}_1(x_1, \dots, x_m), \dots, \mathsf{h}_n(x_1, \dots, x_m))$$

(*σύνθεση της* g *με τις* $\mathsf{h}_i,\ i \in [n]$)

(2) $\mathsf{g} : \mathbb{N}^{m-1} \to \mathbb{N}$ και $\mathsf{h} : \mathbb{N}^{m+1} \to \mathbb{N}$ όντας λύση των εξισώσεων [3]:

$$\begin{cases} f(0, x_1, \dots, x_{m-1}) = \mathsf{g}(x_1, \dots, x_{m-1}) \\ f(y+1, x_1, \dots, x_{m-1}) = \mathsf{h}(f(y, x_1, \dots, x_{m-1}), y, x_1, \dots, x_{m-1}) \end{cases}$$

(*πρωτογενής αναδρομή* [4])

Ο Ορισμός 2.1.1 θα γίνει περισσότερο κατανοητός μέσα από τα παραδείγματα που ακολουθούν.

Παράδειγμα 2.1.2. Οι σταθερές συναρτήσεις $\mathsf{c}_q^m : \mathbb{N}^m \to \mathbb{N}$, με $\mathsf{c}_q^m(x_1, \dots, x_m) = q$, όπου $q \in \mathbb{N}$, είναι πρωτογενώς αναδρομικές καθώς:

$$\mathsf{c}_q^m(x_1, \dots, x_m) = \underbrace{\mathsf{s}(\mathsf{s}(\cdots \mathsf{s}}_{q\text{-φορές}}(\mathsf{z}^m(x_1, \dots, x_m))\cdots))$$

Εδώ θα πρέπει να τονίσουμε κάτι που ίσως έχει ήδη αρχίσει να διαφαίνεται: *Σε αυτό το κεφάλαιο θα δεωρούμε ότι όλα είναι συναρτήσεις, ακόμα και οι φυσικοί αριθμοί!*

[1] Φυσικά $f = \mathsf{s}$ μόνο αν $m = 1$.

[2] Τα (b) και (c) (μαζί με ένα πεπερασμένο πλήθος «εφαρμογών» του (a), δες Παράδειγμα 2.1.2) αντιστοιχούν στις *εντολές ανάδεσης* μίας γλώσσας προγραμματισμού.

[3] Προφανώς ο ορισμός αυτός ισχύει μόνο για $m > 1$. Για $m = 1$ δες την Πρόταση 2.1.7.

[4] Η πρωτογενής αναδρομή αντιστοιχεί στο *for-loop* μίας γλώσσας προγραμματισμού.

Παράδειγμα 2.1.3. Οι συναρτήσεις $h : \mathbb{N}^3 \to \mathbb{N}$, με $\mathsf{h}(x, y, z) = x + 1$, και $\mathsf{plus} : \mathbb{N}^2 \to \mathbb{N}$, με $\mathsf{plus}(x, y) = x + y$, είναι πρωτογενώς αναδρομικές καθώς:

$$\mathsf{h}(x, y, z) = \mathsf{s}(\mathsf{p}_1^3(x, y, z))$$

και η plus αποτελεί λύση των εξισώσεων:

$$\begin{cases} f(0, y) = \mathsf{p}_1^1(y) & [= y\ ] \\ f(x + 1, y) = \mathsf{h}(f(x, y), x, y) & [= f(x, y) + 1\ ] \end{cases}$$

Για να το δείξουμε αυτό θα δείξουμε ότι για κάθε $(x, y) \in \mathbb{N}^2$ ισχύει ότι $f(x, y) = \mathsf{plus}(x, y)$ κάνοντας επαγωγή ως προς την πρώτη μεταβλητή [1]. Παρατηρούμε ότι για κάθε $y \in \mathbb{N}$:

Επαγωγική Βάση: Για $x = 0$ ισχύει ότι $f(0, y) = \mathsf{p}_1^1(y) = y = \mathsf{plus}(0, y)$.

Επαγωγική Υπόθεση: Υποθέτουμε ότι $f(x, y) = \mathsf{plus}(x, y)$.

Επαγωγικό Βήμα: Θα δείξουμε ότι $f(x + 1, y) = \mathsf{plus}(x + 1, y)$. Παρατηρούμε ότι:

$$\begin{aligned} f(x+1, y) &= \mathsf{h}(f(x, y), x, y) \\ &= f(x, y) + 1 \\ &= \mathsf{plus}(x, y) + 1 \quad \text{(Λόγω της Επαγωγικής Υπόθεσης)} \\ &= x + y + 1 \\ &= \mathsf{plus}(x + 1, y) \end{aligned}$$

Παράδειγμα 2.1.4. Η συνάρτηση $\mathsf{mult} : \mathbb{N}^2 \to \mathbb{N}$, με $\mathsf{mult}(x, y) = x \cdot y$, είναι πρωτογενώς αναδρομική καθώς αποτελεί λύση των εξισώσεων:

$$\begin{cases} f(0, y) = \mathsf{z}^1(y) & [= 0\ ] \\ f(x + 1, y) = \mathsf{plus}(\mathsf{p}_1^3(f(x, y), x, y), \mathsf{p}_3^3(f(x, y), x, y)) & [= f(x, y) + y\ ] \end{cases}$$

όπου plus η συνάρτηση του Παραδείγματος 2.1.3.

Είναι η κατάλληλη ώρα να αποδείξουμε μερικές προτάσεις που θα μας διευκολύνουν στον ορισμό πρωτογενών αναδρομικών συναρτήσεων.

Πρόταση 2.1.5. Έστω πρωτογενώς αναδρομικές συναρτήσεις $\mathsf{g} : \mathbb{N}^n \to \mathbb{N}$, $n \geq 1$, και $\mathsf{h}_i : \mathbb{N}^m \to \mathbb{N}$, $m \geq 1$, όπου $i \in [n - 1]$. Η συνάρτηση $f : \mathbb{N}^m \to \mathbb{N}$, με:

$$f(x_1, \ldots, x_m) = \mathsf{g}(\mathsf{h}_1(x_1, \ldots, x_m), \ldots, \mathsf{h}_{n-1}(x_1, \ldots, x_m), y)$$

όπου $y \in \{x_1, \ldots, x_m\}$, είναι πρωτογενώς αναδρομική.

[1] Στα παραδείγματα που ακολουθούν θα αποφύγουμε τις αποδείξεις με επαγωγή καθώς, όπως θα δείτε, δεν παρουσιάζουν μεγάλο ενδιαφέρον.

Απόδειξη. Έστω $y = x_i$. Παρατηρούμε ότι:

$$f(x_1, \dots, x_m) = \mathsf{g}(\mathsf{h}_1(x_1, \dots, x_m), \dots, \mathsf{h}_{n-1}(x_1, \dots, x_m), \mathsf{p}_i^m(x_1, \dots, x_m))$$

Άρα η f είναι πρωτογενώς αναδρομική. □

Η Πρόταση 2.1.5 μπορεί να γενικευτεί άμεσα (ποικιλοτρόπως) δίνοντάς μας το δικαίωμα να ορίζουμε πρωτογενώς αναδρομικές συναρτήσεις εφαρμόζοντας σύνθεση μόνο σε μερικές (ή και καμία) από τις μεταβλητές.Ένα παράδειγμα εφαρμογής της είναι το Παράδειγμα 2.1.4 όπου θα μπορούσαμε να αντικαταστήσουμε το $\mathsf{plus}(\mathsf{p}_1^3(f(x,y),x,y),\ \mathsf{p}_3^3(f(x,y),x,y))$ με $\mathsf{plus}(f(x,y),y)$ στην αναδρομική εξίσωση.

Πρόταση 2.1.6. Έστω πρωτογενώς αναδρομική συνάρτηση $\mathsf{g} : \mathbb{N}^n \to \mathbb{N}$, $n \geq 1$. Η συνάρτηση $f : \mathbb{N}^m \to \mathbb{N}$, $m \geq 1$, με $f(x_1, \dots, x_m) = \mathsf{g}(y_1, \dots, y_n)$, όπου $y_i \in \{x_1, \dots, x_m\}$, $i \in [n]$, είναι πρωτογενώς αναδρομική.

Απόδειξη. Έστω $y_j = x_{i_j}$, $j \in [n]$. Παρατηρούμε ότι:

$$f(x_1, \dots, x_m) = \mathsf{g}(\mathsf{p}_{i_1}^m(x_1, \dots, x_m), \dots, \mathsf{p}_{i_n}^m(x_1, \dots, x_m))$$

Άρα η f είναι πρωτογενώς αναδρομική. □

Σύμφωνα με την Πρόταση 2.1.6 μπορούμε να αντιμεταθέσουμε, να αφαιρέσουμε, ή να επαναλάβουμε μεταβλητές όταν κατασκευάζουμε πρωτογενώς αναδρομικές συναρτήσεις [1]. Για παράδειγμα, στο Παράδειγμα 2.1.3 ορίσαμε τη συνάρτηση $\mathsf{h} : \mathbb{N}^3 \to \mathbb{N}$ που ταυτίζεται με τη συνάρτηση του επομένου στην πρώτη μεταβλητή, θα μπορούσαμε χάριν συντομίας να γράψουμε $\mathsf{h}(x,y,z) = \mathsf{s}(x)$.

Πρόταση 2.1.7. Έστω $\mathsf{h} : \mathbb{N}^2 \to \mathbb{N}$ πρωτογενώς αναδρομική συνάρτηση και $q \in \mathbb{N}$. Η συνάρτηση $f : \mathbb{N} \to \mathbb{N}$ που αποτελεί λύση των εξισώσεων:

$$\begin{cases} f(0) = q \\ f(y+1) = \mathsf{h}(f(y), y) \end{cases} \quad (\textit{πρωτογενής αναδρομή χωρίς παραμέτρους})$$

είναι πρωτογενώς αναδρομική.

Απόδειξη. Η συνάρτηση $g : \mathbb{N}^2 \to \mathbb{N}$ που αποτελεί λύση των εξισώσεων:

$$\begin{cases} g(0,x) = \mathsf{c}_q^1(x) & [\, = q \,] \\ g(y+1,x) = \mathsf{p}_1^3(\mathsf{h}(g(y,x),y),y,x) & [\, = \mathsf{h}(g(y,x),y) \,] \end{cases}$$

όπου c_q^1 η συνάρτηση του Παραδείγματος 2.1.2, είναι πρωτογενώς αναδρομική. Παρατηρούμε ότι $f(y) = g(y,y)$ [2], οπότε, σύμφωνα με την Πρόταση 2.1.6, η f είναι πρωτογενώς αναδρομική. □

[1] Παρατηρήστε ότι για τα n και m στην Πρόταση 2.1.6 μπορεί να ισχύει $n \leq m$ ή $m < n$.

[2] Αν θέλουμε να το δείξουμε αυτό με επαγωγή μπορούμε να δείξουμε ότι $f(y) = g(y,x)$ για κάθε $x \in \mathbb{N}$, άρα και για $x = y$.

Η Πρόταση 2.1.7 συμπληρώνει τον ορισμό της πρωτογενής αναδρομής και μας δίνει το δικαίωμα να την εφαρμόζουμε για να ορίζουμε ακόμα και συναρτήσεις μίας μεταβλητής.

Παράδειγμα 2.1.8. Η συνάρτηση $\mathsf{fact} : \mathbb{N} \to \mathbb{N}$, με $\mathsf{fact}(x) = x!$, είναι πρωτογενώς αναδρομική, σύμφωνα με την Πρόταση 2.1.7, καθώς αποτελεί λύση των εξισώσεων:

$$\begin{cases} f(0) = 1 \\ f(x+1) = \mathsf{mult}(f(x), \mathsf{s}(x)) & [= f(x) \cdot (x+1)\ ] \end{cases}$$

όπου mult η συνάρτηση του Παραδείγματος 2.1.4.

Παράδειγμα 2.1.9. Η συνάρτηση $\mathsf{pd} : \mathbb{N} \to \mathbb{N}$, με:

$$\mathsf{pd}(x) = \begin{cases} 0 & ,\ \text{αν } x = 0 \\ x - 1 & ,\ \text{αλλιώς} \end{cases}$$

είναι πρωτογενώς αναδρομική, σύμφωνα με την Πρόταση 2.1.7, καθώς αποτελεί λύση των εξισώσεων:

$$\begin{cases} f(0) = 0 \\ f(x+1) = \mathsf{p}_2^2(f(x), x) & [= x\ ] \end{cases}$$

Παράδειγμα 2.1.10. Η συνάρτηση $\dot{-} : \mathbb{N}^2 \to \mathbb{N}$, με:

$$\dot{-}(x, y) = \begin{cases} 0 & ,\ \text{αν } x < y \\ x - y & ,\ \text{αλλιώς} \end{cases}$$

είναι πρωτογενώς αναδρομική καθώς αποτελεί λύση των εξισώσεων:

$$\begin{cases} f(x, 0) = \mathsf{p}_1^1(x) & [= x\ ] \\ f(x, y+1) = \mathsf{pd}(f(x, y))\ ^{1} & [= f(x, y) - 1\ ] \end{cases}$$

όπου pd η συνάρτηση του Παραδείγματος 2.1.9. Εδώ κάναμε την πρώτη μας «παρατυπία» (για αυτό το κεφάλαιο): Σύμφωνα με τον Ορισμό 2.1.1 η πρωτογενής αναδρομή γίνεται στην πρώτη μεταβλητή ενώ εδώ την εφαρμόσαμε στη δεύτερη. Αυτό μπορεί να επιτευχθεί λόγω της Πρότασης 2.1.6, ορίζοντας την $f : \mathbb{N}^2 \to \mathbb{N}$ που αποτελεί λύση των εξισώσεων:

$$\begin{cases} f(0, y) = \mathsf{p}_1^1(y) \\ f(x+1, y) = \mathsf{pd}(f(x, y)) \end{cases}$$

και έπειτα ορίζοντας $\dot{-}(x, y) = f(y, x)$ [2]. Για λόγους «αισθητικής» θα γράφουμε $x \dot{-} y$ αντί για $\dot{-}(x, y)$.

[1] Η Πρόταση 2.1.6 μας δίνει το δικαίωμα να το γράψουμε σε αυτήν τη μορφή.Τυπικά θα έπρεπε να γράψουμε: $f(x, y+1) = \mathsf{pd}(\mathsf{p}_1^3(f(x, y), x, y))$.

[2] Με άλλα λόγια ορίσαμε τη συνάρτηση $\dot{-}'(x, y) = \begin{cases} 0 & ,\ \text{αν } y < x \\ y - x & ,\ \text{αλλιώς} \end{cases}$ και απλά αντιστρέψαμε τη σειρά των ορισμάτων της.

Παράδειγμα 2.1.11. Η συνάρτηση $\mathsf{min} : \mathbb{N}^2 \to \mathbb{N}$, με $\mathsf{min}(x, y) = \mathsf{min}\{x, y\}$, είναι πρωτογενώς αναδρομική καθώς:

$$\mathsf{min}(x, y) = x \dot{-} (x \dot{-} y)$$

όπου $\dot{-}$ η συνάρτηση του Παραδείγματος 2.1.10.

Παράδειγμα 2.1.12. Η συνάρτηση $\mathsf{max} : \mathbb{N}^2 \to \mathbb{N}$, με $\mathsf{max}(x, y) = \mathsf{max}\{x, y\}$, είναι πρωτογενώς αναδρομική καθώς:

$$\mathsf{max}(x, y) = \mathsf{plus}(x, y) \dot{-} \mathsf{min}(x, y)$$

όπου $\mathsf{plus}, \dot{-}$ και min οι συναρτήσεις των Παραδειγμάτων 2.1.3, 2.1.10 και 2.1.11.

Παρατήρηση 2.1.13. Οι συναρτήσεις min και max γενικεύονται άμεσα σε συναρτήσεις m μεταβλητών, για κάθε $m \in \mathbb{N}$ (δες Άσκηση 2.3).

Παράδειγμα 2.1.14. Η συνάρτηση $\mathsf{exp} : \mathbb{N}^2 \to \mathbb{N}$, με $\mathsf{exp}(x, y) = x^y$, είναι πρωτογενώς αναδρομική καθώς αποτελεί λύση των εξισώσεων:

$$\begin{cases} f(x, 0) = \mathsf{c}_1^1(x) & [= 1\,] \\ f(x, y+1) = \mathsf{mult}(f(x, y), x) & [= f(x, y) \cdot x\,] \end{cases}$$

όπου c_1^1 και mult οι συναρτήσεις των Παραδειγμάτων 2.1.2 και 2.1.4.

Μπορούμε να μεταφέρουμε τον Ορισμό 2.1.1 και σε υποσύνολα του $\mathbb{N}^m$, για $m \geq 1$, ορίζοντας έτσι *πρωτογενώς αναδρομικές σχέσεις* φυσικών αριθμών.

Ορισμός 2.1.15. Μία σχέση $P \subseteq \mathbb{N}^m$, $m \geq 1$, είναι *πρωτογενώς αναδρομική* ανν η χαρακτηριστική της συνάρτηση $\chi_P : \mathbb{N}^m \to \{0, 1\}$ είναι πρωτογενώς αναδρομική [1].

Παράδειγμα 2.1.16. Η σχέση $\{(x, y) \in \mathbb{N}^2 \mid x = y\}$ είναι πρωτογενώς αναδρομική καθώς η χαρακτηριστική της συνάρτηση είναι πρωτογενώς αναδρομική [2]:

$$\chi_=(x, y) = \mathsf{c}_1^2(x, y) \dot{-} \mathsf{plus}(x \dot{-} y, y \dot{-} x)$$

όπου c_1^2, plus και $\dot{-}$ οι συναρτήσεις των Παραδειγμάτων 2.1.2, 2.1.3 και 2.1.10.

Παρατηρήστε ότι και η σχέση $\{(x, y) \in \mathbb{N}^2 \mid x \neq y\}$ είναι πρωτογενώς αναδρομική καθώς η χαρακτηριστική της συνάρτηση είναι η:

$$\chi_{\neq}(x, y) = \mathsf{c}_1^2(x, y) \dot{-} \chi_=(x, y)$$

Παράδειγμα 2.1.17. Η σχέση $\{(x, y) \in \mathbb{N}^2 \mid x \leq y\}$ είναι πρωτογενώς αναδρομική καθώς η χαρακτηριστική της συνάρτηση είναι πρωτογενώς αναδρομική:

$$\chi_{\leq}(x, y) = \mathsf{c}_1^2(x, y) \dot{-} (x \dot{-} y)$$

όπου c_1^2 και $\dot{-}$ οι συναρτήσεις των Παραδειγμάτων 2.1.2 και 2.1.10.

[1] Θα μπορούσαμε να πούμε ότι αντιπροσωπεύουμε κάθε σύνολο (ή γενικότερα μία m-μελή σχέση) με τη χαρακτηριστική του συνάρτηση. Συνεπώς και τα σύνολα «είναι» συναρτήσεις!

[2] Μπορείτε να εντοπίσετε που εφαρμόζουμε την Πρόταση 2.1.6;

Παράδειγμα 2.1.18. Η σχέση $\{(x,y) \in \mathbb{N}^2 \mid x < y\}$ είναι πρωτογενώς αναδρομική καθώς η χαρακτηριστική της συνάρτηση είναι πρωτογενώς αναδρομική:

$$\chi_<(x,y) = \chi_\leq(\mathsf{s}(x), y)$$

όπου η $\chi_\leq$ ορίζεται στο Παράδειγμα 2.1.17.

Οι αποδείξεις των παρακάτω προτάσεων αφήνονται ως άσκηση (Άσκηση 2.5).

Πρόταση 2.1.19. Έστω πρωτογενώς αναδρομικές σχέσεις $\mathsf{P}, \mathsf{Q} \subseteq \mathbb{N}^m$. Οι σχέσεις $\overline{\mathsf{P}}$, $\mathsf{P} \cup \mathsf{Q}$, $\mathsf{P} \cap \mathsf{Q}$ και $\mathsf{P} \setminus \mathsf{Q}$ είναι πρωτογενώς αναδρομικές.

Πρόταση 2.1.20. Έστω πρωτογενώς αναδρομική σχέση $\mathsf{P} \subseteq \mathbb{N}^m$ και πρωτογενώς αναδρομικές συναρτήσεις $\mathsf{f}_i : \mathbb{N}^n \to \mathbb{N}$, $i \in [m]$. Η σχέση:

$$Q = \{(x_1, \dots, x_n) \in \mathbb{N}^n \mid (\mathsf{f}_1(x_1, \dots, x_n), \dots, \mathsf{f}_\mathsf{m}(x_1, \dots, x_n)) \in \mathsf{P}\}$$

είναι πρωτογενώς αναδρομική.

Σύμβαση 2.1.21. Από εδώ και στο εξής θα χρησιμοποιούμε τους φυσικούς αριθμούς και τα σύμβολα $+, \cdot$ αντί για τις πρωτογενώς αναδρομικές συναρτήσεις που τα ορίζουν. Επίσης, θα γράφουμε την ύψωση σε δύναμη κατά τον συνήθη τρόπο και όχι χρησιμοποιώντας τη συνάρτηση exp του Παραδείγματος 2.1.14.

Πρόταση 2.1.22. Έστω ξένες ανά δύο πρωτογενώς αναδρομικές σχέσεις $\mathsf{P}_i \subseteq \mathbb{N}^m$, $i \in [n]$, και πρωτογενώς αναδρομικές συναρτήσεις $\mathsf{g}_j : \mathbb{N}^m \to \mathbb{N}$, $j \in [n+1]$, όπου $n, m \geq 1$. Η $f : \mathbb{N}^m \to \mathbb{N}$ με:

$$f(x_1, \dots, x_m) = \begin{cases} \mathsf{g}_1(x_1, \dots, x_m) & , \text{ αν } (x_1, \dots, x_m) \in \mathsf{P}_1 \\ \mathsf{g}_2(x_1, \dots, x_m) & , \text{ αν } (x_1, \dots, x_m) \in \mathsf{P}_2 \\ \quad \vdots & \\ \mathsf{g}_n(x_1, \dots, x_m) & , \text{ αν } (x_1, \dots, x_m) \in \mathsf{P}_n \\ \mathsf{g}_{n+1}(x_1, \dots, x_m) & , \text{ αλλιώς} \end{cases}$$

είναι πρωτογενώς αναδρομική [1].

Απόδειξη. Θα αποδείξουμε την πρόταση για $n = 1$ [2]. Παρατηρούμε ότι:

$$f(x_1, \dots, x_m) = \chi_{\mathsf{P}_1}(x_1, \dots, x_m) \cdot \mathsf{g}_1(x_1, \dots, x_m) + (1 \dot{-} \chi_{\mathsf{P}_1}(x_1, \dots, x_m)) \cdot \mathsf{g}_2(x_1, \dots, x_m),$$

από τα Παραδείγματα 2.1.3 και 2.1.4 η πρόσθεση και ο πολλαπλασιασμός είναι πρωτογενώς αναδρομικές συναρτήσεις και το 1 ορίζεται ως $\mathsf{c}_1^m(x_1, \dots, x_m)$ (δες Παράδειγμα 2.1.2). □

[1] Η συνάρτηση f αντιστοιχεί στο *if-then-else* μίας γλώσσας προγραμματισμού.
[2] Η γενική περίπτωση αφήνεται ως άσκηση (Άσκηση 2.5).

Παράδειγμα 2.1.23. Η συνάρτηση $\mathsf{rm} : \mathbb{N}^2 \to \mathbb{N}$, με:

$$\mathsf{rm}(x,y) = \begin{cases} x \bmod y & , \text{ αν } y \neq 0 \\ x+1 & , \text{ αν } y = 0 \end{cases}$$

(το υπόλοιπο της διαίρεσης του x με το y [1]) είναι πρωτογενώς αναδρομική καθώς αποτελεί λύση των εξισώσεων:

$$\begin{cases} f(0,y) = \begin{cases} 0 & , \text{ αν } y \neq 0 \\ 1 & , \text{ αλλιώς } (y=0) \end{cases} \\ f(x+1,y) = \begin{cases} x+2 & , \text{ αν } y = 0 \\ 0 & , \text{ αν } f(x,y)+1 = y \\ f(x,y)+1 & , \text{ αλλιώς} \end{cases} \end{cases}$$

και οι σχέσεις $=$ και $\neq$ είναι πρωτογενώς αναδρομικές (δες Παράδειγμα 2.1.16).

Παράδειγμα 2.1.24. Η σχέση $\{(x,y) \in \mathbb{N}^2 \mid x \mid y\}$ είναι πρωτογενώς αναδρομική καθώς η χαρακτηριστική της συνάρτηση είναι πρωτογενώς αναδρομική :

$$\chi_{|}(x,y) = 1 \dot{-} \mathsf{rm}(y,x)$$

όπου $\dot{-}$ και rm οι συναρτήσεις των Παραδειγμάτων 2.1.10 και 2.1.23.

Παράδειγμα 2.1.25. Η συνάρτηση $\mathsf{qt} : \mathbb{N}^2 \to \mathbb{N}$, με:

$$\mathsf{qt}(x,y) = \begin{cases} \frac{x - x \bmod y}{y} & , \text{ αν } y \neq 0 \\ x+1 & , \text{ αν } y = 0 \end{cases}$$

(το πηλίκο της διαίρεσης του x με το y) είναι πρωτογενώς αναδρομική καθώς αποτελεί λύση των εξισώσεων:

$$\begin{cases} f(0,y) = \begin{cases} 0 & , \text{ αν } y \neq 0 \\ 1 & , \text{ αλλιώς } (y=0) \end{cases} \\ f(x+1,y) = \begin{cases} x+2 & , \text{ αν } y = 0 \\ f(x,y)+1 & , \text{ αν } \mathsf{rm}(x,y)+1 = y \\ f(x,y) & , \text{ αλλιώς} \end{cases} \end{cases}$$

όπου rm η συνάρτηση του Παραδείγματος 2.1.23.

[1] Θα αναρωτιέστε γιατί δώσαμε τιμή ακόμα και όταν έχουμε διαίρεση με το μηδέν. Ο λόγος είναι ότι σε αντίθετη περίπτωση θα ορίζαμε μερική συνάρτηση και θέλουμε οι πρωτογενώς αναδρομικές συναρτήσεις να είναι ολικές (δες Άσκηση 2.2). Θέλουμε να κρατήσουμε τη μη ύπαρξη τιμής για κάποιο όρισμα της συνάρτησης για κάτι πιο ουσιαστικό: *Να σηματοδοτεί τον μη τερματισμό κατά τον υπολογισμού της*. Επιπλέον, η σύμβαση αυτή μας δίνει το δικαίωμα να ελέγχουμε αν έχουμε διαίρεση με το μηδέν.

Παράδειγμα 2.1.26. Η συνάρτηση $\mathsf{dn} : \mathbb{N}^2 \to \mathbb{N}$, με:

$$\mathsf{dn}(x, y) = |\{d \in \mathbb{N} \mid (d \mid x) \wedge (d \leq y)\}|$$

(το πλήθος των διαιρετών του x που είναι μικρότεροι του y) είναι πρωτογενώς αναδρομική καθώς αποτελεί λύση των εξισώσεων:

$$\begin{cases} f(x, 0) = 0 \\ f(x, y+1) = f(x, y) + \chi_{|}(y+1, x) \end{cases}$$

όπου η $\chi_{|}$ ορίζεται στο Παράδειγμα 2.1.24.

Τα παραδείγματα που είδαμε δεν επιλέχθηκαν τυχαία. Όλες οι συναρτήσεις και σχέσεις που ορίσθηκαν σε αυτήν την παράγραφο ήταν απαραίτητες για να φτάσουμε στον ακόλουθο ορισμό.

Παράδειγμα 2.1.27. Η σχέση $\mathsf{Prime} = \{x \in \mathbb{N} \mid x \text{ πρώτος αριθμός}\}$ είναι πρωτογενώς αναδρομική καθώς η χαρακτηριστική της συνάρτηση είναι πρωτογενώς αναδρομική:

$$\chi_{\mathsf{Prime}}(x) = \begin{cases} 1 & , \text{ αν } \mathsf{dn}(x, x) = 2 \\ 0 & , \text{ αλλιώς} \end{cases}$$

όπου dn η συνάρτηση του Παραδείγματος 2.1.26.

Κλείνοντας αυτόν τον πρώτο κύκλο παραδειγμάτων θα πρέπει να τονίσουμε ότι ο τρόπος ορισμού των συναρτήσεων που είδαμε δεν είναι ο μοναδικός (όπως επίσης δεν αντιστοιχεί στον μοναδικό τρόπο να υπολογισθούν).

2.2 Φραγμένη ελαχιστοποίηση

Ορισμός 2.2.1. Έστω ολική συνάρτηση $g : \mathbb{N}^{m+1} \to \mathbb{N}$, $m \geq 1$ και $y \in \mathbb{N}$. Ο *τελεστής φραγμένης ελαχιστοποίησης της* g [1] ορίζεται ως εξής:

$$(\mu\, i \leq y)[g(i, x_1, \ldots, x_m) = 0] = \begin{cases} \min\{i \leq y \mid g(i, x_1, \ldots, x_m) = 0\} & , \text{ αν υπάρχει} \\ y + 1 & , \text{ αλλιώς} \end{cases}$$

Σκοπεύουμε να εφαρμόσουμε τον τελεστή της φραγμένης ελαχιστοποίησης σε πρωτογενώς αναδρομικές συναρτήσεις ούτως ώστε να παράξουμε καινούργιες συναρτήσεις. Για να μπορέσουμε όμως να το κάνουμε αυτό χρειαζόμαστε την ακόλουθη πρόταση (η απόδειξη αφήνεται ως Άσκηση 2.2).

Πρόταση 2.2.2. Κάθε πρωτογενώς αναδρομική συνάρτηση είναι ολική συνάρτηση.

[1] Η φραγμένη ελαχιστοποίηση αντιστοιχεί στο *φραγμένο while* μίας γλώσσας προγραμματισμού.

Πρόταση 2.2.3. Έστω $\mathsf{g} : \mathbb{N}^{m+1} \to \mathbb{N}$, $m \geq 1$, πρωτογενώς αναδρομική συνάρτηση. Η συνάρτηση $f : \mathbb{N}^{m+1} \to \mathbb{N}$ με:

$$f(y, x_1, \dots, x_m) = (\mu\ i \leq y)[\mathsf{g}(i, x_1, \dots, x_m) = 0]$$

είναι πρωτογενώς αναδρομική.

Απόδειξη. [1] Ορίζουμε τις πρωτογενώς αναδρομικές συναρτήσεις:

$$\mathsf{h}(j, x_1, \dots, x_m) = \begin{cases} 1 & , \text{αν } \mathsf{g}(j, x_1, \dots, x_m) \neq 0 \\ 0 & , \text{αν } \mathsf{g}(j, x_1, \dots, x_m) = 0 \end{cases}$$

$$\mathsf{s}(i, x_1, \dots, x_m) = \mathsf{prod}_{\mathsf{h}}(i, x_1, \dots, x_m) \qquad [= \prod_{j=0}^{i} \mathsf{h}(j, x_1, \dots, x_m)\ ]$$

και

$$f(y, x_1, \dots, x_m) = \mathsf{sum}_{\mathsf{s}}(y, x_1, \dots, x_m) \qquad [= \sum_{i=0}^{y} \mathsf{s}(i, x_1, \dots, x_m)\ ]$$

Παρατηρήστε ότι αν υπάρχει $i \leq y$ τέτοιο ώστε $g(i, x_1, \dots, x_m) = 0$, οι τιμές του $\mathsf{prod}_{\mathsf{h}}(j, x_1, \dots, x_m)$ για κάθε $i \leq j \leq y$ θα είναι 0, οπότε το $\mathsf{sum}_{\mathsf{s}}(y, x_1, \dots, x_m)$ θα ισούται με i [2]. □

Αντίστοιχα μπορούμε να αποδείξουμε και την ακόλουθη πρόταση.

Πρόταση 2.2.4. Έστω $\mathsf{h} : \mathbb{N}^m \to \mathbb{N}$ και $\mathsf{g} : \mathbb{N}^{m+1} \to \mathbb{N}$, $m \geq 1$, πρωτογενώς αναδρομικές συναρτήσεις. Η συνάρτηση $f : \mathbb{N}^m \to \mathbb{N}$ με:

$$f(x_1, \dots, x_m) = (\mu\ i \leq \mathsf{h}(x_1, \dots, x_m))[\mathsf{g}(i, x_1, \dots, x_m) = 0]$$

είναι πρωτογενώς αναδρομική.

Οι Προτάσεις 2.2.3 και 2.2.4 αποδεικνύουν ότι η φραγμένη ελαχιστοποίηση δεν «διευρύνει» την κλάση των πρωτογενώς αναδρομικών συναρτήσεων. Παρ' όλα αυτά ο τελεστής της φραγμένης ελαχιστοποίησης μας είναι πολύ χρήσιμος. Ας δούμε ένα παράδειγμα εφαρμογής του.

[1] Στην απόδειξη θα χρησιμοποιήσουμε το γεγονός ότι οι συναρτήσεις:

$$\mathsf{sum}_{\mathsf{g}}(y, x_1, \dots, x_m) = \sum_{i=0}^{y} \mathsf{g}(i, x_1, \dots, x_m)$$
$$\mathsf{prod}_{\mathsf{g}}(y, x_1, \dots, x_m) = \prod_{i=0}^{y} \mathsf{g}(i, x_1, \dots, x_m)$$

όπου $\mathsf{g} : \mathbb{N}^{m+1} \to \mathbb{N}$ πρωτογενώς αναδρομική συνάρτηση, είναι πρωτογενώς αναδρομικές (δες Άσκηση 2.4).

[2] Ενώ αν για κάθε $i \in [y]$ έχουμε $\mathsf{g}(i, x_1, \dots, x_m) \neq 0$, τότε $\mathsf{sum}_{\mathsf{s}}(y, x_1, \dots, x_m) = y + 1$. Τέλος, αν η τιμή της g δεν ορίζεται για κάποιο i τότε και η τιμή της ελαχιστοποίησης δεν θα ορίζεται (αν φυσικά η g είναι πρωτογενώς αναδρομική αυτό δεν πρόκειται να συμβεί).

Παράδειγμα 2.2.5. Η συνάρτηση $\mathsf{pn} : \mathbb{N} \to \mathbb{N}$ όπου ο $\mathsf{pn}(x)$ είναι ο x-οστός πρώτος αριθμός, δηλαδή:

$$\mathsf{pn}(x) = \begin{cases} 1 & , \text{ αν } x = 0 \\ \min\{p \in \mathbb{N} \mid p \text{ πρώτος και υπάρχουν} \geq x \text{ πρώτοι μικρότεροι του}\} & , \text{ αλλιώς} \end{cases}$$

μπορεί να οριστεί ως λύση των εξισώσεων:

$$\begin{cases} f(0) = 1 \\ f(x+1) = \begin{cases} 2 & , \text{ αν } x = 0 \\ (\mu\, i \leq \mathsf{fact}(f(x)) + 1)[\mathsf{g}(i, f(x)) = 0] & , \text{ αλλιώς} \end{cases} \end{cases}$$

όπου $\mathsf{g}(i,x) = 1 \dot{-} \chi_{\mathsf{P}}(i,x)$, $\mathsf{P} = \{(i,x) \in \mathbb{N}^2 \mid x < i \text{ και } i \in \mathsf{Prime}\}$ και fact η συνάρτηση του Παραδείγματος 2.1.8. Για να αποδείξουμε ότι η pn είναι πρωτογενώς αναδρομική πρέπει να δείξουμε ότι:

α) Η g είναι πρωτογενώς αναδρομική συνάρτηση.

και για να αποδείξουμε ότι όντως επιστρέφει τον x-οστός πρώτο ότι:

β) Για κάθε $n \in \mathbb{N}$ υπάρχει πρώτος αριθμός p τέτοιος ώστε $n < p \leq n! + 1$ [1].

Για το *α)* παρατηρήστε ότι $\chi_{\mathsf{P}}(i,x) = \chi_{<}(x,i) + \chi_{\mathsf{Prime}}(i) \dot{-} 1$, όπου οι $\chi_{<}$ και χ_{Prime} ορίζονται στα Παραδείγματα 2.1.18 και 2.1.27, άρα τόσο η χ_{P} όσο και η g είναι πρωτογενώς αναδρομικές.

Για το *β)* υποθέτουμε ότι ο $n! + 1$ δεν είναι πρώτος, τότε θα υπάρχει πρώτος αριθμός $p < n! + 1$ τέτοιος ώστε $p \mid n! + 1$. Ο p δεν μπορεί να διαιρεί το $n!$ γιατί τότε θα έπρεπε να διαιρεί το 1, άρα ο p δεν διαιρεί κανέναν από τους αριθμούς $1, 2, \ldots, n$. Συνεπώς ο p είναι ο ζητούμενος πρώτος αριθμός καθώς $n < p \leq n! + 1$.

Στο Παράδειγμα 2.2.5 δεν μπορούμε να εφαρμόσουμε άμεσα πρωτογενή αναδρομή καθώς δεν είναι γνωστό το «πλήθος επαναλήψεων» που θα χρειαστεί να κάνουμε μέχρι να βρούμε τον επόμενο πρώτο αριθμό.

Σύμβαση 2.2.6. Έστω σχέση $P \subseteq \mathbb{N}^{m+1}$, $m \geq 1$ και $y \in \mathbb{N}$. Είναι βολικό πολλές φορές να χρησιμοποιούμε τον τελεστή φραγμένης ελαχιστοποίησης ως εξής:

$$(\mu\, i \leq y)[(i, x_1, \ldots, x_m) \in P] = \begin{cases} \min\{i \leq y \mid (i, x_1, \ldots, x_m) \in P\} & , \text{ αν υπάρχει} \\ y + 1 & , \text{ αλλιώς} \end{cases}$$

καθώς ελαφρύνει λίγο τον συμβολισμό [2].

[1] Παρατηρήστε ότι αν αντικαταστήσω το n με $\mathsf{pn}(x)$, από τον ισχυρισμό έπεται ότι υπάρχει πρώτος αριθμός στο διάστημα $(\mathsf{pn}(x), \mathsf{pn}(x)! + 1]$.

[2] Σύμφωνα με τον Ορισμό 2.2.1 τυπικά θα έπρεπε να γράψουμε $(\mu\, i \leq y)[1 \dot{-} \chi_P(i, x_1, \ldots, x_m) = 0]$ (προφανώς η χ_P είναι ολική συνάρτηση).

2.3 Πλήρης πρωτογενής αναδρομή

Προτού ορίσουμε την *πλήρη πρωτογενή αναδρομή*, σύμφωνα με την οποία ορίζουμε αναδρομικά μία συνάρτηση χρησιμοποιώντας όλες τις ήδη υπολογισμένες τιμές της, θα χρειαστεί να κωδικοποιήσουμε ακολουθίες φυσικών αριθμών. Όπως αποδεικνύει η Πρόταση 2.3.5 ούτε η πλήρης πρωτογενής αναδρομή επεκτείνει την κλάση των πρωτογενώς αναδρομικών συναρτήσεων.

Κωδικοποίηση ακολουθιών φυσικών αριθμών

Μπορούμε να κωδικοποιήσουμε μονοσήμαντα μία ακολουθία φυσικών αριθμών $x_1, x_2, \dots, x_n$ ως το γινόμενο των n-πρώτων πρώτων αριθμών, όπου ο i-οστός πρώτος έχει υψωθεί στη $(x_i + 1)$-οστή δύναμη [1]. Για παράδειγμα κωδικοποιούμε την ακολουθία 0,1,2,3 στον αριθμό $2^1 \cdot 3^2 \cdot 5^3 \cdot 7^4 = 5402250$ [2].

Αν κάποιος μας δώσει έναν φυσικό αριθμό n που αποτελεί κωδικοποίηση κάποιας ακολουθίας μπορούμε εύκολα να βρούμε τον i-οστό όρο της βρίσκοντας τη μέγιστη δύναμη του i-οστού πρώτου αριθμού που διαιρεί τον n και αφαιρώντας ένα από αυτή. Στο παράδειγμα που δώσαμε παραπάνω, αναζητώντας τον τρίτο όρο της ακολουθίας παρατηρούμε ότι οι $5, 5^2, 5^3$ διαιρούν τον 5402250 ενώ ο 5^4 όχι. Συνεπώς ο ζητούμενος όρος ισούται με $3 - 1 = 2$. Ας κάνουμε αυτήν την περιγραφή τυπικό ορισμό.

Ορισμός 2.3.1. Ορίζουμε για κάθε $n \in \mathbb{N}$ τις συναρτήσεις $\mathsf{enc}_n : \mathbb{N}^n \to \mathbb{N}$:

$$\begin{aligned} &\mathsf{enc}_0 = 1 \text{ [3]} \\ &\mathsf{enc}_n(x_1, \dots, x_n) = 2^{x_1+1} \cdot 3^{x_2+1} \cdot \ \cdots \ \cdot p_n^{x_n+1}, \quad \text{για } n \geq 1 \end{aligned}$$

όπου p_n ο n-οστος πρώτος αριθμός. Ορίζουμε επίσης τη σχέση:

$$\mathsf{seq} = \{x \in \mathbb{N} \mid x = 1 \text{ ή υπάρχουν } n, x_1, \dots, x_n \in \mathbb{N} \text{ τέτοια ώστε } x = \mathsf{enc}_n(x_1, \dots, x_n)\}$$

και τη συνάρτηση $\mathsf{dec} : \mathbb{N}^2 \to \mathbb{N}$ με:

$$\mathsf{dec}(i, x) = \begin{cases} x_i & , \text{ αν } x \in \mathsf{seq}, \text{ έστω } x = \mathsf{enc}_n(x_1, \dots, x_n), \text{ και } i \in [n] \\ x + 1 & , \text{ αλλιώς} \end{cases}$$

Πρόταση 2.3.2. Οι συναρτήσεις enc_n, dec και η σχέση seq είναι πρωτογενώς αναδρομικές.

Απόδειξη. Ορίζουμε:

$$\begin{aligned} &\mathsf{enc}_0 = 1 \\ &\mathsf{enc}_n(x_1, \dots, x_n) = \mathsf{pn}(1)^{x_1+1} \cdot \ \cdots \ \cdot \mathsf{pn}(n)^{x_n+1} \end{aligned}$$

[1] Το $+1$ χρειάζεται γιατί μπορεί κάποιος από τους όρους της ακολουθίας να είναι 0.

[2] Προφανώς η κωδικοποίηση αυτή δεν είναι καθόλου αποδοτική όσον αφορά τον χρόνο που χρειαζόμαστε να κωδικοποιήσουμε και να αποκωδικοποιήσουμε μία ακολουθία.

[3] Στην περίπτωση αυτή έχουμε την *κενή ακολουθία φυσικών αριθμών.*

όπου pn η συνάρτηση του Παραδείγματος 2.2.5.

Παρατηρήστε ότι ένας φυσικός αριθμός (μεγαλύτερος της μονάδας) αποτελεί κωδικοποίηση ακολουθίας n φυσικών αριθμών αν είναι το γινόμενο δυνάμεων των n-πρώτων πρώτων αριθμών. Με άλλα λόγια, θα πρέπει οι n-πρώτοι αριθμοί να τον διαιρούν (και μόνο αυτοί). Επομένως, μπορούμε να ορίσουμε τη χαρακτηριστική συνάρτηση της seq ως εξής:

$$\chi_{\mathsf{seq}}(x) = \begin{cases} 1 & , \text{ αν } x = 1 \\ 1 \dot{-} ((x+1) \dot{-} (\mu\, j \leq x)[(j > (\mu\, i \leq x)[\mathsf{pn}(i) \nmid x]) \wedge \mathsf{pn}(j) \mid x]) & , \text{ αλλιώς } [1] \end{cases}$$

όπου γράφουμε $\mathsf{pn}(i) \nmid x$ αντί για $(\mathsf{pn}(i), x) \in \overline{\{(x,y) \in \mathbb{N}^2 \mid x \mid y\}}$ [2].

Τέλος ορίζουμε:

$$\mathsf{dec}(i,x) = \begin{cases} (\mu\, j \leq x)[\mathsf{pn}(i)^{j+1} \nmid x] \dot{-} 1 & , \text{ αν } x \in \mathsf{seq} \text{ και } \mathsf{pn}(i) \mid x \\ x+1 & , \text{ αλλιώς} \end{cases}$$

□

Σύμβαση 2.3.3. Για να ελαφρύνουμε λίγο τον συμβολισμό θα γράφουμε $\langle\ \rangle$ αντί για enc_0 και $\langle x_1, \ldots, x_n \rangle$ αντί για $\mathsf{enc}_n(x_1, \ldots, x_n)$ [3].

Η απόδειξη της παρακάτω πρότασης αφήνεται ως άσκηση (Άσκηση 2.9).

Πρόταση 2.3.4. Οι συναρτήσεις $\mathsf{length} : \mathbb{N} \to \mathbb{N}$, $\mathsf{add} : \mathbb{N}^2 \to \mathbb{N}$, $\mathsf{replace} : \mathbb{N}^3 \to \mathbb{N}$ και $\mathsf{remove} : \mathbb{N}^2 \to \mathbb{N}$ με:

$$\mathsf{length}(x) = \begin{cases} n & , \text{ αν } x \in \mathsf{seq}, \text{ έστω } x = \langle x_1, \ldots, x_n \rangle \\ x+1 & , \text{ αλλιώς} \end{cases}$$

$$\mathsf{add}(x,y) = \begin{cases} \langle x_1, \ldots, x_n, y \rangle & , \text{ αν } x \in \mathsf{seq}, \text{ έστω } x = \langle x_1, \ldots, x_n \rangle \\ 0 & , \text{ αλλιώς} \end{cases}$$

$$\mathsf{replace}(x,i,y) = \begin{cases} \langle x_1, \ldots, x_{i-1}, y, x_{i+1}, \ldots, x_n \rangle, \text{αν } x \in \mathsf{seq}, \text{ έστω } x = \langle x_1, \ldots, x_n \rangle, \text{ και } i \in [n] \\ 0 \qquad\qquad , \text{αλλιώς} \end{cases}$$

και

$$\mathsf{remove}(x) = \begin{cases} \langle x_1, \ldots, x_{n-1} \rangle & , \text{ αν } x \in \mathsf{seq}, \text{ έστω } x = \langle x_1, \ldots, x_n \rangle, \text{ και } n \geq 2 \\ 1 & , \text{ αν } x \in \mathsf{seq} \text{ και } x = \langle x_1 \rangle \\ 0 & , \text{ αλλιώς} \end{cases}$$

είναι πρωτογενώς αναδρομικές.

[1] Λίγη βοήθεια ενδεχομένως να χρειάζεται εδώ... Για να πάρει η $\chi_{\mathsf{seq}}(x)$ τιμή 1 θα πρέπει ($x = 1$ ή) η ελαχιστοποίηση να πάρει τιμή $x+1$. Έστω $\mathsf{pn}(i)$ ο πρώτος πρώτος αριθμός που δεν διαιρεί τον x. Παρατηρήστε ότι αν δεν υπάρχει άλλος πρώτος μεγαλύτερος του $\mathsf{pn}(i)$ που να διαιρεί τον x (δηλαδή ο x διαιρείται από όλους τους πρώτους πριν από τον i-οστό, και μόνο από αυτούς) τότε η ελαχιστοποίηση (θα «αποτύχει» και) θα επιστρέψει $x+1$.

[2] Χρησιμοποιούμε επίσης την Παρατήρηση 2.2.6.

[3] Για να δούμε ποια απ' όλες τις συναρτήσεις κωδικοποίησης enc_n χρησιμοποιούμε κάθε φορά αρκεί να μετρήσουμε το πλήθος των όρων μέσα στις αγκύλες.

Πρόταση 2.3.5 (Πλήρης πρωτογενής αναδρομή). Έστω $\mathsf{g} : \mathbb{N}^{m-1} \to \mathbb{N}$ και $\mathsf{h} : \mathbb{N}^{m+1} \to \mathbb{N}$ πρωτογενώς αναδρομικές συναρτήσεις, όπου $m > 1$. Η συνάρτηση $f : \mathbb{N}^m \to \mathbb{N}$ που αποτελεί λύση των εξισώσεων:

$$\begin{cases} f(0, x_1, \dots, x_{m-1}) = \mathsf{g}(x_1, \dots, x_{m-1}) \\ f(y+1, x_1, \dots, x_{m-1}) = \mathsf{h}(\langle f(0, x_1, \dots, x_{m-1}), \dots, f(y, x_1, \dots, x_{m-1})\rangle, y, x_1, \dots, x_{m-1}) \end{cases}$$

είναι πρωτογενώς αναδρομική.

Απόδειξη. Πρώτα θεωρούμε την πρωτογενώς αναδρομική συνάρτηση $k : \mathbb{N}^m \to \mathbb{N}$ που αποτελεί λύση των εξισώσεων:

$$\begin{cases} k(0, x_1, \dots, x_{m-1}) = \langle \mathsf{g}(x_1, \dots, x_{m-1})\rangle \\ k(y+1, x_1, \dots, x_{m-1}) = \mathsf{add}(k(y, x_1, \dots, x_{m-1}), \mathsf{h}(k(y, x_1, \dots, x_{m-1}), y, x_1, \dots, x_{m-1})) \end{cases}$$

και ορίζουμε την f ως εξής:

$$f(y, x_1, \dots, x_{m-1}) = \mathsf{dec}(y+1, k(y, x_1, \dots, x_{m-1}))$$

□

Παρατήρηση 2.3.6. Αντίστοιχα με την Πρόταση 2.1.7 μπορούμε να ορίσουμε την πλήρη πρωτογενή αναδρομή και χωρίς παραμέτρους.

Παράδειγμα 2.3.7 (Αριθμοί Fibonacci). Η συνάρτηση $\mathsf{fib} : \mathbb{N} \to \mathbb{N}$ με:

$$\mathsf{fib}(n) = \begin{cases} 0 & , \text{ αν } n = 0 \\ 1 & , \text{ αν } n = 1 \\ \mathsf{fib}(n-1) + \mathsf{fib}(n-2) & , \text{ αν } n \geq 2 \end{cases}$$

είναι πρωτογενώς αναδρομική, καθώς αποτελεί λύση των εξισώσεων:

$$\begin{cases} f(0) = 0 \\ f(n+1) = \begin{cases} 1 & , \text{ αν } n = 0 \\ \mathsf{dec}(n+1, \langle f(0), \dots, f(n)\rangle) + \mathsf{dec}(n, \langle f(0), \dots, f(n)\rangle) & , \text{ αλλιώς} \end{cases} \end{cases}$$

Παράδειγμα 2.3.8 (Ο αλγόριθμος του Ευκλείδη). Θα δείξουμε ότι η συνάρτηση $\mathsf{gcd} : \mathbb{N}^2 \to \mathbb{N}$, με $\mathsf{gcd}(x, y) = \max\{d \in \mathbb{N} \mid d = 0 \ \vee \ (d \mid x \ \wedge \ d \mid y)\}$ (ο *μέγιστος κοινός διαιρέτης των x και y* δηλαδή), είναι πρωτογενώς αναδρομική.

Ας θυμηθούμε πρώτα τον αλγόριθμο του Ευκλείδη [1]:

$$\text{ΜΚΔ}(x, y) = \begin{cases} 0 & , \text{ αν } x = 0 \text{ ή } y = 0 \\ x & , \text{ αν } x, y \geq 1 \text{ και } x \mid y \\ \text{ΜΚΔ}(y \bmod x, y) & , \text{ αν } 1 \leq x \leq y \text{ και } x \nmid y \\ \text{ΜΚΔ}(x \bmod y, y) & , \text{ αν } 1 \leq y < x \end{cases}$$

[1] Η εκδοχή αυτή δεν είναι η αποδοτικότερη δυνατή (όσον αφορά το πλήθος επαναλήψεων).

Παρατηρούμε ότι η συνάρτηση gcd αποτελεί λύση των εξισώσεων:

$$\begin{cases} f(0,y)=0 \\ f(x+1,y)=\begin{cases} 0 & ,\text{αν } y=0 \\ x+1 & ,\text{αν } y\geq 1 \text{ και } x+1 \mid y \\ \mathsf{dec}(\mathsf{rm}(y,x+1)+1,\langle f(0,y),\dots,f(x,y)\rangle) & ,\text{αν } x+1\leq y \text{ και } x+1\nmid y \\ \mathsf{dec}(\mathsf{rm}(x+1,y)+1,\langle f(0,y),\dots,f(x,y)\rangle) & ,\text{αλλιώς } (1\leq y<x+1) \end{cases} \end{cases}$$

[1]

όπου rm η συνάρτηση του Παραδείγματος 2.1.23, άρα όντως είναι πρωτογενώς αναδρομική.

Στις ασκήσεις θα δούμε ότι υπάρχουν και άλλες μορφές αναδρομής, όπως για παράδειγμα η *αμοιβαία αναδρομή* (Άσκηση 2.10) και η *εμφωλευμένη αναδρομή* (Άσκηση 2.11), που πάλι όμως δεν επεκτείνουν την κλάση των πρωτογενώς αναδρομικών συναρτήσεων. Για τη *διπλή αναδρομή* (Άσκηση 2.13) δεν ισχύει το ίδιο. Συνεπώς ακόμα και βασικές παραλλαγές τις αναδρομής μπορούν να ορίσουν συναρτήσεις που δεν είναι πρωτογενώς αναδρομικές. Αυτό μας οδηγεί άμεσα στη διαπίστωση ότι η κλάση των πρωτογενώς αναδρομικών συναρτήσεων είναι πολύ «στενή [2]» για τους σκοπούς μας.

2.4 Ελαχιστικά αναδρομικές συναρτήσεις

Οι πρωτογενώς αναδρομικές συναρτήσεις είναι ολικές συναρτρήσεις. Όμως στο Κεφάλαιο 1, που ορίσαμε τις υπολογίσιμες (κατά Turing) συναρτήσεις, είδαμε παραδείγματα συναρτήσεων που είναι υπολογίσιμες αλλά όχι ολικές. Για να φτάσουμε συνεπώς σε έναν δεύτερο ορισμό των υπολογίσιμων συναρτήσεων θα πρέπει να ορίσουμε μία γενικότερη κλάση από αυτήν των πρωτογενώς αναδρομικών. Στην κλάση αυτή θα μας οδηγήσει ένας τελεστής που μπορεί να παράγει και μερικές συναρτήσεις, ο τελεστής της *μη-φραγμένης* ελαχιστοποίησης [3].

Ορισμός 2.4.1. Έστω συνάρτηση $g:\mathbb{N}^{m+1}\to\mathbb{N}$, $m\geq 1$, και $y\in\mathbb{N}$. Ο *τελεστής ελαχιστοποίησης της* g (ή *μ-ελαχιστοποίησης*) [4] ορίζεται ως εξής:

$$(\mu\, i\geq y)[g(i,x_1,\dots,x_m)=0]=\begin{cases} \min\{i\geq y \mid g(i,x_1,\dots,x_m)=0\} & ,\text{αν υπάρχει τέτοιο } i \text{ και} \\ & \quad \text{για κάθε } j \text{ με } y\leq j<i \\ & \quad \text{ισχύει } g(j,x_1,\dots,x_m)>0 \\ \bot & ,\text{ αλλιώς} \end{cases}$$

[1] Παρατηρήστε ότι η τιμή $f(\mathsf{rm}(y,x+1),y)$ υπάρχει στην ακολουθία $\langle f(0,y),\dots,f(x,y)\rangle$, καθώς ισχύει ότι $y \bmod (x+1)\leq x$. Μάλιστα είναι ο $(y \bmod (x+1)+1)$-οστός όρος της ακολουθίας.

[2] *Στενή είναι η αρετή, δεν μπορώ ν' αναπνέψω· μικρός, στενός είναι ο Παράδεισος, δε με χωράει· σαν άνθρωπος μου φαίνεται ο Θεός σας, δεν τον θέλω!* [12].

[3] Συνεχίζοντας την παραβολή της προηγούμενης υποοσημείωσης θα μπορούσαμε να πούμε ότι για να ορίσουμε τις υπολογίσιμες συναρτήσεις θα πρέπει να ξεφύγουμε από το ανθρώπινο-πεπερασμένο και να φτάσουμε στο άπειρο, εισάγωντας τον υπολογισμό που διαρκεί για πάντα (αυτό που στο Κεφάλαιο 1 αναφέραμε ως «κόλλημα»).

[4] Η ελαχιστοποίηση αντιστοιχεί στο *(μη-φραγμένο) while* μίας γλώσσας προγραμματισμού.

Παρατήρηση 2.4.2. Ας τονίσουμε μία σημαντική λεπτομέρεια του Ορισμού 2.4.1: Αν για κάποιο $j \geq y$ ισχύει ότι $g(j, x_1, \dots, x_m) = \perp$ και για κάθε i με $y \leq i < j$ ισχύει ότι $g(i, x_1, \dots, x_m) \geq 0$, ακόμα και αν υπάρχει k με $j < k$ για το οποίο $g(k, x_1, \dots, x_m) = 0$, έχουμε ότι $(\mu\, i \geq y)[g(i, x_1, \dots, x_m) = 0] = \perp$.

Ορισμός 2.4.3. Μία συνάρτηση $f : \mathbb{N}^m \to \mathbb{N}$, $m \geq 1$ είναι *ελαχιστικά αναδρομική* (ή *μ-αναδρομική* ή και σκέτο *αναδρομική*) ανν είναι μία εκ των (a), (b) και (c) του Ορισμού 2.1.1 ή προκύπτει με εφαρμογή των (1), (2) του Ορισμού 2.1.1 και του τελεστή ελαχιστοποίησης, σε ελαχιστικά αναδρομικές συναρτήσεις.

Ορισμός 2.4.4. Μία σχέση $P \subseteq \mathbb{N}^m$, $m \geq 1$, είναι *ελαχιστικά αναδρομική* (ή *μ-αναδρομική*, ή και σκέτο *αναδρομική*) ανν η χαρακτηριστική της συνάρτηση $\chi_P : \mathbb{N}^m \to \{0, 1\}$ είναι ελαχιστικά αναδρομική.

Παράδειγμα 2.4.5. Ο αριθμός $p \in \mathbb{N}$ καλείται *δίδυμος πρώτος* ανν οι p και $p + 2$ είναι πρώτοι αριθμοί. Η συνάρτηση $\mathsf{tpn} : \mathbb{N} \to \mathbb{N}$ όπου ο $\mathsf{tpn}(x)$ είναι ο x-οστός δίδυμος πρώτος αριθμός, δηλαδή:

$$\mathsf{tpn}(x) = \begin{cases} 1 & , \text{ αν } x = 0 \\ \min\{p \in \mathbb{N} \mid \ p \text{ δίδυμος πρώτος και υπάρχουν } \geq x \\ \qquad\qquad \text{δίδυμοι πρώτοι αριθμοί μικρότεροι του } p\} & , \text{ αλλιώς} \end{cases}$$

είναι ελαχιστικά αναδρομική καθώς αποτελεί λύση των εξισώσεων:

$$\begin{cases} f(0) = 1 \\ f(x+1) = \begin{cases} 3 & , \text{ αν } x = 0 \\ (\mu\, i \geq f(x) + 1)[2 \dot{-} (\chi_{\mathsf{Prime}}(i) + \chi_{\mathsf{Prime}}(i+2)) = 0] & , \text{ αλλιώς} \end{cases} \end{cases}$$

όπου η χ_{Prime} ορίζεται στο Παράδειγμα 2.1.27.

Σημείωση 2.4.6. Αν υπήρχε ένα άνω φράγμα μέχρι το οποίο θα έπρεπε να ψάξουμε για να βρούμε τον επόμενο δίδυμο πρώτο αριθμό, θα μπορούσαμε να ορίσουμε την tpn του Παραδείγματος 2.4.5 χρησιμοποιώντας τον τελεστή της φραγμένης ελαχιστοποίησης. Όμως δεν έχει βρεθεί ακόμα τέτοιο άνω φράγμα, όπως δεν έχει ακόμα δοθεί απάντηση στο ερώτημα αν υπάρχουν άπειροι το πλήθος δίδυμοι πρώτοι.

Σύμφωνα με την παραπάνω σημείωση η tpn είναι μία ελαχιστικά αναδρομική συνάρτηση για την οποία δεν μπορούμε να αποφασίσουμε «ακόμα» [1] αν επιπλέον είναι και πρωτογενώς αναδρομική. Ενδεχομένως το πιο γνωστό παράδειγμα ελαχιστικά αναδρομικής συνάρτησης

[1] Σύμφωνα με το πρώτο Θεώρημα Μη-πληρότητας του Gödel ενδέχεται να μην πάρουμε ποτέ θετική ή αρνητική απάντηση σε αυτό το ερώτημα!

που (αποδεδειγμένα) δεν είναι πρωτογενώς αναδρομική είναι η συνάρτηση του Ackermann που αποτελεί λύση των εξισώσεων [1]:

$$\begin{cases} A(0,y) = y+1 \\ A(x+1,0) = A(x,1) \\ A(x+1,y+1) = A(x,A(x+1,y)) \end{cases}$$

Συνεπώς ισχύει το ακόλουθο θεώρημα (το οποίο προκύπτει από την Άσκηση 2.16).

Θεώρημα 2.4.7. Η κλάση των πρωτογενώς αναδρομικών συναρτήσεων αποτελεί γνήσιο υποσύνολο της κλάσης των ελαχιστικά αναδρομικών συναρτήσεων.

2.5 Δεύτερος ορισμός υπολογίσιμων συναρτήσεων

Ο δεύτερος ορισμός των υπολογίσιμων συναρτήσεων είναι ο Ορισμός 2.4.3 και η εξήγηση δίνεται στο ακόλουθο θεώρημα.

Θεώρημα 2.5.1. Μία συνάρτηση $f : \mathbb{N}^m \to \mathbb{N}$ είναι ελαχιστικά αναδρομική ανν είναι (Turing) υπολογίσιμη.

Η απόδειξη του Θεωρήματος 2.5.1

Για το ευθύ θα περιγράψουμε μόνο την κεντρική ιδέα και θα αφήσουμε τις περισσότερες λεπτομέρειες ως άσκηση για τον αναγνώστη.

Το αντίστροφο παρουσιάζει μεγαλύτερο ενδιαφέρον και θα το δούμε πολύ προσεκτικά. Έστω υπολογίσιμη συνάρτηση f και έστω M μία TM που την υπολογίζει. Το σχεδιάγραμμα της απόδειξης είναι το εξής:

Στάδιο 1: Κωδικοποιούμε τα στιγμιότυπα λειτουργίας της M, για κάποια είσοδο $n \in \mathbb{N}$, με αριθμούς από το seq (δες Ορισμό 2.3.1). Έτσι ο υπολογισμός $M(n)$ θα αντιστοιχεί σε μια ακολουθία από αριθμούς.

Στάδιο 2: Ορίζουμε πρωτογενώς αναδρομική συνάρτηση που «ακολουθεί» τον υπολογισμό $M(n)$: Δεδομένου του αριθμού ενός στιγμιοτύπου μας επιστρέφει τον αριθμό του επόμενου στιγμιοτύπου.

Στάδιο 3: Ορίζουμε τη συνθήκη που μας δείχνει ότι η $M(n)$ τερμάτισε [2].

Στάδιο 4: Υπολογίζουμε την τιμή της $f(n)$.

[1] Η απόδειξη ότι η Ackermann είναι ελάχιστικά αλλά όχι πρωτογενώς αναδρομική αφήνεται ως άσκηση (δες Άσκηση 2.16). Με λίγα λόγια θα μπορούσαμε να πούμε ότι η Ackermann «αυξάνει» πιο γρήγορα από οποιαδήποτε πρωτογενώς αναδρομική συνάρτηση.

[2] Μέχρι αυτό το σημείο δεν θα χρειαστεί να χρησιμοποιήσουμε την ελαχιστοποίηση. Εδώ όμως είμαστε αναγκασμένοι να τη χρησιμοποιήσουμε καθώς θα αναζητήσουμε το ελάχιστο «βήμα» για το οποίο ο υπολογισμός της $M(n)$ δεν έκανε «πρόοδο» (δηλαδή η κεφαλή της M δεν κινήθηκε).

Τελευταία ενημέρωση 10/1/2025, στις 08:17.

Απόδειξη Θεωρήματος 2.5.1. ($\Rightarrow$) Αρκεί να δείξουμε ότι οι συναρτήσεις (a), (b) και (c) του Ορισμού 2.1.1 είναι υπολογίσιμες συναρτήσεις και ότι τα (1), (2) του Ορισμού 2.1.1 και η ελαχιστοποίηση, αν εφαρμοστούν σε υπολογίσιμες συναρτήσεις, δίνουν υπολογίσιμη συνάρτηση (δες Άσκηση 2.21).

($\Leftarrow$) Έστω υπολογίσιμη συνάρτηση $f : \mathbb{N} \to \mathbb{N}$ και έστω ότι η ΤΜ $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{τέλος}})$ την υπολογίζει. Χωρίς βλάβη της γενικότητας, θα κάνουμε τις κάτωθι παραδοχές για την M:

1. $Q = \{q_0, q_1, \dots, q_n\}$ και η q_n είναι η τερματική κατάσταση.
2. $\Sigma = \{1\}$, δηλαδή ο φυσικός αριθμός της εισόδου (και η τιμή της εξόδου) δίνεται στο *μοναδιαίο* σύστημα αρίθμησης [1].
3. $\Gamma = \{a_0, a_1, \dots, a_k\}$ όπου $a_0 = \sqcup$, $a_1 = \triangleright$ και $a_2 = 1$.
4. Η M είναι μονοταινιακή και ντετερμινιστική.
5. Τέλος, θα πρέπει η M να μην κολλάει εξαιτίας μη ύπαρξης επόμενου στιγμιότυπου σύμφωνα με τη δ (δες Υποσημείωση 2 Σελίδα 17, και Υποσημείωση 1 Σελίδα 77 για τον λόγο που αυτό είναι απαραίτητο).

Στάδιο 1.1 Κωδικοποίηση: Σύμφωνα με τον Ορισμό 1.1.6 ένα στιγμιότυπο χαρακτηρίζεται από τρεις πληροφορίες: την κατάσταση που βρίσκεται η M, τη λέξη που περιέχει η ταινία της και τη θέση της κεφαλής. Αρχίζουμε *αριθμητικοποιώντας* (ο όρος αυτός αναλύεται στην Παράγραφο A.5.1) τις τρεις αυτές πληροφορίες, όπου με $\langle * \rangle_{\mathbb{N}}$ συμβολίζουμε τον αριθμό που αντιστοιχίσαμε στο $*$:

- Για κάθε κατάσταση $q_i \in Q$ ορίζουμε $\langle q_i \rangle_{\mathbb{N}} = i$.
- Για κάθε σύμβολο $a_i \in \Gamma$ ορίζουμε $\langle a_i \rangle_{\mathbb{N}} = i$.
- Κάθε λέξη $s_1 \cdots s_l \in \Gamma^*$ ορίζουμε $\langle s_1 \cdots s_l \rangle_{\mathbb{N}} = \mathsf{enc}_l(\langle s_1 \rangle_{\mathbb{N}}, \dots, \langle s_l \rangle_{\mathbb{N}})$.
- Αντιστοιχούμε τη θέση της κεφαλής στον αριθμό του κελιού που βρίσκεται η κεφαλή.
- Αριθμητικοποιήσουμε τα A, Δ ως εξής: $\langle \mathrm{A} \rangle_{\mathbb{N}} = 0$ και $\langle \Delta \rangle_{\mathbb{N}} = 2$.

Συνεπώς, μπορούμε να θεωρήσουμε το στιγμιότυπο $\triangleright\, w_1 q_i w_2$ ως μία ακολουθία τριών αριθμών, των: i (κατάσταση), $|w_1| + 2$ (θέση κεφαλής) και $\langle \triangleright\, w_1 w_2 \rangle_{\mathbb{N}}$ (λέξη ταινίας), και να το αριθμητικοποιήσουμε περαιτέρω ως εξής:

$$\langle \triangleright\, w_1 q_i w_2 \rangle_{\mathbb{N}} = \mathsf{enc}_3(i, |w_1| + 2, \langle \triangleright\, w_1 w_2 \rangle_{\mathbb{N}})$$

Για παράδειγμα το αρχικό στιγμιότυπο αριθμητικοποιείται ως:

$$\langle \triangleright\, q_0 \underbrace{1 \cdots 1}_{n+1 \text{ φορές}} \rangle_{\mathbb{N}} = \mathsf{enc}_3(0, 2, \langle \triangleright \underbrace{1 \cdots 1}_{n+1 \text{ φορές}} \rangle_{\mathbb{N}}) = 2^1 \cdot 3^3 \cdot 5^{2^2 \cdot 3^3 \cdot 5^3 \cdot \cdots \cdot p_{n+2}^3 + 1}$$

[1] Σε αυτό το σύστημα το 0 γράφεται ως 1 και ο αριθμός n ως $\underbrace{1 \cdots 1}_{n+1 \text{ φορές}}$.

Στάδιο 1.2 Αποκωδικοποίηση: Έστω $x \in \mathsf{seq}$ η κωδικοποίηση ενός στιγμιοτύπου της $M(n)$. Θα συμβολίσουμε τις συναρτήσεις που αποκωδικοποιούν το x ως εξής [1]:

- $\mathsf{cs}(x) = \mathsf{dec}(1, x)$ (επιστρέφει τον αριθμό της κατάστασης)

- $\mathsf{ctp}(x) = \mathsf{dec}(2, x)$ (επιστρέφει τη θέση της κεφαλής)

- $\mathsf{ctn}(x) = \mathsf{dec}(3, x)$ (επιστρέφει τον αριθμό που αντιστοιχεί στη λέξη που περιέχει η ταινία)

- $\mathsf{cts}(x) = \mathsf{dec}(\mathsf{ctp}(x), \mathsf{ctn}(x))$ (επιστρέφει το σύμβολο που διαβάζει η κεφαλή)

Στάδιο 2: Θα ορίσουμε τη συνάρτηση $\mathsf{tr}_M : \mathbb{N}^2 \to \mathbb{N}$ με το $\mathsf{tr}_M(x, t$ να ισούται με τον αριθμό που αντιστοιχεί στο στιγμιότυπο της $M(x)$ μετά από t βήματα υπολογισμού [2]. Πρώτα θα ορίσουμε συναρτήσεις που μας επιστρέφουν τον αριθμό που αντιστοιχεί στην επόμενη κατάσταση, στην επόμενη θέση της κεφαλής και στην επόμενη λέξη στην ταινία, και μετά θα τα κωδικοποιήσουμε όλα μαζί σε έναν αριθμό που θα αντιστοιχεί στο επόμενο στιγμιότυπο.

Ας υποθέσουμε ότι η συνάρτηση δ περιέχει τις μεταβάσεις:

$$\begin{aligned} \delta(q_{i_0}, b_0) &= (q_{j_0}, c_0, d_0) \\ \delta(q_{i_1}, b_1) &= (q_{j_1}, c_1, d_1) \\ &\vdots \\ \delta(q_{i_m}, b_m) &= (q_{j_m}, c_m, d_m) \\ \delta(q_n, b) &= \bot,\ \forall b \in \Gamma \ [3] \end{aligned}$$

όπου $q_{i_r} \in Q \setminus \{q_n\}, q_{j_r} \in Q$, $b_r, c_r \in \Gamma$ και $d_r \in \{\mathrm{A}, \Delta\}$ για $r \in [m]$. Ορίζουμε τη συνάρτηση $\mathsf{ns} : \mathbb{N} \to \mathbb{N}$ με:

$$\mathsf{ns}(x) = \begin{cases} j_0 & , \text{ αν } \mathsf{cs}(x) = i_0 \text{ και } \mathsf{cts}(x) = \langle b_0 \rangle_{\mathbb{N}} \\ j_1 & , \text{ αν } \mathsf{cs}(x) = i_1 \text{ και } \mathsf{cts}(x) = \langle b_1 \rangle_{\mathbb{N}} \\ \vdots & \\ j_m & , \text{ αν } \mathsf{cs}(x) = i_m \text{ και } \mathsf{cts}(x) = \langle b_m \rangle_{\mathbb{N}} \\ \mathsf{cs}(x) & , \text{ αλλιώς} \end{cases}$$

που επιστρέφει την αριθμητικοποίηση της επόμενης κατάστασης, τη συνάρτηση $\mathsf{ntp} : \mathbb{N} \to \mathbb{N}$

[1] Για να κρατήσουμε την απόδειξη όσο πιο απλή γίνεται δεν θα ορίσουμε τις ακόλουθες συναρτήσεις για τα $x \notin \mathsf{seq}$. Για αυτά θα επιστρέφουν κάποια «παράλογη» τιμή.

[2] Για παράδειγμα: $\mathsf{tr}_M(x, 0) = \langle \triangleright\ q_0 \underbrace{1 \cdots 1}_{x+1 \text{ φορές}} \rangle_{\mathbb{N}}$.

[3] Σύμφωνα με τις παροχές που έχουμε κάνει για την M, αυτά είναι τα μόνα ορίσματα για τα οποία η τιμή της δ δεν ορίζεται.

με:

$$\mathsf{ntp}(x) = \begin{cases} \mathsf{ctp}(x) + \langle d_0 \rangle_{\mathbb{N}} \dot{-} 1 & , \text{ αν } \mathsf{cs}(x) = i_0 \text{ και } \mathsf{cts}(x) = \langle b_0 \rangle_{\mathbb{N}} \ ^{1} \\ \mathsf{ctp}(x) + \langle d_1 \rangle_{\mathbb{N}} \dot{-} 1 & , \text{ αν } \mathsf{cs}(x) = i_1 \text{ και } \mathsf{cts}(x) = \langle b_1 \rangle_{\mathbb{N}} \\ \quad \vdots & \\ \mathsf{ctp}(x) + \langle d_m \rangle_{\mathbb{N}} \dot{-} 1 & , \text{ αν } \mathsf{cs}(x) = i_m \text{ και } \mathsf{cts}(x) = \langle b_m \rangle_{\mathbb{N}} \\ \mathsf{ctp}(x) & , \text{ αλλιώς} \end{cases}$$

που επιστρέφει την αριθμητικοποίηση της επόμενης θέσης στην ταινία και, τέλος, τη συνάρτηση $\mathsf{nts} : \mathbb{N} \to \mathbb{N}$ με:

$$\mathsf{nts}(x) = \begin{cases} \langle c_0 \rangle_{\mathbb{N}} & , \text{ αν } \mathsf{cs}(x) = i_0 \text{ και } \mathsf{cts}(x) = \langle b_0 \rangle_{\mathbb{N}} \\ \langle c_1 \rangle_{\mathbb{N}} & , \text{ αν } \mathsf{cs}(x) = i_1 \text{ και } \mathsf{cts}(x) = \langle b_1 \rangle_{\mathbb{N}} \\ \quad \vdots & \\ \langle c_m \rangle_{\mathbb{N}} & , \text{ αν } \mathsf{cs}(x) = i_m \text{ και } \mathsf{cts}(x) = \langle b_m \rangle_{\mathbb{N}} \\ \mathsf{cts}(x) & , \text{ αλλιώς} \end{cases}$$

που επιστρέφει την αριθμητικοποίηση του συμβόλου που πρέπει να γράψουμε στην ταινία.

Παρατηρήστε ότι μετά από μία μετάβαση της M αλλάζει μόνο το σύμβολο που διαβάζει η κεφαλή. Συνεπώς αν $x \in \mathbb{N}$ είναι ο αριθμός που αντιστοιχεί σε ένα στιγμιότυπο, για να βρούμε τον αριθμό που αντιστοιχεί στην επόμενη λέξη πρέπει να αλλάξουμε στον αριθμό $\mathsf{ctn}(x)$ τη δύναμη του $\mathsf{ctp}(x)$-οστού πρώτου από $\mathsf{cts}(x) + 1$ σε $\mathsf{nts}(x) + 1$. Αυτό μπορούμε να το κάνουμε διαιρώντας τον $\mathsf{ctn}(x)$ με $\mathsf{pn}(\mathsf{ctp}(x))^{\mathsf{cts}(x)+1}$ και πολλαπλασιάζοντας τον με $\mathsf{pn}(\mathsf{ctp}(x))^{\mathsf{nts}(x)+1}$ (pn είναι η συνάρτηση του Παραδείγματος 2.2.5). Ορίζουμε λοιπόν τη συνάρτηση $\mathsf{ntn} : \mathbb{N} \to \mathbb{N}$ με:

$$\mathsf{ntn}(x) = \begin{cases} \mathsf{replace}(\mathsf{ctn}(x), \mathsf{ctp}(x), \mathsf{nts}(x)) & , \text{ αν } \mathsf{pn}(\mathsf{ctp}(x)) \mid \mathsf{ctn}(x) \\ \mathsf{add}(\mathsf{ctn}(x), \mathsf{nts}(x)) & , \text{ αλλιώς } ^{2} \end{cases}$$

που επιστρέφει την αριθμητικοποίηση της επόμενης λέξης στην ταινία (qt είναι η συνάρτηση του Παραδείγματος 2.1.25).

Τώρα είμαστε σε θέση να ορίσουμε τη συνάρτηση tr_M. Η tr_M είναι η λύση των εξισώσεων:

$$\begin{cases} f(x, 0) = \langle \triangleright \, q_0 \underbrace{1 \cdots 1}_{x+1 \text{ φορές}} \rangle_{\mathbb{N}} \\ f(x, t+1) = \mathsf{enc}_3(\mathsf{ns}(f(x,t)), \mathsf{ntp}(f(x,t)), \mathsf{ntn}(f(x,t))) \end{cases}$$

Οι συναρτήσεις cs, ctp, ctn, cts και ns, ntp, nts, ntn είναι όλες πρωτογενώς αναδρομικές, άρα και η tr_M είναι πρωτογενώς αναδρομική.

[1] Εδώ γίνεται εμφανής ο λόγος που αντιστοιχήσαμε το A το 0 και το Δ στο 2.

[2] Δηλαδή όταν επισκεπτόμαστε κελί της ταινίας που δεν έχουμε προσεγγίσει στο παρελθόν.

Στάδιο 3: Παρατηρήστε ότι αν η M με είσοδο $x \in \mathbb{N}$ τερματίσει σε t-βήματα τότε $\mathsf{tr}_M(x,t') = \mathsf{tr}_M(x,t)$ για κάθε $t' \geq t$. Επιπλέον, αν η $M(x)$ δεν τερματίζει στο βήμα t τότε $\mathsf{tr}_M(x,t+1) \neq \mathsf{tr}_M(x,t)$ [1] . Συνεπώς η συνθήκη που μας δείχνει ότι η $M(x)$ τερμάτισε είναι η ακόλουθη:

Υπάρχει $t_0 \in \mathbb{N}$ τέτοιο ώστε το $\mathsf{tr}_M(x,t)$ να έχει την ίδια τιμή για κάθε $t \geq t_0$.

Από τον τρόπο που ορίσαμε την tr_M, αυτό συμβαίνει άπαξ και δύο συνεχόμενες τιμές της είναι ίσες. Επομένως για να βρούμε το βήμα κατά το οποίο η $M(x)$ τερματίζει (αν φυσικά τερματίζει) πρέπει να βρούμε το ελάχιστο $t \in \mathbb{N}$ για το οποίο $\mathsf{tr}_M(x,t+1) = \mathsf{tr}_M(x,t)$ (αν φυσικά υπάρχει). Ορίζουμε λοιπόν την ελαχιστικά αναδρομική συνάρτηση $\mathsf{term} : \mathbb{N} \to \mathbb{N}$ με:

$$\mathsf{term}(x) = (\mu\, t \geq 0)[1 \dot{-} \chi_{=}(\mathsf{tr}_M(x,t+1), \mathsf{tr}_M(x,t)) = 0]$$

που επιστρέφει το (ελάχιστο) πλήθος βημάτων που χρειάζεται η $M(x)$ για να τερματίσει (η $\chi_=$ ορίζεται στο Παράδειγμα 2.1.16).

Στάδιο 4: Τέλος, ορίζουμε:

$$f(x) = \mathsf{length}(\mathsf{ctn}(\mathsf{tr}_M(x, \mathsf{term}(x)))) \dot{-} 2$$

□

Μέσα από την απόδειξη του Θεωρήματος 2.5.1 προκύπτει άμεσα το ακόλουθο Πόρισμα.

Πόρισμα 2.5.2 (Κανονική Μορφή Kleene). Για κάθε ελαχιστικά αναδρομική συνάρτηση $f : \mathbb{N}^m \to \mathbb{N}$, $m \geq 1$, υπάρχουν πρωτογενώς αναδρομικές συναρτήσεις $g : \mathbb{N}^{m+1} \to \mathbb{N}$ και $h : \mathbb{N} \to \mathbb{N}$ τέτοιες ώστε:

$$f(x_1, \cdots, x_m) = h((\mu\, i \geq 0)[g(i, x_1, \dots, x_m) = 0])$$

Η ακόλουθη πρόταση θα μας φανεί χρήσιμη στη συνέχεια.

Παρατήρηση 2.5.3. Υπάρχει ΤΜ $M_{TM \to \mu}$ που δέχεται σαν είσοδο την κωδικοποίηση μίας ΤΜ M και επιστρέφει την κωδικοποίηση [2] της ελαχιστικά αναδρομικής συνάρτησης που υπολογίζει η M.

Ασκήσεις

2.1 (☆☆☆). Δώστε εναλλακτικούς ορισμούς των συναρτήσεων plus, mult, fact, $\dot{-}$, min, max και exp.

[1] Για παράδειγμα η κεφαλή κινείται, συνεπώς $\mathsf{ntp}(\mathsf{tr}_M(x,t)) \neq \mathsf{ctp}(\mathsf{tr}_M(x,t))$ και κατ' επέκταση $\mathsf{tr}_M(x,t+1) \neq \mathsf{tr}_M(x,t)$. Αυτός είναι ο λόγο που στην αρχή θεωρήσαμε ότι η M δεν κολλάει εξαιτίας μη ύπαρξης επόμενου στιγμιότυπου σύμφωνα με τη συνάρτηση μεταβάσεών της.

[2] Ένα παράδειγμα κωδικοποίησης ελαχιστικά αναδρομικών συναρτήσεων δίνεται από το Θεώρημα 3.3.8 στομοποίο θα «αντιστοιχίσουμε» σε κάθε αναδρομική συνάρτηση έναν λ-όρο, μία λέξη δηλαδή στο αλφάβητο $\{x, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, (,), \lambda, .\}$.

2.2 (☆☆☆). Δείξτε ότι όλες οι πρωτογενώς αναδρομικές συναρτήσεις είναι ολικές συναρτήσεις και ότι η κλάση των πρωτογενώς αναδρομικών συναρτήσεων είναι αριθμήσιμη.

2.3 (☆☆☆). Δείξτε ότι για κάθε $m \in \mathbb{N}$ οι συναρτήσεις $\mathsf{min}, \mathsf{max} : \mathbb{N}^m \to \mathbb{N}$, με

$$\mathsf{min}_m = \mathbf{min}\{x_1, \ldots, x_m\} \text{ και } \mathsf{max}_m = \mathbf{max}\{x_1, \ldots, x_m\}$$

είναι πρωτογενώς αναδρομικές.

2.4 (★☆☆). Έστω $\mathsf{g} : \mathbb{N}^2 \to \mathbb{N}$ πρωτογενώς αναδρομική συνάρτηση. Δείξτε ότι οι συναρτήσεις $\mathsf{sum}_\mathsf{g}, \mathsf{prod}_\mathsf{g} : \mathbb{N}^2 \to \mathbb{N}$, με

$$\mathsf{sum}_\mathsf{g}(z, x) = \sum_{i=0}^{z} \mathsf{g}(i, x) \text{ και } \mathsf{prod}_\mathsf{g}(z, x) = \prod_{i=0}^{z} \mathsf{g}(i, x)$$

είναι πρωτογενώς αναδρομικές.

2.5 (☆☆☆). Αποδείξτε τις Προτάσεις 2.1.22, 2.1.19 και 2.1.20.

2.6 (☆☆☆). Έστω $\mathsf{R} \subseteq \mathbb{N}^2$ πρωτογενώς αναδρομική σχέση. Δείξτε ότι οι σχέσεις:

$$\begin{aligned} (\forall y < z)[\mathsf{R}] &= \{x \in \mathbb{N} \mid \text{Για κάθε } y < z \text{ ισχύει ότι} (x, y) \in \mathsf{R}\} \\ (\exists y < z)[\mathsf{R}] &= \{x \in \mathbb{N} \mid \text{Υπάρχει } y < z \text{ για το οποίο ισχύει ότι} (x, y) \in \mathsf{R}\} \end{aligned}$$

είναι πρωτογενώς αναδρομικές.

2.7 (★☆☆). Έστω $\mathsf{R} \subseteq \mathbb{N}^2$ πρωτογενώς αναδρομική σχέση. Δείξτε ότι η συνάρτηση $f : \mathbb{N}^2 \to \mathbb{N}$, με $f(z, x) = (\mu\, i \leq z)[(i, x) \in \mathsf{R}]$ είναι πρωτογενώς αναδρομική.

2.8 (★☆☆). Δείξτε ότι για κάθε $b \in \mathbb{N} \setminus \{0, 1\}$ η συνάρτηση $\mathsf{log}_b : \mathbb{N} \to \mathbb{N}$ με:

$$\mathsf{log}_b(x) = \begin{cases} \mathbf{max}\{n \in \mathbb{N} \mid b^n \mid x\} & , \text{ αν } x > 0 \\ 0 & , \text{ αλλιώς} \end{cases}$$

είναι πρωτογενώς αναδρομική.

2.9 (★☆☆). Αποδείξτε την Πρόταση 2.3.4.

2.10 (★☆☆). *(Αμοιβαία πρωτογενής αναδρομή)* Έστω $\mathsf{g}_1, \mathsf{g}_2 : \mathbb{N} \to \mathbb{N}$ και $\mathsf{h}_1, \mathsf{h}_2 : \mathbb{N}^4 \to \mathbb{N}$ πρωτογενώς αναδρομικές συναρτήσεις. Δείξτε ότι οι $f_1, f_2 : \mathbb{N}^2 \to \mathbb{N}$ που ικανοποιούν τις εξισώσεις:

$$\begin{cases} f_1(0,x) = \mathsf{g}_1(x) \\ f_1(y+1,x) = \mathsf{h}_1(f_1(y,x), f_2(y,x), y, x) \\ f_2(0,x) = \mathsf{g}_2(x) \\ f_2(y+1,x) = \mathsf{h}_2(f_1(y,x), f_2(y,x), y, x) \end{cases}$$

είναι πρωτογενώς αναδρομικές συναρτήσεις.

2.11 (★★★). *(Εμφωλευμένη πρωτογενής αναδρομή)* Έστω συναρτήσεις $g : \mathbb{N} \to \mathbb{N}$, $h : \mathbb{N}^3 \to \mathbb{N}$ και $\tau : \mathbb{N}^2 \to \mathbb{N}$. Δείξτε ότι υπάρχει συνάρτηση που είναι λύση των εξισώσεων:

$$\begin{cases} f(0,y) = g(y) \\ f(x+1,y) = h(f(x,\tau(x,y)), x, y) \end{cases}$$

και ότι αν οι g, h και τ είναι πρωτογενώς αναδρομικές, τότε και η f είναι πρωτογενώς αναδρομική.

2.12 (★★☆). Έστω συναρτήσεις $h : \mathbb{N}^3 \to \mathbb{N}$ και $g_1, g_2 : \mathbb{N} \to \mathbb{N}$. Δείξτε ότι υπάρχει συνάρτηση που είναι λύση των εξισώσεων:

$$\begin{cases} f(0,y) = g_1(y) \\ f(1,y) = g_2(y) \\ f(x+2,y) = h(f(x+1), f(x), y) \end{cases}$$

και ότι αν οι h, g_1, g_2 είναι πρωτογενώς αναδρομικές, τότε και η f είναι πρωτογενώς αναδρομική.

2.13 (★★★). *(Διπλή αναδρομή)* Έστω συναρτήσεις $g : \mathbb{N} \to \mathbb{N}$, $h : \mathbb{N}^2 \to \mathbb{N}$, $\tau : \mathbb{N}^4 \to \mathbb{N}$ και $z \in \mathbb{N}$. Δείξτε ότι υπάρχει συνάρτηση που είναι λύση των εξισώσεων:

$$\begin{cases} f(0,y) = g(y) \\ f(x+1,0) = h(f(x,z), x) \\ f(x+1,y+1) = \tau(f(x+1,y), f(x,z), x, y) \end{cases}$$

και ότι αν οι g, h και τ είναι ελαχιστικά αναδρομικές, τότε και η f είναι ελαχιστικά αναδρομική.

2.14 (☆☆☆). Έστω $\mathsf{h} : \mathbb{N}^m \to \mathbb{N}$ και $\mathsf{g} : \mathbb{N}^{m+1} \to \mathbb{N}$, $m \geq 1$, πρωτογενώς αναδρομικές συναρτήσεις. Ορίστε τη συνάρτηση $f : \mathbb{N}^m \to \mathbb{N}$ με:

$$f(x_1, \dots, x_m) = (\mu\, i \leq \mathsf{h}(x_1, \dots, x_m))[\mathsf{g}(i, x_1, \dots, x_m) = 0]$$

χρησιμοποιώντας τον τελεστή της (μη-φραγμένης) ελαχιστοποίησης.

2.15 (★☆☆). Δείξτε ότι η συνάρτηση $- : \mathbb{N}^2 \to \mathbb{N}$ με:

$$-(x,y) = \begin{cases} x - y & , \text{ αν } x \geq y \\ \perp & , \text{ αλλιώς} \end{cases}$$

είναι ελαχιστικά αναδρομική.

2.16 (★★☆). Δείξτε ότι η συνάρτηση του Ackermann (Σελίδα 73) είναι ελαχιστικά αλλά όχι πρωτογενώς αναδρομική.

2.17 (☆☆☆). Δώστε παράδειγμα ολικής, ελαχιστικά αναδρομικής συνάρτησης, που δεν είναι πρωτογενώς αναδρομική και παίρνει τιμές 0 και 1.

2.18 (★★★). Δώστε παράδειγμα ολικής, ελαχιστικά αναδρομικής συνάρτησης, που δεν είναι πρωτογενώς αναδρομική και παίρνει τιμές 0 και 1, χωρίς να χρησιμοποιήσετε τη συνάρτηση του Ackermann.

2.19 (☆☆☆). Ο Αρχιμήδης σε επιστολή του προς τον Βασιλιά Γέλωντα τον Συρακούσιο, προκειμένου να τον πείσει ότι υπάρχουν φυσικοί αριθμοί μεγαλύτεροι σε μέγεθος από το πλήθος κόκκων άμμου που χρειάζεται για να γεμίσει το σύμπαν (σύμφωνα φυσικά με την τότε αντίληψη για το σύμπαν), εκτίμησε ότι το πλήθος κόκκων που θα χρειαστεί είναι μικρότερο από 10^{63} χρησιμοποιώντας την ακόλουθη συνάρτηση (που ορίζεται με διπλή αναδρομή):

$$\begin{cases} f(0,y) = 1 \\ f(x+1,0) = f(x,a) \\ f(x+1,y+1) = a \cdot f(x+1,y) \end{cases}$$

για $a = 10^8$ που ισοδυναμεί με μία *μυριάδα μυριάδες* (αυτός θεωρείται ο μεγαλύτερος αριθμός για τον οποίο οι αρχαίοι Έλληνες είχαν όνομα). Δείξτε ότι η συνάρτηση αυτή είναι ελαχιστικά αναδρομική.

2.20 (☆☆☆). Δείξτε ότι υπάρχει συνάρτηση $f : \mathbb{N} \to \mathbb{N}$ που δεν είναι ελαχιστικά αναδρομική (δες και Άσκηση 2.2).

2.21 (★☆☆). Συμπληρώστε τις λεπτομέρειες του ευθέως της απόδειξης του Θεωρήματος 2.5.1.

ΚΕΦΑΛΑΙΟ 3

λ-ΛΟΓΙΣΜΟΣ

3.1 Εισαγωγή

Συνεχίζοντας την παρουσίαση των διαφόρων μοντέλων υπολογισμού θα μελετήσουμε τον *λ-λογισμός*, το πρώτο χρονικά μοντέλο που αναπτύχθηκε σε τόσο μεγάλο βαθμό ώστε να δώσει απάντηση στα καίρια ερωτήματα που απασχολούσαν την κοινότητα των λογικών στις αρχές του εικοστού αιώνα. Ο λ-λογισμός εισήχθη στις αρχές του 1930 από τον Alonzo Church ως ένα σύστημα που θα μπορούσε να θεμελιώσει τα μαθηματικά με κεντρικό όργανο την συνάρτηση. Όταν αποδείχθηκε όμως ότι αυτός ο στόχος δεν είναι επιτεύξιμος, ο Church έστρεψε την προσοχή του στον ορισμό της «Υπολογισιμότητας», με απώτερο σκοπό την απάντηση του Entscheidungsproblem που είχε θέσει ο David Hilbert.

Στον μετέπειτα «αγώνα» για την επικράτηση ενός μοντέλου υπολογισμού, δηλαδή τυπικής προσέγγισης της έννοιας του αλγορίθμου, παρόλο που σε κάθε βασικό σταθμό ο λ-λογισμός έφτασε πρώτος μπροστά από της μηχανές Turing, τελικά τερμάτισε πίσω από αυτές. Ο λόγος φυσικά είναι ότι η μηχανές Turing αποτελούσαν μια καλή αποτύπωση στο χαρτί ενός υποτυπώδους ηλεκτρονικού υπολογιστή και ως εκ τούτου, όταν τελικά η Θεωρία Υπολογισμού αυτονομήθηκε από τη Λογική, κρίθηκαν διαισθητικότερες των *λ-όρων*. Όμως στο πεδίο στο οποίο ο λ-λογισμός αναμφισβήτητα επικρατεί είναι ο λεγόμενος *Συναρτησιακός Προγραμματισμός*, δηλαδή η αποκλειστική χρήση συναρτήσεων για τον υπολογισμό.

Σκοπός του κεφαλαίου αυτού είναι να αποκαλύψουμε μέσω του λ-λογισμού την πραγματική διάσταση της έννοιας της συνάρτηση. Ας ξεκινήσουμε λοιπόν με μια «φιλοσοφική» συζήτηση περί συναρτήσεων.

3.1.1 Περί συναρτήσεων

Στο Κεφάλαιο 0 δώσαμε τον συνολοθεωρητικό ορισμό της συνάρτησης. Στα υπόλοιπα κεφάλαια προσπαθήσαμε να δώσουμε ισοδύναμους αλλά εντελώς διαφορετικούς ορισμούς της κλάσης των υπολογίσιμων συναρτήσεων. Αυτό που δεν κάναμε σαφές τότε είναι ότι έχει

εξίσου μεγάλη σημασία ο τρόπος με τον οποίο υπολογίζεται μία συνάρτηση, ο αλγόριθμος δηλαδή που την υπολογίζει (είτε αυτός είναι μία ΤΜ είτε ο ορισμός της ως αναδρομική συνάρτηση). Για παράδειγμα οι συναρτήσεις $f : \mathbb{N} \to \mathbb{N}$ με $f(x) = 2x$ και $g : \mathbb{N} \to \mathbb{N}$ με $g(x) = x + x$ σύμφωνα με τον Ορισμό 0.1.9 αποτελούν την «ίδια» συνάρτηση, καθώς σαν σύνολα είναι ίσα, όμως ακολουθώντας τον Ορισμό 2.1.1 την πρώτη θα την ορίζαμε ως $f(x) = \mathsf{mult}(\mathsf{c}_2^1(x), x)$ ενώ τη δεύτερη ως $g(x) = \mathsf{plus}(x, x)$. Ο λόγος που αυτές οι δύο συναρτήσεις διαφέρουν υπό το πρίσμα της Θεωρίας Αναδρομής είναι ότι διαφέρει ο αλγόριθμος που τις υπολογίζει. Αυτή η διάκριση για το μεγαλύτερο κομμάτι των Θεωρητικών Μαθηματικών δεν έχει καμία απολύτως σημασία, στο κομμάτι όμως των Υπολογιστικών Μαθηματικών έχει κεντρικό ρόλο, κυρίως όταν βάλουμε στην εξίσωση και την «αποδοτικότητα» του υπολογισμού μίας συνάρτησης. Μία ενδεικτική περίπτωση είναι η συνάρτηση fib που είδαμε στο Παράδειγμα 2.3.7, όπου ο αναδρομικός αλγόριθμος που εφαρμόζει τυφλά τον τύπο $f(n) = f(n-1) + f(n-2)$ χρειάζεται πολύ παραπάνω «χρόνο» από τον αλγόριθμο που υπολογίζει τις τιμές $f(0), f(1), \ldots, f(n)$ χρησιμοποιώντας τις ήδη υπολογισμένες τιμές (ο αλγόριθμος του Παραδείγματος 2.3.7 δηλαδή).

Ένα ακόμα σημείο όπου ο συνολοθεωρητικός ορισμός δεν επαρκεί για τους σκοπούς μας είναι το γεγονός ότι δεν μας επιτρέπει να έχουμε συναρτήσεις που έχουν ως είσοδο άλλες συναρτήσεις. Φυσικά κάποιος θα προβάλει τον ορισμό της σύνθεσης συναρτήσεων (Ορισμός 0.1.14) και θα ισχυριστεί ότι μπορεί υπό περιπτώσεις να λύσει αυτό το πρόβλημα. Η σύνθεση όμως δεν μπορεί να μας επιτρέψει να έχουμε συναρτήσεις που έχουν σαν είσοδο τον ίδιο τους τον εαυτό! Στην Πληροφορική το φαινόμενο της *αυτοεφαρμογής* είναι αρκετά σύνηθες και ο λόγος που είναι εφικτό είναι ότι οι συναρτήσεις αντιμετωπίζονταν σαν κανόνες υπολογισμού (ή αλγόριθμοι αν προτιμάτε). Συνεπώς όταν μια συνάρτηση δέχεται σαν είσοδο τον εαυτό της στην ουσία έχουμε μία επαναληπτική εκτέλεση των κανόνων υπολογισμού της.

Το γεγονός ότι στον λ-λογισμό μπορούμε να έχουμε συναρτήσεις που δέχονται ως είσοδο άλλες συναρτήσεις μας δίνει το δικαίωμα να επικεντρωθούμε αποκλειστικά σε συναρτήσεις μίας μεταβλητής. Ο τρόπος που το κάνουμε αυτό είναι ο εξής: Όταν θέλουμε να ορίσουμε μια συνάρτηση n μεταβλητών ορίζουμε μία συνάρτηση μίας μεταβλητής στην οποία έπειτα θα δώσουμε ως είσοδο μία συνάρτηση με $n-1$ μεταβλητές. Θα επανέλθουμε σε αυτό το θέμα με μεγαλήτερη λεπτομέρεια όταν θα έχουμε δει το συντακτικό του λ-λογισμού [1].

3.1.2 Περί συμβολισμού

Στον λ-λογισμός ο συμβολισμός έχει κυρίαρχο ρόλο. Παρόλο που οι λ-όροι ενδεχομένως δείχνουν αρκετά περίπλοκοι, ο ορισμός τους βασίζεται σε τρεις πολύ απλές ιδέες:

1. *Εφαρμογή*
2. *Αφαίρεση*
3. *Συστολή*

Ας θεωρήσουμε μία συνάρτηση φυσικών αριθμών, παραδείγματος χάρη την $f(x) = x^2$. Μας ενδιαφέρει η τιμή που έχει η f για κάποιον συγκεκριμένο αριθμό, ας υποθέσουμε

[1] Η ιδέα αυτή στη βιβλιογραφία συναντάται ως *Currying*, προς τιμήν του *Haskell Curry* που την έκανε δημοφιλή.

τον αριθμό 3. Η συνήθης γραφή αυτής της *εφαρμογής* της f πάνω στον αριθμό 3 είναι $f(3)$. Στους λ-όρους για να συμβολίσουμε την εφαρμογή αυτή απλά θα μεταφέρουμε τις παρενθέσεις γράφοντας $(f3)$. Εδώ θα πρέπει να τονίσουμε ότι η εφαρμογή γίνεται μόνο μεταξύ δύο λ-όρων [1], ως εκ τούτου θα πρέπει να ορίσουμε τους φυσικούς αριθμούς ως λ-όρους (ως συναρτήσεις δηλαδή, Ορισμός 3.3.2).

Ας υποθέσουμε τώρα ότι θέλουμε να εκφράσουμε τις συναρτήσεις $f(x) = x + y$ και $g(y) = x + y$, όπου η x για την f και η y για την g αποτελούν *ελεύθερες μεταβλητές*. Ο Church εισήγαγε έναν τρόπο που μας επιτρέπει να συμβολίσουμε τις δύο συναρτήσεις χωρίς να χρειαζόμαστε δύο διαφορετικά ονόματα για να τις ξεχωρίσουμε: Την πρώτη τη συμβόλισε ως $\lambda x.(x+y)$ και τη δεύτερη ως $\lambda y.(x+y)$. Η *λ-αφαίρεση* χρησιμοποιείται για να υποδηλώσει αυτό που συνήθως αποκαλούμε «μεταβλητή» της συνάρτησης. Η πιο σημαντική χρήση όμως της λ-αφαίρεσης είναι ότι μας δείχνει τη θέση μέσα στον λ-όρο που θα γίνει η εφαρμογή κατά τον υπολογισμό της τιμής της συνάρτησης. Ο υπολογισμός αυτός γίνεται σε συμβολικό επίπεδο μέσω μιας ακολουθίας αντικαταστάσεων μεταβλητών με λ-όρους. Αυτές οι αντικαταστάσεις αποκαλούνται *β-συστολές*.

Ας δούμε ένα παράδειγμα. Θεωρήστε τον όρο $\lambda x.M$ και υποθέστε ότι θέλουμε να τον εφαρμόσουμε στον όρο N. Η εφαρμογή γίνεται μέσω της β-συστολής ως εξής [2]:

$$(\lambda x.M)N \rightarrow_\beta M[x/N]$$

όπου με $M[x/N]$ συμβολίσουμε τον όρο που προκύπτει μετά από την αντικατάσταση κάθε «ελεύθερης» εμφάνισης της x με τον όρο N.

Η συστολή λοιπόν είναι ο συνδετικός κρίκος μεταξύ της αφαίρεσης και της εφαρμογής και βάση αυτής υλοποιείται ο υπολογισμός, ή πιο σωστά η *αποτίμηση*. Όταν πλέον δεν είναι δυνατόν να εφαρμοστούν β-συστολές (έχουμε φτάσει σε μία *κανονική μορφή*) ο υπολογισμός-αποτίμηση έχει ολοκληρωθεί και έτσι έχουμε πάρει τη ζητούμενη τιμή.

Θα πρέπει να αναφέρουμε ξανά για να γίνει σαφές ότι η αποτίμηση γίνεται σε καθαρά συμβολικό επίπεδο (κάνουμε απλή *συντακτική αντικατάσταση*) και δεν έχουμε δικαίωμα να απλοποιούμε τους όρους καθ' οιονδήποτε τρόπο. Για παράδειγμα ο όρος $\lambda x.(x + x)$ δεν θα είναι δυνατό να «απλοποιηθεί» στον όρο $\lambda x.2x$. Ο λόγος είναι ότι ο αλγόριθμος υπολογισμού των δύο εκφράσεων ($x + x$ και $2x$) διαφέρει, συνεπώς οι δύο όροι δεν θα πρέπει να ταυτίζονται.

3.2 Συντακτικό λ-λογισμού

Ας περάσουμε στον ορισμό του συστήματος του *Καθαρού λ-λογισμού* (η *λ-λογισμού χωρίς τύπους* [3]). Θα χρησιμοποιήσουμε ένα αριθμήσιμο πλήθος μεταβλητών: $x_0, x_1, ...$

[1] Ακόμα και του ίδιου λ-όρου, π.χ. (ff).

[2] Παραλείπουμε τις εξωτερικές παρενθέσεις της εφαρμογής χάριν απλότητας.

[3] Στον *λ-λογισμό με τύπους* οι μεταβλητές (και κατ' επέκταση οι όροι) ανήκουν σε κάποιον τύπο ούτως ώστε να «απαγορεύονται» εφαρμογές όποτε οι τύποι δεν «ταιριάζουν». Αυτό μας γλιτώνει από πολλές «δυσάρεστες καταστάσεις» που μπορεί να προκύψουν με την αυτοεφαρμογή ενός όρου. Θα πρέπει να διευκρινίσουμε όμως εδώ ότι η αυτοεφαρμογή δίνει στον λ-λογισμό (ως υπολογιστικό μοντέλο) την ισχύ που έχουν π.χ. οι TM ή οι αναδρομικές συναρτήσεις.

Ορισμός 3.2.1. Το σύνολο των *λ-ορών* ορίζεται αναδρομικά ως εξής:

1. Οι μεταβλητές είναι λ-όροι.
2. Αν οι M, N είναι λ-όροι τότε και το (MN) είναι λ-όρος που αποκαλείται *όρος της εφαρμογής (του M στον N).*
3. Αν ο M είναι λ-όρος και η x μεταβλητή τότε και το $(\lambda x.M)$ είναι όρος που αποκαλείται *όρος της λ-αφαίρεσης.*

Παράδειγμα 3.2.2. Αν τα x, y είναι μεταβλητές τότε οι ακόλουθες εκφράσεις είναι λ-όροι:

- $(\lambda x.x)$ *(ταυτοτική συνάρτηση)*
- $(\lambda y.x)$ *(σταθερή συνάρτηση)*
- $(\lambda x.(xx))$ *(συνδυαστής ω)*
- $((\lambda x.(xx))(\lambda x.(xx)))$ *(συνδυαστής Ω)*

Παρατηρήστε ότι στον τελευταίο όρο έχουμε αυτοεφαρμογή.

Θα χρησιμοποιούμε τα μικρά γράμματα x, y, z κ.λπ. για τις μεταβλητές και τα κεφαλαία F, M, N κ.λπ. για τους όρους. Όπως είναι κατανοητό για να απλοποιήσουμε λίγο τους όρους θα χρειαστεί να καταργήσουμε κάποιες παρενθέσεις.

Συμβολισμός 3.2.3. Αν έχουμε όρο της μορφής $(\cdots((FM_1)M_2)\cdots M_n)$ θα τον συμπτύξουμε στην έκφραση $FM_1M_2\cdots M_n$. Αν έχουμε όρο της μορφής $(\lambda x_1.(\lambda x_2.(\cdots(\lambda x_n.M)\cdots))$ θα τον συμπτύξουμε στην έκφραση $\lambda x_1x_2\cdots x_n.M$. Τέλος η εφαρμογή θα έχει προτεραιότητα έναντι της λ-αφαίρεσης, έτσι θα μπορούμε να γράφουμε τον όρο $\lambda x.(MN)$ ως $\lambda x.MN$.

Παράδειγμα 3.2.4. Οι όροι του Παραδείγματος 3.2.2 μπορούν να απλοποιηθούν ως ακολούθως: $\lambda x.x$, $\lambda y.x$, $\lambda x.xx$, $(\lambda x.xx)\lambda x.xx$.

Αναφέρθηκε πριν επιγραμματικά ότι κατά τη διαδικασία της συστολής γίνεται συντακτική αντικατάσταση των ελεύθερων μεταβλητών με κάποιους όρους. Το σύνολο των ελεύθερων μεταβλητών καθορίζεται στον ακόλουθο ορισμό.

Ορισμός 3.2.5. Για έναν όρο M ορίζουμε το σύνολο των *ελεύθερων μεταβλητών* του, συμβολισμός $FV(M)$, και το σύνολο των *δεσμευμένων μεταβλητών* του, συμβολισμός $BV(M)$, αναδρομικά ως εξής:

1. Αν $M = x$ [1], όπου x μεταβλητή, τότε $FV(M) = \{x\}$ και $BV(M) = \varnothing$.
2. Αν $M = (PQ)$, όπου P, Q όροι, τότε $FV(M) = FV(P) \cup FV(Q)$ και $BV(M) = BV(P) \cup BV(Q)$.
3. Αν $M = (\lambda x.N)$, όπου x μεταβλητή και N όρος, τότε $FV(M) = FV(N) \setminus \{x\}$ και $BV(M) = BV(N) \cup \{x\}$.

[1] Να τονίσουμε ότι το σύμβολο $=$ υποδουλώνει συντακτική ισότητα.

Παράδειγμα 3.2.6. Για τον όρο $M = (\lambda x.xy)xy$ έχουμε $FV(M) = \{x, y\}$ και $BV(M) = \{x\}$.

Το φαινόμενο που παρατηρήσαμε στο προηγούμενο παράδειγμα, τα σύνολα δηλαδή των ελεύθερων και δεσμευμένων μεταβλητών να έχουν μη κενή τομή, καλό θα ήταν να αποφευχθεί για λόγους σαφήνειας. Γι' αυτό θα θεωρούμε πάντα ότι τα ονόματα των δεσμευμένων μεταβλητών διαφέρουν από τα ονόματα των ελευθέρων. Αυτό μπορεί να φαίνεται κάπως αυθαίρετο, όμως όπως θα δούμε ευθύς αμέσως σημασία δεν έχει το όνομα μίας δεσμευμένης μεταβλητής αλλά η θέση της μέσα στον όρο. Για παράδειγμα οι όροι $\lambda x.xy$ και $\lambda z.zy$ πρέπει να θεωρούνται ισοδύναμοι καθώς η εφαρμογή τους στον ίδιο όρο θα μας οδηγήσει μέσω της β-συστολής ακριβώς στον ίδιο όρο (υποδηλώνουν ακριβώς τον ίδιο αλγόριθμο). Θα μπορούσαμε να αντιμετωπίσουμε αυτό το «πρόβλημα» και τυπικότερα [1] αλλά αυτό ξεφεύγει των σκοπών μας.

Ορισμός 3.2.7. Ένας όρος M με $FV(M) = \varnothing$ καλείται *κλειστός όρος ή συνδυαστής*.

Στο Παράδειγμα 3.2.2 είδαμε τους συνδυαστές ω και Ω. Αργότερα θα συναντήσουμε και άλλους γνωστούς συνδυαστές.

Ορισμός 3.2.8. Για κάθε όρους M, N και μεταβλητή x με $M[x/N]$ συμβολίζουμε τον όρο που προκύπτει με *αντικατάσταση* της x (στις ελεύθερες εμφανίσεις της) από τον N. Τυπικά ο όρος $M[x/N]$ ορίζεται αναδρομικά ως εξής:

1. Αν $M = x$ τότε $M[x/N] = N$.
2. Αν $M = y$, όπου y μεταβλητή διαφορετική της x, τότε $M[x/N] = y$.
3. Αν $M = (PQ)$, όπου P, Q όροι, τότε $M[x/N] = (P[x/N]Q[x/N])$.
4. Αν $M = (\lambda x.P)$, όπου P όρος, τότε $M[x/N] = (\lambda x.P)$.
5. Αν $M = (\lambda y.P)$, όπου y μεταβλητή διαφορετική της x και P όρος, τότε $M[x/N] = (\lambda y.P[x/N])$.

Για οικονομία χώρου, καθώς η αντικατάσταση είναι μία στοιχειώδης διαδικασία, θα μελετήσουμε ένα μόνο παράδειγμα. Η επιλογή όμως του παραδείγματος δεν είναι τυχαία γιατί όπως θα δούμε σε αυτήν την περίπτωση η αντικατάσταση είναι «προβληματική».

Παράδειγμα 3.2.9. Παρατηρήστε ότι αν x, y, z μεταβλητές τότε $(\lambda x.y)[y/z] = \lambda x.z$ (η σταθερή συνάρτηση) ενώ $(\lambda z.y)[y/z] = \lambda z.z$ (η ταυτοτική συνάρτηση). Συνεπώς κάνοντας την ίδια αντικατάσταση σε δύο όρους όπου σύμφωνα με όσα αναφέραμε πριν θα πρέπει να θεωρούνται ταυτόσημοι προκύπτουν δύο διαφορετικοί όροι. Ο τρόπος να το αποφύγουμε αυτό είναι ξανά η μετονομασία των δεσμευμένων μεταβλητών [2]: Προτού εφαρμόσουμε την αντικατάσταση θα αλλάξουμε στον δεύτερο όρο το όνομα της δεσμευμένης μεταβλητής z π.χ. σε x.Έτσι η αντικατάσταση θα μας οδηγήσει στον ίδιο όρο [3].

[1] Ο φιλομαθής αναγνώστης μπορεί να ψάξει τους όρους α-conversion ή α-equivalence στη βιβλιογραφία.

[2] Ούτε εδώ θα προβούμε σε τυπικότερη ανάλυση. Δείτε σχετική προηγούμενη υποσημείωση.

[3] Δεν είναι απαραίτητο να μετονομάσουμε τη z σε x. Θα μπορούσαμε να χρησιμοποιήσουμε οποιαδήποτε άλλη μεταβλητή που δεν εμφανίζεται ελεύθερη στον όρο z.

Ο λόγος που στο προηγούμενο παράδειγμα χρειάστηκε να προσθέσουμε παρενθέσεις στον όρο $\lambda x.y$ είναι ότι η αντικατάσταση έχει προτεραιότητα έναντι της αφαίρεσης και της εφαρμογής. Για παράδειγμα ο όρος $\lambda x.x[x/y]$ είναι ο όρος $\lambda x.y$ και όχι ο όρος $\lambda x.x$.

Ας έλθουμε τώρα στην ουσία του συμβολισμού και πώς αυτός φέρει εις πέρας τον υπολογισμό της συνάρτησης. Μπορούμε να φανταστούμε έναν όρο της μορφής $(\lambda x.M)N$ ως εφαρμογή της συνάρτησης που αναπαριστά ο όρος $\lambda x.M$ (όπου μεταβλητή είναι η x) πάνω στον όρο N. Η εφαρμογή αυτή στον λ-λογισμό υλοποιείται μέσω της αντικατάστασης $M[x/N]$.

Ορισμός 3.2.10. Κάθε όρος της μορφής $(\lambda x.M)N$ καλείται *β-redex*, ενώ ο όρος $M[x/N]$ καλείται *contractum* [1]. Ορίζουμε τη σχέση της *β-συστολής* μεταξύ δύο όρων M, N, συμβολισμός $M \to_\beta N$, αναδρομικά ως εξής:

1. Αν $M = x$, όπου x μεταβλητή, τότε δεν υπάρχει όρος N τέτοιος ώστε $M \to_\beta N$.
2. Αν $M = (PQ)$, όπου P, Q όροι, τότε $M \to_\beta N$ ανν
   - $N = (P'Q)$ και $P \to_\beta P'$ ή
   - $N = (PQ')$ και $Q \to_\beta Q'$ ή
   - $P = (\lambda x.R)$, όπου x μεταβλητή και R όρος, και $N = R[x/Q]$.
3. Αν $M = (\lambda x.P)$, όπου x μεταβλητή και P όρος, τότε $M \to_\beta N$ ανν $N = (\lambda x.P')$ και $P \to_\beta P'$.

Τέλος, η μεταβατική και ανακλαστική κλειστότητα της σχέσης $\to_\beta$ καλείται *β-αναγωγή* και συμβολίζεται με $\to_\beta^*$.

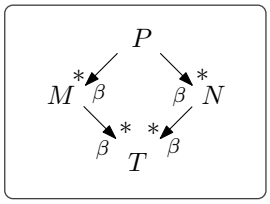
Αν θέλαμε να απλοποιήσουμε λίγο τον παραπάνω ορισμό θα λέγαμε επιγραμματικά ότι $M \to_\beta N$ ανν μέσα στον M υπάρχει κάποιο β-redex που το αντικαθιστούμε με το contractum του και καταλήγουμε στον όρο N. Επίσης $M \to_\beta^* N$ ανν υπάρχει μία ακολουθία όρων $P_1, P_2, \ldots, P_n$ τέτοια ώστε $M = P_1 \to_\beta P_2 \to_\beta \cdots \to_\beta P_n = N$ ή απλά αν $N = M$.

Παράδειγμα 3.2.11. Έστω M όρος. Τότε:

- $(\lambda x.x)M \to_\beta x[x/M] = M$
- $(\lambda x.y)M \to_\beta y[x/M] = y$
- $(\lambda x.xx)\lambda x.xx \to_\beta (xx)[x/\lambda x.xx] = (\lambda x.xx)\lambda x.xx$

Παρατηρήστε ότι ο συνδυαστής Ω μέσω της β-συστολής μας δίνει τον ίδιο του τον εαυτό. Αυτό αποτελεί μία ένδειξη ότι μπορούν να υπάρξουν άπειρες β-αναγωγές. Ας δούμε ένα ακόμα ενδεικτικό παράδειγμα:

[1] Θα μπορούσαμε να χρησιμοποιήσουμε τους ελληνικούς όρους *β-μειωτέο* και *μειωμένο*, *συνεσταλμένο* ή κάτι αντίστοιχο, όμως ακόμα και στην ελληνική βιβλιογραφία έχουν επικρατήσει οι αγγλικοί-λατινικοί όροι ελλείψει ικανοποιητικής μετάφρασης.



Σχήμα 3.2.1: *Σχηματική αναπαράσταση του Θεωρήματος Church-Rosser.*

- $(\lambda x.xxy)\lambda x.xxy \to_\beta (\lambda x.xxy)(\lambda x.xxy)y \to_\beta (\lambda x.xxy)(\lambda x.xxy)yy \to_\beta \cdots$

Ο υπολογισμός διεξάγεται μέσα από την υλοποίηση της εφαρμογής μιας συνάρτησης πάνω σε μία άλλη. Αυτή η εφαρμογή στη γλώσσα του λ-λογισμού αναπαριστάται μέσω ενός β-redex και υλοποιείται μέσω της β-συστολής. Το αποτέλεσμα της β-συστολής (γνωστό ως contractum) «αξιοποιείται» κατά αντίστοιχο τρόπο και συνεχίζεται ο υπολογισμός. Στις δύο πρώτες περιπτώσεις στο παραπάνω παράδειγμα, αν υποθέσουμε ότι ο όρος M δεν περιέχει μέσα του κάποιο β-redex, οδηγούμαστε σε έναν όρο στον οποίο δεν μπορούμε πλέον να κάνουμε β-συστολή. Σε αυτήν την περίπτωση θεωρούμε ότι ο υπολογισμός ολοκληρώθηκε και το αποτέλεσμά του ήταν η συνάρτηση που αναπαριστά ο τελικός όρος. Στις υπόλοιπες δύο περιπτώσεις οι όροι που δίνει η β-συστολή συνεχώς περιέχουν κάποιο β-redex και έτσι η β-αναγωγή θα είναι άπειρη. Σε αυτές τις περιπτώσεις ο υπολογισμός δεν τερματίζει [1].

Ορισμός 3.2.12. Ένας όρος M *βρίσκεται σε β-κανονική μορφή* ανν δεν υπάρχει όρος N τέτοιος ώστε $M \to_\beta N$. Ισοδύναμα, ο M είναι σε β-κανονική μορφή ανν δεν περιέχει μέσα του (ως *υποόρο*) κάποιο β-redex.

Συνεπώς ο υπολογισμός τερματίζει ανν η β-αναγωγή οδηγήσει σε κάποιον όρο που βρίσκεται σε β-κανονική μορφή.

Όταν ο όρος περιέχει παραπάνω από ένα β-redex μπορούμε να κάνουμε β-συστολή σε οποιοδήποτε από αυτά. Θα ήταν μεγάλη αποτυχία του υπολογιστικού μας μοντέλου αν αυτή η αυθαίρετη επιλογή οδηγούσε σε διαφορετικές κανονικές μορφές.

Παράδειγμα 3.2.13. Στις ακόλουθες β-αναγωγές έχουμε υπογραμμίσει το β-redex που συστέλλουμε:

- $\underline{(\lambda x.(\lambda y.yx)z)x} \to_\beta \underline{(\lambda y.yx)z} \to_\beta zx$
- $(\lambda x.\underline{(\lambda y.yx)z})x \to_\beta \underline{(\lambda x.zx)x} \to_\beta zx$

Η μοναδικότητα της κανονικής μορφής (εφόσον αυτή υπάρχει) προκύπτει από το ακόλουθο Θεώρημα που παραθέτουμε χωρίς απόδειξη.

Θεώρημα 3.2.14 (Θεώρημα Church-Rosser). Έστω όροι P, M, N τέτοιοι ώστε $P \to_\beta^* M$ και $P \to_\beta^* N$. Τότε υπάρχει όρος T τέτοιος ώστε $M \to_\beta^* T$ και $N \to_\beta^* T$ (δες Σχήμα 3.2.1).

[1] Θυμηθείτε ότι ο μη-τερματισμός είναι απαραίτητος για ένα υπολογιστικό μοντέλο αν θέλουμε να έχει την ίδια «ισχύ» με τα υπόλοιπα μοντέλα που μελετήσαμε. Αυτό οφείλεται στις υπολογίσιμες μερικές συναρτήσεις.

Άμεσο είναι το παρακάτω πόρισμα.

Πόρισμα 3.2.15. Έστω όροι P, M, N τέτοιοι ώστε $P \to_\beta^* M$ και $P \to_\beta^* N$ και οι όροι M, N βρίσκονται σε κανονική μορφή. Τότε $M = N$ [1].

Ορισμός 3.2.16. Αν για τους όρους M, N ισχύει ότι $M \to_\beta^* N$ και ο N βρίσκεται σε κανονική μορφή τότε θα λέμε ότι *ο N είναι η κανονική μορφή του M*.

3.3 Ισοδυναμία λ-λογισμού με Αναδρομικές Συναρτήσεις

Θα ξεκινήσουμε βλέποντας πως μπορούμε να αναπαραστήσουμε με λ-όρους συναρτήσεις πολλών μεταβλητών. Θα εξετάσουμε μόνο την περίπτωση όπου έχουμε δύο μεταβλητές [2]. Θεωρήστε μία συνάρτηση $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Για κάθε φιξαρισμένο x ορίζουμε τη συνάρτηση $f_x : \mathbb{N} \to \mathbb{N}$, με $f_x(y) = f(x, y)$. Για να αναπαραστήσουμε την f αρκεί να αναπαραστήσουμε τη συνάρτηση που «στέλνει» τα x στις συναρτήσεις f_x [3]. Χρησιμοποιώντας τον συμβολισμό της λ-αφαίρεσης θα μπορούσαμε να αναπαραστήσουμε την f_x ως $F_x = \lambda y.f(x, y)$ και έπειτα την f ως $F = \lambda x.F_x = \lambda x.(\lambda y.f(x, y))$. Έτσι αν M, N όροι θα έχουμε $FMN = (\lambda x.(\lambda y.f(x, y)))MN \to_\beta (\lambda y.f(M, y))N \to_\beta f(M, N)$. Γενικότερα, θα αναπαριστούμε μία συνάρτηση με $n \geq 2$ μεταβλητές αναδρομικά φιξάροντας κάθε φορά και από μία μεταβλητή.

Παράδειγμα 3.3.1. Ας δούμε πως μπορούμε να αναπαραστήσουμε τις συναρτήσεις $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, με $f(x, y) = x$ και $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, με $g(x, y) = y$. Πρώτα αναπαριστούμε τη συνάρτηση $f_x(y) = x$ με τον όρο $F_x = \lambda y.x$ και έπειτα την f με τον όρο $F = \lambda x.F_x = \lambda x.(\lambda y.x)$. Αντίστοιχα θα αναπαραστήσουμε την g με τον όρο $G = \lambda x.(\lambda y.y)$.

Ορισμός 3.3.2. Για κάθε $n \in \mathbb{N}$ ορίζουμε τους συνδυαστές c_n ως εξής:

$$\begin{aligned} c_0 &= \lambda fx.x \\ c_1 &= \lambda fx.fx \\ &\vdots \\ c_n &= \lambda fx.f^n(x) \end{aligned}$$

όπου με $f^n(x)$ συμβολίζουμε τον όρο $\underbrace{f(f(\cdots(fx)\cdots))}_{n \text{ φορές}}$.

Οι συνδυαστές αυτοί αναφέρονται συχνά στη βιβλιογραφία ως *αριθμοί του Church (Church Numerals)* και χρησιμοποιούνται για να αναπαραστήσουμε τους φυσικούς αριθμούς. Παρατηρήστε ότι οι αριθμοί του Church βρίσκονται σε β-κανονική μορφή. Ο λόγος που επιλέξαμε να αναπαραστήσουμε τους φυσικούς αριθμούς κατά αυτόν τον τρόπο φαίνεται στο ακόλουθο παράδειγμα.

[1] Τυπικά οι δύο όροι δεν είναι απαραίτητο ότι θα ταυτίζονται. Υπάρχει το ενδεχόμενο κάποιες δεσμευμένες μεταβλητές να έχουν διαφορετικό όνομα.

[2] Για $n > 2$ μεταβλητές δουλεύουμε αναλόγως.

[3] Ορίζουμε δηλαδή την f ως συνάρτηση $f : \mathbb{N} \to (\mathbb{N} \to \mathbb{N})$, όπου $\mathbb{N} \to \mathbb{N}$ το σύνολο των συναρτήσεων από το $\mathbb{N}$ στο $\mathbb{N}$.

Παράδειγμα 3.3.3. Έστω F λ-όρος και z μεταβλητή τότε:

$$c_n F z = (\lambda f x.f^n(x))Fz \to_\beta (\lambda x.F^n(x))z \to_\beta F^n(z)$$

και, καθώς ο συμβολισμός $F^n(z)$ υποδουλώνει n εφαρμογές του συνδυαστή F πάνω στη z, ο συνδυαστής c_n στην ουσία εφαρμόζει επαναληπτικά τη συνάρτηση που αναπαριστά ο F πάνω στο αρχικό όρισμα z.

Ορισμός 3.3.4. Μία συνάρτηση $f : \mathbb{N}^m \to \mathbb{N}$ καλείται *λ-ορίσιμη* ανν υπάρχει λ-όρος F τέτοιος ώστε για κάθε $n_1, n_2, \dots, n_m \in \mathbb{N}$:

1. Αν $f(n_1, n_2, \dots, n_m) \neq \perp$ τότε $Fc_{n_1}c_{n_2}\cdots c_{n_m} \to^*_\beta c_{f(n_1,n_2,\_,n_m)}$.
2. Αν $f(n_1, n_2, \dots, n_m) = \perp$ τότε ο $Fc_{n_1}c_{n_2}\cdots c_{n_m}$ δεν ανάγεται σε όρο που είναι σε κανονική μορφή (η β-αναγωγή είναι άπειρη).

Σκοπός αυτής της παραγράφου είναι να δείξουμε ότι οι κλάσεις των αναδρομικών συναρτήσεων και των λ-ορίσιμων συναρτήσεων ταυτίζονται. Όπως φαντάζεσθε θα χρειαστεί να κάνουμε πρώτα κάποια προετοιμασία.

Παράδειγμα 3.3.5. Ας εξετάσουμε μερικές αριθμητικές συναρτήσεις που συναντήσαμε στο Κεφάλαιο 2:

- Η $\mathsf{z}^1(n) = 0$ ορίζεται από τον όρο $Z = \lambda x.c_0$, καθώς για κάθε $n \in N$ ισχύει ότι:

$$Zc_n = (\lambda x.c_0)c_n \to_\beta c_0$$

- Η $\mathsf{s}(n) = n + 1$ ορίζεται από τον όρο $S = \lambda xyz.y(xyz)$, καθώς για κάθε $n \in N$ ισχύει ότι:

$$Sc_n = (\lambda xyz.y(xyz))c_n \to_\beta \lambda yz.y(c_n yz) \to^*_\beta \lambda yz.y(y^n(z)) = \lambda yz.y^{n+1}(z) = c_{n+1}$$

- Η συνάρτηση $\mathsf{plus}(m, n) = m + n$ ορίζεται από τον όρο $F_+ = \lambda xypq.xp(ypq)$, καθώς για κάθε $m, n \in \mathbb{N}$ ισχύει ότι:

$$\begin{aligned} F_+c_mc_n &= (\lambda xypq.xp(ypq))c_mc_n \\ &\to_\beta (\lambda ypq.c_mp(ypq))c_n \\ &\to_\beta \lambda pq.c_mp(c_npq) \\ &\to^*_\beta \lambda pq.p^m(p^n(q)) \\ &= \lambda pq.p^{m+n}(q) \\ &= c_{m+n} \end{aligned}$$

Στη συνέχεια θα χρειαστεί να αναπαραστήσουμε ζεύγη λ-όρων και να ορίσουμε συναρτήσεις που προβάλουν το ζεύγος στην πρώτη ή στη δεύτερη μεταβλητή.

Ορισμός 3.3.6. Έστω M, N όροι. Ορίζουμε τους ακόλουθους συνδυαστές:

$$\begin{aligned} \langle M,N\rangle &= \lambda z.zMN \text{ (Συδυαστής ζεύγους)} \\ True &= \lambda xy.x \text{ (Αληθής αληθοτιμή)} \\ False &= \lambda xy.y \text{ (Ψευδής αληθοτιμή)} \end{aligned}$$

Παρατηρήστε ότι:

$$\langle M,N\rangle True = (\lambda z.zMN)\lambda xy.x \to_\beta (\lambda xy.x)MN \to_\beta^* M$$

και αντίστοιχα $\langle M,N\rangle False \to_\beta^* N$. Συνεπώς οι όροι $True, False$ αναπαριστούν τις *προβολές* στις δύο μεταβλητές του ζεύγους. Επιπλέον τον συνδυαστή του ζεύγους μπορούμε να τον χρησιμοποιήσουμε για να εκφράσουμε (το γνωστό μας από την πληροφορική) if-then-else. Για λόγους παραστατικότητας συχνά θα γράφουμε $If(X)\ Then(M)\ Else(N)$ αντί για τον όρο $\langle M,N\rangle X$. Τέλος, ο όρος $False$ ταυτίζεται με τον όρο που έχουμε αντιστοιχίσει στον αριθμό 0.

Παράδειγμα 3.3.7. Θα κατασκευάσουμε έναν συνδυαστή $IsZero$ τέτοιον ώστε:

$$IsZero\ c_n = \begin{cases} True & , \text{ αν } n = 0 \\ False & , \text{αλλιώς} \end{cases}$$

Έστω $IsZero = \langle True\ False, True\rangle$, τότε:

$$IsZero\ c_0 \quad = \quad \langle True\ False, True\rangle False \to_\beta True$$

και για κάθε όρο $n > 0$:

$$\begin{aligned} IsZero\ c_n \quad &= \quad \langle True\ False, True\rangle c_n = (\lambda z.z(True\ False)True)c_n \\ &\to_\beta \quad c_n(True\ False)True = (\lambda fx.f^n(x))(True\ False)True \\ &\to_\beta^* \quad (True\ False)^n(True) = (True\ False)^{n-1}((True\ False)True) \\ &= \quad (True\ False)^{n-1}(((\lambda xy.x)False)True) \\ &\to_\beta^* \quad (True\ False)^{n-1}(False) = (True\ False)^{n-2}((True\ False)False) \\ &\to_\beta^* \quad (True\ False)^{n-2}(False) \\ &\to_\beta \quad \cdots \quad \to_\beta False \end{aligned}$$

Θεώρημα 3.3.8. Μία συνάρτηση $f : \mathbb{N}^m \to \mathbb{N}$ είναι ελαχιστικά αναδρομική ανν είναι λ-ορίσιμη.

Θα μοιράσουμε την απόδειξη του Θεωρήματος 3.3.8 σε μερικά επιμέρους Λήμματα και Προτάσεις.

Λήμμα 3.3.9. Για κάθε $m > 1$ οι συναρτήσεις:

(a) $\mathsf{s}(x) = x + 1$

(b) $\mathsf{z}^m(x_1, \dots, x_m) = 0$

(c) $\mathsf{p}_i^m(x_1, \dots, x_m) = x_i$, όπου $i \in [m]$

είναι λ-ορίσιμες.

Απόδειξη. Παρατηρούμε ότι την s την ορίζει ο όρος S του Παραδείγματος 3.3.5, τις σταθερές μηδενικές συναρτήσεις οι όροι $Z_m = \lambda x_1 \cdots x_m.c_0$, και τις προβολές οι όροι $P_i^m = \lambda x_1 \cdots x_m.x_i$. □

Λήμμα 3.3.10. Έστω ότι οι συναρτήσεις $g : \mathbb{N}^n \to \mathbb{N}$ και $h_i : \mathbb{N}^m \to \mathbb{N}$, $i \in [n]$ είναι λ-ορίσιμες, τότε και η $f(x_1, \dots, x_m) = g(h_1(x_1, \dots, x_m), \dots, h_n(x_1, \dots, x_m))$ είναι λ-ορίσιμη.

Απόδειξη. Αν υποθέσουμε ότι ο όρος G ορίζει την g και οι όροι $H_1, \dots, H_n$ τις $h_1, \dots, h_n$, τότε ο όρος: $F_f = \lambda x_1 \cdots x_m.G(H_1 x_1 \cdots x_m) \cdots (H_n x_1 \cdots x_m)$ ορίζει την f. □

Λήμμα 3.3.11. Έστω λ-ορίσιμες συναρτήσεις $g : \mathbb{N}^{m-1} \to \mathbb{N}$ και $h : \mathbb{N}^{m+1} \to \mathbb{N}$. Η συνάρτηση $f : \mathbb{N}^m \to \mathbb{N}$ που είναι λύση των εξισώσεων:

$$\begin{cases} f(0, x_1, \dots, x_{m-1}) = g(x_1, \dots, x_{m-1}) \\ f(y+1, x_1, \dots, x_{m-1}) = h(f(y, x_1, \dots, x_{m-1}), y, x_1, \dots, x_{m-1}) \end{cases}$$

είναι λ-ορίσιμη.

Απόδειξη. Έστω ότι οι όροι G, H ορίζουν τις συναρτήσεις g, h αντίστοιχα. Θεωρούμε τον όρο:

$$Next = \lambda p.\langle S(pTrue), H(pFalse)(pTrue)x_1 \cdots x_{m-1}\rangle$$

όπου $\langle , \rangle, True, False$ οι συνδυαστές του Ορισμού 3.3.6 [1] και S ο συνδυαστής του Παραδείγματος 3.3.5. Παρατηρήστε ότι αν y μεταβλητή και M όρος τότε:

$$Next\langle y, M\rangle \to_\beta^* \langle Sy, HMyx_1 \cdots x_{m-1}\rangle$$

Συνεπώς, αν ο M αντιστοιχεί στην τιμή $f(y, x_1, \dots, x_{m-1})$ τότε η δεύτερη συντεταγμένη του $Next\langle y, M\rangle$ αντιστοιχεί στην τιμή $f(y+1, x_1, \dots, x_{m-1})$ [2]. Ο όρος:

$$F_f = \lambda y x_1 \cdots x_{m-1}.yNext\langle c_0, Gx_1 \cdots x_{m-1}\rangle False$$

ορίζει την f, καθώς:

$$\begin{aligned} F_f c_y c_{x_1} \cdots c_{x_{m-1}} &\to_\beta^* c_y Next\langle c_o, Gc_{x_1} \cdots c_{c_{x_{m-1}}}\rangle False \\ &\to_\beta Next^y(\langle c_o, Gc_{x_1} \cdots c_{c_{x_{m-1}}}\rangle) False \end{aligned}$$

άρα έχουμε y επαναλήψεις, ξεκινώντας από το ζευγάρι $\langle 0, g(x_1, \dots, x_{m-1})\rangle$, και στο τέλος παίρνουμε τη δεύτερη προβολή, δηλαδή την τιμή $h(f(y, x_1, \dots, x_{m-1}), y, x_1, \dots, x_{m-1})$. □

[1] Θυμηθείτε ότι οι συνδυαστές $True$ και $False$ δρουν σαν την πρώτη και τη δεύτερη προβολή πάνω στον $\langle , \rangle$.

[2] Η πρώτη χρησιμοποιείται για να «σημειώνουμε» τον αριθμό της επανάληψης.

Από τα παραπάνω Λήμματα προκύπτει άμεσα η ακόλουθη πρόταση.

Πρόταση 3.3.12. Κάθε πρωτογενώς αναδρομική συνάρτηση είναι λ-ορίσιμη.

Υπάρχει ένας πιο γενικός τρόπος να ορίσουμε την αναδρομή. Θα χρειαστούμε ένα *Θεώρημα Σταθερού Σημείου*.

Θεώρημα 3.3.13 (Θεώρημα Σταθερού Σημείου)**.** Για κάθε λ-όρο F υπάρχει λ-όρος X τέτοιος ώστε $X \rightarrow_\beta^* FX$. Ο όρος X ονομάζεται *σταθερό σημείο του* F.

Απόδειξη. Θεωρούμε τον συνδυαστή $\Theta = (\lambda xy.y(xxy))\lambda xy.y(xxy)$. Θα δείξουμε ότι:

$$\Theta F \rightarrow_\beta^* F(\Theta F)$$

δηλαδή ο ΘF είναι σταθερό σημείο του F.Έστω $U = \lambda xy.y(xxy)$. Παρατηρούμε ότι:

$$\Theta F = (\lambda xy.y(xxy))UF \rightarrow_\beta^* F(UUF) = F(\Theta F)$$

□

Παρατήρηση 3.3.14. Παρατηρήστε ότι αν θέλουμε να ορίσουμε όρο F τέτοιον ώστε για κάθε όρο X να ισχύει ότι:

$$FX \rightarrow_\beta^* M(X, F)$$

όπου $M(X, F)$ ένας όρος στον οποίο εμφανίζεται ο όρος F (ο F δηλαδή ορίζεται μέσω μιας *αναδρομικής εξίσωσης* και αναπαριστά μια αναδρομική συνάρτηση) τότε αρκεί να ορίσουμε $F = \Theta J$, όπου $J = (\lambda fx.M(x, f))$, καθώς:

$$FX = \Theta JX \rightarrow_\beta^* J(\Theta J)X = JFX = (\lambda fx.M(x, f))FX \rightarrow_\beta^* M(X, F)$$

Λήμμα 3.3.15. Έστω λ-ορίσιμη συνάρτηση $g : \mathbb{N}^{m+1} \rightarrow \mathbb{N}$, $m \geq 1$, τέτοια ώστε για κάθε $i, x_1, \ldots, x_n \in \mathbb{N}$ ισχύει ότι $g(i, x_1, \ldots, x_m) \neq \perp$, τότε η συνάρτηση $f(x_1, \ldots, x_m) = (\mu\ i \geq 0)[g(i, x_1, \ldots, x_m) = 0]$ είναι λ-ορίσιμη.

Απόδειξη. Έστω ότι ο όρος G ορίζει την g. Θεωρούμε τον όρο:

$$M(i, f) = \lambda x_1 \cdots x_m.If(IsZero\ (Gix_1 \cdots x_m))\ Then(i)\ Else(f(Si)x_1 \cdots x_m)$$

όπου $IsZero$ ο συνδυαστής του Παραδείγματος 3.3.7, S ο συνδυαστής του Παραδείγματος 3.3.5 και $If(\ )\ Then(\ )\ Else(\ )$ ο συνδυαστής που υλοποιεί το if-then-else. Τέλος, θεωρούμε τους συνδυαστές:

$$J = \lambda fi.M(i, f) \quad \text{και} \quad F = \Theta J$$

και παρατηρούμε ότι για το πρώτο $i \in \mathbb{N}$ που είναι τέτοιο ώστε $g(i, n_1, \dots, n_m) = 0$:

$$\begin{aligned}
Fc_0c_{n_1}\cdots c_{n_m} &= \Theta J c_0 c_{n_1}\cdots c_{n_m} \\
&\to^*_\beta M(c_0, F)c_{n_1}\cdots c_{n_m} \\
&= (\lambda x_1\cdots x_m.If(IsZero\ (Gc_0x_1\cdots x_m)) \\
&\qquad\qquad Then(c_0)\ Else(F(Sc_0)x_1\cdots x_m))c_{n_1}\cdots c_{n_m} \\
&\to^*_\beta If(IsZero\ (Gc_0c_{n_1}\cdots c_{n_m}))\ Then(c_0)\ Else(F(Sc_0)c_{n_1}\cdots c_{n_m}) \\
&\to^*_\beta If(IsZero\ (Gc_0c_{n_1}\cdots c_{n_m}))\ Then(c_0)\ Else(Fc_1c_{n_1}\cdots c_{n_m}) \\
&\to^{*\ 1}_\beta Fc_1c_{n_1}\cdots c_{n_m} \\
&\ \ \vdots \\
&\to^*_\beta Fc_ic_{n_1}\cdots c_{n_m} \\
&\to^*_\beta If(IsZero\ c_0)\ Then(c_i)\ Else(Fc_{i+1}c_{n_1}\cdots c_{n_m}) \\
&\to^*_\beta c_i
\end{aligned}$$

Φυσικά αν δεν υπάρχει τέτοιο i τότε η β-αναγωγή θα είναι άπειρη. Τέλος, ο όρος που ορίζει την f είναι ο $F_f = Fc_0$. □

Αν συνδυάσουμε το παραπάνω Λήμμα με την Πρόταση 3.3.12 συμπεραίνουμε ότι κάθε ολική ελαχιστικά αναδρομική συνάρτηση είναι λ-ορίσιμη. Τι συμβαίνει όμως με τις μερικές ελαχιστικά αναδρομικές συναρτήσεις; Για να δείξουμε ότι είνα λ-ορίσιμες θα χρησιμοποιήσουμε την Πρόταση 3.3.12, το Λήμμα 3.3.15 και την *κανονική μορφή του Kleene* που είδαμε στο Πόρισμα 2.5.2.

Απόδειξη Θεωρήματος 3.3.8. ($\Rightarrow$) Από το Πόρισμα 2.5.2 προκύπτει ότι υπάρχουν πρωτογενώς αναδρομικές συναρτήσεις $g : \mathbb{N}^{m+1} \to \mathbb{N}$ και $h : \mathbb{N} \to \mathbb{N}$ τέτοιες ώστε $f(x_1, \cdots, x_m) = h((\mu\ i \geq 0)[g(i, x_1, \dots, x_m) = 0])$. Από την Πρόταση 3.3.12 υπάρχουν λ-όροι H, G που ορίζουν τις h, g αντίστοιχα. Τέλος, από το Λήμμα 3.3.10 έπεται ότι η f είναι λ-ορίσιμη [2].

($\Leftarrow$) Η απόδειξη ότι κάθε λ-ορίσιμη συνάρτηση είναι αναδρομική μοιάζει πολύ με την απόδειξη του αντιστρόφου του Θεωρήματος 2.5.1 (για αυτό θα την παραλείψουμε): Ξεκινάμε αντιστοιχίζοντας σε κάθε λ-όρο έναν φυσικό αριθμό. Έπειτα ορίζουμε μια πρωτογενώς αναδρομική συνάρτηση που με όρισμα τον αριθμό του όρου μας δίνει τον αριθμό του όρου που προκύπτει μετά από μία β-συστολή. Τέλος, ορίζουμε ελαχιστική αναδρομική συνάρτηση που με όρισμα τον αριθμό που αντιστοιχεί σε έναν λ-όρο μας επιστρέφει τον αριθμό της κανονικής μορφής του εφόσον αυτή υπάρχει. Αν δεν υπάρχει κανονική μορφή τότε η συνάρτηση δεν ορίζεται. □

[1] Αφού $g(0, x_1, \dots, x_m) \neq 0$ ισχύει ότι $IsZero\ Gc_0c_{n_1}\cdots c_{n_m} \to^*_\beta False$.

[2] Παρατηρήστε ότι καθώς η g είναι πρωτογενώς αναδρομική συνάρτηση θα είναι ολική συνάρτηση. Συνεπώς δεν υπάρχει πρόβλημα στην εφαρμογή του Λήμματος 3.3.15. Αν η f είναι μερική συνάρτηση αυτό θα οφείλετε στο γεγονός ότι δεν θα υπάρχει $i \in \mathbb{N}$ τέτοιο ώστε $g(i, n_1, \dots, n_m) = 0$.

Ασκήσεις

3.1 (★☆☆). (Λήμμα αντικατάστασης) Έστω μεταβλητές x, y, z και λ-όροι M, N, L τέτοιοι ώστε $BV(M) \cap FV(zNL) = \varnothing$. Δείξτε ότι:

- $M[y/L][x/N] = M[x/N][y/L[x/N]]$ αν $y \notin FV(N)$
- $M[y/L][x/N] = M[x/N][y/L]$ αν $y \notin FV(N)$ και $x \notin FV(L)$
- $M[x/L][x/N] = M[x/[L[x/N]]]$

3.2 (★★☆). Έστω λ-όροι M, M', N, N' και μεταβλητή x. Εξετάστε αν ισχύουν τα ακόλουθα:

1. Αν $N \to_\beta N'$ τότε $M[x/N] \to_\beta M[x/N']$.
2. Αν $M \to_\beta^* M'$ και $N \to_\beta^* N'$ τότε $M[x/N] \to_\beta^* M'[x/N']$.

3.3 (★★☆). Βρείτε λ-όρους M, N με την ιδιότητα ότι κανένας τους δεν έχει β-κανονική μορφή αλλά ο λ-όρος MN έχει.

3.4 (★☆☆). Βρείτε λ-όρο που ορίζει τη συνάρτηση $\mathsf{mult}(m, n) = m \cdot n$.

3.5 (★☆☆). Βρείτε λ-όρο που ορίζει τη συνάρτηση $\mathsf{exp}(m, n) = m^n$.

3.6 (★★☆). Βρείτε λ-όρο που ορίζει τη συνάρτηση $\mathsf{fact}(n) = n!$.

3.7 (★★★). Βρείτε λ-όρο που ορίζει τη συνάρτηση $\mathsf{pd}(n) = \begin{cases} 0 & , \text{ αν } n = 0 \\ n-1 & , \text{ αλλιώς} \end{cases}$.

3.8 (★☆☆). Βρείτε λ-όρο που ορίζει τη συνάρτηση $f : \mathbb{N} \to \mathbb{N}$ με $f(x) = \begin{cases} 1 & , \text{ αν } x = 0 \\ \bot & , \text{ αλλιώς} \end{cases}$.

3.9 (★☆☆). Έστω $M_1, \ldots, M_n$, $n \geq 2$ λ-όροι. Ορίστε συνδυαστή $\langle M_1, \ldots, M_n \rangle$ που αναπαριστά τη n-άδα των όρων και συνδυαστή X_i^n τέτοιο ώστε $\langle M_1, \ldots, M_n \rangle X_i^n \to_\beta^* M_i$, για $1 \leq i \leq n$.

3.10 (★★★). Αποδείξτε το Λήμμα 3.3.11 χρησιμοποιώντας το Θεώρημα 3.3.13.

ΚΕΦΑΛΑΙΟ 4

ΓΡΑΜΜΑΤΙΚΕΣ-ΙΕΡΑΡΧΙΑ CHOMSKY

Στα Κεφάλαιο 1 ασχοληθήκαμε αρκετά με τις γλώσσες ενός πεπερασμένου αλφαβήτου. Το ενδιαφέρον μας στράφηκε στο κατά πόσον μπορούμε να αποφανθούμε αν μια λέξη ανήκει σε μία υπό εξέταση γλώσσα. Η ύπαρξη μίας ΤΜ που μπορεί να αναγνωρίσει ή να αποφασίσει μία γλώσσα με λίγη φαντασία μπορεί να ιδωθεί σαν ένας (πεπερασμένος) ορισμός μίας (πιθανώς άπειρης) γλώσσας. Αυτός ο ορισμός μας δίνει περισσότερη πληροφορία από την απλή συνολοθεωρητική περιγραφή της, που στην ουσία απλά μας περιγράφει κάποιες ιδιότητες που έχουν οι λέξεις της: Μας δίνει μία μέθοδο ελέγχου για το «ανήκειν» στη γλώσσα.

Σε αυτό το κεφάλαιο θα παρουσιάσουμε έναν φορμαλισμό, που πάλι δεν είναι «μηχανιστικός» όπως οι ΤΜ, και μπορεί επίσης να χαρακτηρίσει μία γλώσσα. Θα ερευνήσουμε αν υπάρχει ένα πεπερασμένο σύνολο κανόνων που συνδυαζόμενοι μεταξύ τους ένα πεπερασμένο πλήθος φορών, είναι ικανοί να παράξουν οποιαδήποτε λέξη της γλώσσας. Όπως κάνουμε και στις «φυσικές γλώσσες» [1] θα ορίσουμε μία *Γραμματική*, ένα σύνολο κανόνων δηλαδή που διέπει ποιες λέξεις επιτρέπονται και ποιες όχι [2]. Θα δείξουμε ότι οι γλώσσες για τις οποίες υπάρχουν γραμματικές που τις παράγουν (χωρίς περιορισμούς) είναι ακριβώς οι αναδρομικά απαριθμήσιμες γλώσσες. Αργότερα θα θέσουμε περιορισμούς στους κανόνες μίας γραμματικής και έτσι θα ορίσουμε νέες κλάσεις γλωσσών που θα αποτελέσουν τελικά την *Ιεραρχία Chomsky*.

Ως «παράπλευρο αποτέλεσμα» θα δώσουμε μέσα από τον φορμαλισμό των γραμματικών έναν ακόμα ορισμό των υπολογίσιμων συναρτήσεων.

4.1 Γενικές γραμματικές

Ορισμός 4.1.1. *Γενική γραμματική* (ή *γραμματική χωρίς περιορισμούς* ή *γραμματική Τύπου*

[1] Όπως για παράδειγμα στα ελληνικά.

[2] Για παράδειγμα, σύμφωνα με τη γραμματική της ελληνικής γλώσσας, η λέξη «καλλιτέχνης» είναι αποδεκτή ενώ η λέξη «καλητέχνης» επιεικώς απαράδεκτη.

0 ή απλά *γραμματική*) είναι μία τετράδα $G = (V, \Sigma, R, S)$ όπου:

1. V είναι ένα πεπερασμένο αλφάβητο
2. $\Sigma \subseteq V$ είναι το σύνολο των *τερματικών συμβόλων*
3. $V \setminus \Sigma$ είναι το σύνολο των *μη-τερματικών συμβόλων*
4. $S \in V \setminus \Sigma$ είναι το *αρχικό σύμβολο*
5. $R \subseteq V^*(V \setminus \Sigma)V^* \times V^*$ [1] είναι το πεπερασμένο *σύνολο κανόνων παραγωγής*

Συμβολισμός 4.1.2. Έστω γραμματική $G = (V, \Sigma, R, S)$. Αν $(u, v) \in R$ θα γράφουμε $u \to v$ καθώς είναι πιο παραστατικό.

Ένας κανόνας $u \to v \in R$ μας επιτρέπει να μετατρέψουμε τη λέξη u στη λέξη v. Βασική προϋπόθεση όμως (σύμφωνα με το 5. του Ορισμού 4.1.1) είναι η λέξη u να περιέχει κάποιο μη-τερματικό σύμβολο. Τους κανόνες παραγωγής, όπως θα δούμε στον ακόλουθο ορισμό, μπορούμε να τους εφαρμόσουμε σε οποιαδήποτε υπολέξη.

Ορισμός 4.1.3. Έστω γραμματική $G = (V, \Sigma, R, S)$ και $u, v \in V^*$. Ορίζουμε τις σχέσεις $\Rightarrow_G, \Rightarrow_G^* \subseteq V^* \times V^*$ ως εξής:

- $u \Rightarrow_G v$ ανν υπάρχουν $w_1, w_2 \in V^*$ και κανόνας $u' \to v' \in R$ έτσι ώστε $u = w_1 u' w_2$ και $v = w_1 v' w_2$.
- $\Rightarrow_G^*$ είναι η μεταβατική και ανακλαστική κλειστότητα της $\Rightarrow_G$.

Αν $u \Rightarrow_G^* v$ θα λέμε ότι η u *παράγει τη* v *στην* G.

«Αφετηρία» όλων το παραγωγών λέξεων που θα μας απασχολήσουν θα είναι το αρχικό σύμβολο S. Επιπλέον, από όλες τις δυνατές παραγωγές ενδιαφερόμαστε μόνο για αυτές που «καταλήγουν» σε μία λέξη που απαρτίζεται αποκλειστικά από τερματικά σύμβολα. Παρατηρήστε ότι, εφόσον το αριστερό μέρος των κανόνων απαιτεί να υπάρχει στη λέξη που θα μετασχηματίσουμε μη-τερματικό σύμβολο, όταν φτάσουμε σε λέξη που περιέχει μόνο τερματικά σύμβολα η παραγωγή έχει «τελειώσει» (δεν μπορούμε πλέον να εφαρμόσουμε κάποιον κανόνα δηλαδή). Φυσικά υπάρχει η περίπτωση να μην μπορούμε να εφαρμόσουμε κάποιον κανόνα ενώ η τελευταία λέξη της παραγωγής περιέχει μη-τερματικά σύμβολα (η παραγωγή «κολλάει») ή ακόμα μία παραγωγή να συνεχίζεται επ' άπειρον [2].

Σε κάθε γραμματική αντιστοιχούμε μία γλώσσα σύμφωνα με τον ορισμό που ακολουθεί.

Ορισμός 4.1.4. Έστω γραμματική $G = (V, \Sigma, R, S)$. Η γλώσσα που *παράγει η* G είναι η γλώσσα:

$$L(G) = \{w \in \Sigma^* \mid S \Rightarrow_G^* w\}$$ [3]

Αν $w \in L(G)$ θα λέμε ότι η w *παράγεται από την* G.

[1] $V^*(V \setminus \Sigma)V^* = \{w \in V^* \mid \exists w_1, w_2 \in V^* \ \exists a \in V \setminus \Sigma \ (w = w_1 a w_2)\}$

[2] Όπως και στις ΤΜ το πρώτο είδος κολλήματος δεν είναι ουσιαστικό καθώς θα μπορούσε να αποφευχθεί αν προσθέταμε κατάλληλους κανόνες στη γραμματική (π.χ. τους κανόνες $a \to a$ για κάθε σύμβολο $a \in V \setminus \Sigma$).

[3] Προσέξτε ότι η w αποτελείται μόνο από τερματικά σύμβολά του V^*.

Ορισμός 4.1.5. Δύο γραμματικές G_1, G_2 είναι *ισοδύναμες* ανν $L(G_1) = L(G_2)$.

Οι ορισμοί αυτοί θα γίνουν ευκολότερα κατανοητοί μέσω μερικών παραδειγμάτων.

Παράδειγμα 4.1.6. Ας θεωρήσουμε τη γραμματική $G = (V, \Sigma, R, S)$ με $V = \{0, 1, S\}$, $\Sigma = \{0, 1\}$ και $R = \{S \to 0S1, S \to \epsilon\}$ [1]. Μία *παραγωγή από την* G είναι η ακόλουθη:

$$S \Rightarrow_G 0S1 \Rightarrow_G 00S11 \Rightarrow_G 000S111 \Rightarrow_G 000111$$

όπου στις τρεις πρώτες παραγωγές εφαρμόζουμε τον κανόνα $S \to 0S1$ και στην τέταρτη τον κανόνα $S \to \epsilon$. Παρατηρήστε ότι $L(G) = \{0^n 1^n \in \{0,1\}^* \mid n \in \mathbb{N}\}$ [2].

Παράδειγμα 4.1.7. Έστω γραμματική $G = (V, \Sigma, R, S)$ με $V = \{A, B, C, T_a, T_b, T_c, S\} \cup \Sigma$, $\Sigma = \{a, b, c\}$ και

$$\begin{array}{l|l} R = \{S \to ABCS, & CT_c \to T_b c, \\ \quad S \to T_c, & BT_b \to T_b b, \\ \quad CA \to AC, & BT_b \to T_a b, \\ \quad BA \to AB, & AT_a \to T_a a, \\ \quad CB \to BC, & T_a \to \epsilon\} \\ \quad CT_c \to T_c c, & \end{array}$$

Μία *παραγωγή από την* G είναι η ακόλουθη [3]:

$$\begin{aligned}
\underline{S} &\Rightarrow_G && \text{(εφαρμόζουμε τον κανόνα } S \to ABCS) \\
ABC\underline{S} &\Rightarrow_G && \text{(εφαρμόζουμε τον κανόνα } S \to ABCS) \\
ABCABC\underline{S} &\Rightarrow_G && \text{(εφαρμόζουμε τον κανόνα } S \to ABCS) \\
ABCABCABC\underline{S} &\Rightarrow_G && \text{(εφαρμόζουμε τον κανόνα } S \to T_c) \\
AB\underline{CA}BCABCT_c &\Rightarrow_G && \text{(εφαρμόζουμε τον κανόνα } CA \to AC) \\
A\underline{BA}CBCABCT_c &\Rightarrow_G && \text{(εφαρμόζουμε τον κανόνα } BA \to AB) \\
AAB\underline{CB}CABCT_c &\Rightarrow_G && \text{(εφαρμόζουμε τον κανόνα } CB \to BC) \\
AABBC\underline{CA}BCT_c &\Rightarrow_G && \text{(εφαρμόζουμε τον κανόνα } CA \to AC) \\
AABB\underline{CA}CBCT_c &\Rightarrow_G && \text{(εφαρμόζουμε τον κανόνα } CA \to AC) \\
AAB\underline{BA}CCBCT_c &\Rightarrow_G && \text{(εφαρμόζουμε τον κανόνα } BA \to AB) \\
AA\underline{BA}BCCBCT_c &\Rightarrow_G && \text{(εφαρμόζουμε τον κανόνα } BA \to AB) \\
AAABBC\underline{CB}CT_c &\Rightarrow_G && \text{(εφαρμόζουμε τον κανόνα } CB \to BC) \\
AAABB\underline{CB}CCT_c &\Rightarrow_G && \text{(εφαρμόζουμε τον κανόνα } CB \to BC) \\
AAABBBCC\underline{CT_c} &\Rightarrow_G && \text{(εφαρμόζουμε τον κανόνα } CT_c \to T_c c) \\
AAABBBC\underline{CT_c}c &\Rightarrow_G && \text{(εφαρμόζουμε τον κανόνα } CT_c \to T_c c)
\end{aligned}$$

[1] Παρατηρήστε ότι έχουμε μη-ντετερμινισμό στους κανόνες της γραμματικής καθώς το S μπορεί να μετατραπεί είτε σε $0S1$ είτε σε ϵ.

[2] Μπορείτε για εξάσκηση να αποδείξετε αυτόν τον ισχυρισμό τυπικά.

[3] Υπογραμίζουμε την υπολέξη που αλλάζει σε κάθε βήμα.

$$
\begin{aligned}
AAABBB\underline{CT_c}cc &\Rightarrow_G \quad (\text{εφαρμόζουμε τον κανόνα } CT_c \to T_bc)\\
AAABB\underline{BT_b}ccc &\Rightarrow_G \quad (\text{εφαρμόζουμε τον κανόνα } BT_b \to T_bb)\\
AAAB\underline{BT_b}bccc &\Rightarrow_G \quad (\text{εφαρμόζουμε τον κανόνα } BT_b \to T_bb)\\
AAA\underline{BT_b}bbccc &\Rightarrow_G \quad (\text{εφαρμόζουμε τον κανόνα } BT_b \to T_ab)\\
AA\underline{AT_a}bbbccc &\Rightarrow_G \quad (\text{εφαρμόζουμε τον κανόνα } AT_a \to T_aa)\\
A\underline{AT_a}abbbccc &\Rightarrow_G \quad (\text{εφαρμόζουμε τον κανόνα } AT_a \to T_aa)\\
\underline{AT_a}aabbbccc &\Rightarrow_G \quad (\text{εφαρμόζουμε τον κανόνα } AT_a \to T_aa)\\
\underline{T_a}aaabbbccc &\Rightarrow_G \quad (\text{εφαρμόζουμε τον κανόνα } T_a \to \epsilon)\\
aaabbbccc &
\end{aligned}
$$

Παρατηρήστε ότι αν εφαρμόσουμε τους κανόνες που περιέχουν τα σύμβολα T_a, T_b πρίν από τους κανόνες «αντιστροφής», θα καταλήξουμε σε μία λέξη στην οποία, ναι μεν δεν μπορεί να εφαρμοστεί κάποιος κανόνας, αλλά θα περιέχει μη-τερματικά σύμβολα. Επίσης το ίδιο θα συμβεί αν επιλέξουμε λανθασμένα μεταξύ των κανόνων $CT_c \to T_cc$ και $CT_c \to T_bc$ ή $BT_b \to T_bb$ και $BT_b \to T_ab$. Τέλος θα πρέπει να προσέξουμε να μην εφαρμόσουμε τον κανόνα $T_a \to \epsilon$ πολύ νωρίς.

Έυκολα συμπαιρένουμε ότι η γλώσσα που παράγει η γραμματική είναι η $L(G) = \{a^nb^nc^n \in \{a,b,c\}^* \mid n \geq 1\}$.

Για να αποδείξουμε Θεωρήματα Ισοδυναμίας (και λοιπά άλλα σημαντικά αποτελέσματα) θα χρειαστεί να συμφωνήσουμε μία κωδικοποίηση γραμματικών.

Κωδικοποίηση γραμματικών στο $\{0,1\}$

Σύμβαση 4.1.8. Όπως κάναμε και στο παρελθόν, θα θεωρήσουμε ότι όλες οι γλώσσες ανήκουν στο $2^{\{0,1\}^*}$. Συνεπώς από τούδε και στο εξής τα τερματικά σύμβολα των γραμματικών θα είναι πάντα τα $0, 1$.

Έστω γραμματική $G = (V, \{0,1\}, R, S)$ με $V = \{v_1, v_2, \dots, v_n\} \cup \{0,1\}$, για κάποιο $n \in \mathbb{N}$, όπου (χωρίς βλάβη της γενικότητας) $v_1 = S, v_2 = 0, v_3 = 1$. Έστω επίσης ότι $R = \{x_1 \to y_1, x_2 \to y_2, \dots, x_l \to y_l\}$, για κάποιο $l \in \mathbb{N}$. Μία γραμματική χαρακτηρίζεται πλήρως από το σύνολο των κανόνων της , συνεπώς προκειμένου να κωδικοποιήσουμε την G αρκεί να κωδικοποιήσουμε το R. Πρώτα το κωδικοποιούμε σε μία λέξη του $V \cup \{\to, ;\}$ ως εξής [1]:

$$\langle R \rangle_{V \cup \{\to,;\}} = x_1 \to y_1; x_2 \to y_2; \ \cdots \ ; x_l \to y_l$$

Έπειτα κωδικοποιούμε τα σύμβολα του $V \cup \{\to, ;\}$ στο $\{0,1\}$:

[1] Τυπικά θα πρέπει να σταθεροποιήσουμε τη σειρά που κωδικοποιούνται οι κανόνες, αλλιώς θα προκύψουν πολλαπλές κωδικοποιήσεις της ίδιας γραμματικής (σε γενικές γραμμές αυτό δεν δημιουργεί πρόβλημα). Ας υποθέσουμε ότι οι κανόνες τοποθετούνται στην κωδικοποίηση σύμφωνα με τη λεξικογραφική διάταξη του $V \cup \{\to\}$.

$$\begin{aligned}
\langle 0\rangle_{\{0,1\}} &= 01\\
\langle 1\rangle_{\{0,1\}} &= 011\\
\langle \to\rangle_{\{0,1\}} &= 0111\\
\langle ;\rangle_{\{0,1\}} &= 01111\\
\langle v_i\rangle_{\{0,1\}} &= 0\underbrace{1\cdots 1}_{i+4 \text{ φορές}}\text{, για κάθε } i \in [n]
\end{aligned}$$

Επομένως μπορούμε να κωδικοποιήσουμε την G στη λέξη $\langle\langle R\rangle_{V\cup\{\to,;\}}\rangle_{\{0,1\}}$ [1]. Από εδώ και στο εξής θα γράφουμε $\langle G\rangle$ αντί για $\langle G\rangle_{\{0,1\}}$.

Οι γενικές γραμματικές αποτελούν το τέταρτο (και τελευταίο) «υπολογιστικό μοντέλο» που θα δούμε σε αυτές τις σημειώσεις [2]. Και αυτό είναι ισοδύναμο με τις ΤΜ. Η απόδειξη οφείλεται στον *Noam Chomsky*.

Θεώρημα 4.1.9 (Chomsky). *Μία γλώσσα $L \subseteq \{0,1\}^*$ είναι αναδρομικά απαριθμήσιμη ανν υπάρχει γενική γραμματική G που την παράγει.*

Απόδειξη. ($\Rightarrow$) Έστω γλώσσα $L \in$ RE και ΤΜ $M = (Q, \{0,1\}, \Gamma, \delta, q_0, q_{\text{ναι}}, q_{\text{όχι}})$ που την ημι-αποφασίζει. Υποθέτουμε χωρίς βλάβη της γενικότητας [3] ότι:

1. Η M είναι ντετερμινιστική και μονοταινιακή.
2. Η M είτε τερματίζει στην $q_{\text{ναι}}$ είτε κολλάει [4].
3. Η M πριν τερματίσει σβήνει την ταινία της, δηλαδή το καταληκτικό στιγμιότυπο είναι πάντα το $\triangleright\, q_{\text{ναι}}$.
4. Η κατάσταση «σβησίματος» είναι η $q_\sigma \in Q$ και η M σβήνει την ταινία από το τέλος (πρώτο σύμβολο $\sqcup$) προς την αρχή ($\triangleright$).

Θεωρούμε τη γραμματική $G_M = (V, \{0,1\}, R, S)$ όπου $V = \Gamma \cup Q \cup \{S\}$ [5] και:

[1] Παρατηρήστε ότι πολλές γραμματικές κωδικοποιούνται με την ίδια λέξη! Για τους σκοπούς του κεφαλαίου αυτού δεν είναι απαραίτητο η κωδικοποίηση να είναι μονοσήμαντη. Το μόνο που χρειαζόμαστε είναι ένας τρόπος να εκφράσουμε τις γραμματικές ως λέξεις του $\{0,1\}^*$.

[2] Δεν μετράμε φυσικά τις επεκτάσεις των ΤΜ που είδαμε στο Κεφάλαιο 1 και θα δούμε και στο Κεφάλαιο 8, καθώς και τους περιορισμούς των ΤΜ που θα δούμε σε αυτό το κεφάλαιο.

[3] Υπο την έννοια ότι αν υπάρχει ΤΜ που ημι-αποφασίζει την L τότε υπάρχει και ΤΜ που την ημι-αποφασίζει με τις επιπλέον ιδιότητες που ζητάμε.

[4] Αυτό μπορούμε να το επιτύχουμε αν αφαιρέσουμε από την συνάρτηση μεταβάσεων όλες τις μεταβάσεις στην κατάσταση $q_{\text{όχι}}$.

[5] Θεωρούμε τις καταστάσεις σύμβολα. Για να είμαστε τυπικοί θα πρέπει επιπλέον να υποθέσουμε ότι τα σύμβολα του Q δεν εμφανίζονται στο Γ.

$$
\begin{aligned}
R = \{ & S \to \triangleright\, q_{\text{ναι}} \sqcup \} \cup \\
& \cup \{ \triangleright\, q_{\text{ναι}} \to q_\sigma\, \triangleright \} \cup \\
& \cup \{ bp \to qa \mid \exists q, p \in Q \setminus \{q_\sigma\}\ \exists a, b \in \Gamma\ (\delta(q,a) = (p,b,\Delta)) \} \cup \\
& \cup \{ p * b \to *qa \mid \exists q, p \in Q \setminus \{q_\sigma\}\ \exists a, b \in \Gamma\ (\delta(q,a) = (p,b,\mathrm{A})), \text{για } * \in \Gamma \} \cup \\
& \cup \{ q_\sigma * \sqcup \to *qa \mid \exists q \in Q\ \exists a \in \Gamma\ (\delta(q,a) = (q_\sigma, \sqcup, \mathrm{A})), \text{για } * \in \Gamma \} \cup \\
& \cup \{ \triangleright\, q_0 \to \epsilon, \sqcup \to \epsilon \}
\end{aligned}
$$

Έστω $w \in \{0,1\}^*$ είσοδος της M. Αντιστοιχούμε κάθε στιγμιότυπο $\triangleright\, w_1 q w_2$ της $M(w)$ (όπου $w_1, w_2 \in \Gamma$ και $q \in Q$) στη λέξη $\triangleright\, w_1 q w_2 \sqcup \in (\Gamma \cup Q)^*$ και, έχοντας προσθέσει στο R κανόνες που εφαρμόζουν τις μεταβάσεις της δ αντίστροφα [1], προσομοιώνουμε τη λειτουργία της $M(w)$ από το τέλος (το στιγμιότυπο $\triangleright\, q_{\text{ναι}}$ δηλαδή) προς την αρχή (το στιγμιότυπο $\triangleright\, q_0 w$). Παρατηρήστε ότι $M(w) \downarrow_{q_{\text{ναι}}}$ ανν $S \Rightarrow^*_{G_M} w$, άρα $L(G_M) = L(M) = L$.

($\Leftarrow$) Έστω γραμματική $G = (V, \{0,1\}, R, S)$. Θα ορίσουμε μία NTM $N_G = (Q, \{0,1\}, \Gamma, \delta, q_0, q_{\text{ναι}}, q_{\text{όχι}})$, με $V \subseteq \Gamma$, που θα ημι-αποφασίζει την $L(G)$. Η N_G έχει τρεις ταινίες: Η πρώτη περιέχει τη λέξη εισόδου (και δεν μεταβάλλεται ποτέ), η δεύτερη είναι η ταινία εργασίας και η τρίτη περιέχει την κωδικοποίηση της G (δηλαδή τη λέξη $\langle G \rangle$).

Η N_G ελέγχει αν είναι δυνατό να παραχθεί η είσοδος $w \in \{0,1\}^*$ σύμφωνα με τους κανόνες της G. Στην αρχή του υπολογισμού η δεύτερη ταινία περιέχει το σύμβολο S και σε κάθε βήμα κάνει τα ακόλουθα:

1. Είτε επιλέγει μη-ντετερμινιστικά έναν κανόνα από το R, είτε ελέγχει αν η δεύτερη ταινία ταυτίζεται με την πρώτη.

2. (α΄) Αν επιλέξει τον κανόνα $u \to v \in R$, η N_G:
   i. Σαρώνει τη δεύτερη ταινία (από τα αριστερά προς τα δεξιά),
   ii. σταματάει μη-ντετερμινιστικά σε ένα σύμβολο,
   iii. ελέγχει αν τα επόμενα $|u|$ σύμβολα ταυτίζονται με τη u:
      - αν ταυτίζονται τα αντικαθιστά με τη v (δημιουργώντας χώρο ή «διαγράφοντας» κενά όταν χρειαστεί),
      - αν δεν ταυτίζονται η N_G «κολλάει».

   (β΄) Αν επιλέξει να ελέγξει αν η δεύτερη ταινία ταυτίζεται με την πρώτη:
      - Αν όντως ταυτίζονται η N_G πάει στην $q_{\text{ναι}}$ και τερματίζει.
      - Αν δεν ταυτίζονται η N_G «κολλάει».

Εύκολα βλέπουμε ότι υπάρχει παραγωγή της w από την G ανν υπάρχει μη-ντετερμινιστικός κλάδος της $N_G(w)$ που καταλήγει στην $q_{\text{ναι}}$, άρα $L(M_G) = L(G)$. Για να ολοκληρωθεί η απόδειξη θα πρέπει να δείξουμε ότι για κάθε μη-ντετερμινιστική TM k-ταινιών υπάρχει ισοδύναμη μονοταινιακή και ντετερμινιστική TM [2]. □

[1] Αν $C_1 \vdash_M C_2$ για δύο στιγμιότυπα C_1, C_2 της $M(w)$ τότε, σύμφωνα με τους κανόνες της G_M, έχουμε $C_2 \Rightarrow_{G_M} C_1$ όπου πλέον τα C_1, C_2 τα βλέπουμε ως λέξεις του $(\Gamma \cup Q)^*$.

[2] Αφήνεται ως άσκηση.

Οι γενικές γραμματικές πέρα από το να παράγουν λέξεις μπορούν να υπολογίσουν και συναρτήσεις.

Ορισμός 4.1.10. Η γραμματική $G = (V, \Sigma, R, S)$ *υπολογίζει τη συνάρτηση* $f : \Sigma^* \to \Sigma^*$ ανν για κάθε $x, y \in \Sigma^*$:

$$SxS \Rightarrow_G^* y \Leftrightarrow f(x) = y$$

και αν $x \notin \mathsf{dom}(f)$ τότε δεν υπάρχει $y \in \Sigma^*$ τέτοιο ώστε $SxS \Rightarrow_G^* y$.

Μία συνάρτηση $f : \Sigma^* \to \Sigma^*$ καλείται *γραμματικά υπολογίσιμη* ανν υπάρχει γενική γραμματική που την υπολογίζει [1].

Παράδειγμα 4.1.11. Η συνάρτηση $f : \{1\}^* \to \{1\}^*$ με $f(x) = xx$ είναι γραμματικά υπολογίσιμη καθώς η γραμματική $G = (\{1, S\}, \{1\}, S, R)$, όπου $R = \{S1 \to 11S, SS \to \epsilon\}$, την υπολογίζει.

Παράδειγμα 4.1.12. Η συνάρτηση $f : \mathbb{N} \to \mathbb{N}$, με $f(x) = 3x + 5$ είναι γραμματικά υπολογίσιμη, αν χρησιμοποιήσουμε το μοναδιαίο σύστημα αρίθμησης (δες σελίδα 74), καθώς η γραμματική $G = (\{1, S\}, \{1\}, R, S)$, όπου $R = \{S1 \to 111S, S1S \to 111111\}$, την υπολογίζει.

Αντίστοιχα με το Θεώρημα 4.1.9 μπορούμε να αποδείξουμε το ακόλουθο θεώρημα (τέταρτος ορισμός υπολογίσιμων συναρτήσεων).

Θεώρημα 4.1.13. Μία συνάρτηση $f : \Sigma^* \to \Sigma^*$ είναι υπολογίσιμη ανν είναι γραμματικά υπολογίσιμη.

4.2 Γραμματικές με συμφραζόμενα

Ορισμός 4.2.1. *Γραμματική με συμφραζόμενα* (ή *γραμματική Τύπου 1*) είναι μία γραμματική $G = (V, \{0, 1\}, R, S)$ όπου για κάθε κανόνα $u \to v \in R$ ισχύει ότι $|u| \leq |v|$.

Το ακόλουθο Θεώρημα αναφέρεται χωρίς απόδειξη (δες Άσκηση 4.11).

Θεώρημα 4.2.2. Για κάθε γραμματική $G = (V, \{0, 1\}, R, S)$ με συμφραζόμενα υπάρχει ισοδύναμη γραμματική $G' = (V', \{0, 1\}, R', S)$, όπου $V \subseteq V'$ και κάθε κανόνας $u \to v \in R'$ έχει τη μορφή $w_1 A w_2 \to w_1 w w_2$, όπου $w, w_1, w_2 \in V'^*$, $A \in V' \setminus \{0, 1\}$ και $w \neq \epsilon$ [2].

Ορισμός 4.2.3. Μία γλώσσα $L \subseteq \{0, 1\}^*$ ονομάζετε *γλώσσα με συμφραζόμενα* ανν υπάρχει γραμματική με συμφραζόμενα που την παράγει. Συμβολίζουμε το σύνολο των γλωσσών με συμφραζόμενα ως CS.

[1] Μια βασική ιδιότητα που θα πρέπει να αποδειχθεί είναι ότι η σειρά με την οποία εφαρμόζονται οι κανόνες πάντα τελικά οδηγεί στην ίδια ακριβώς λέξη, την τιμή της συνάρτησης (θα πρέπει να δειχθεί ένα αντίστοιχο του Θεωρήμαστος 3.2.14). Αυτή η ιδιότητα συνήθως αναφέρεται ως ιδιότητα Church-Rosser.

[2] Με λόγια: Το σύμβολο A όταν έχει συμφραζόμενα w_1 και w_2 μετατρέπεται στη λέξη w.

Σημείωση 4.2.4. Παρατηρήστε ότι σύμφωνα με τον Ορισμό 4.2.1 οι γλώσσες του CS δεν μπορούν να περιέχουν την κενή λέξη. Αυτό θα μας δημιουργίσει πρόβλημα στην απόδειξη του Θεωρήματος 4.2.8 και στην Ιεραρχία Chomsky (Παράγραφος 4.5), όπου θα ιεραρχήσουμε (σύμφωνα με τη σχέση του συνολοθεωρητικού εγκλεισμού) τις κλάσεις των γλωσσών που παράγονται από τους τύπους γραμματικών που θα δούμε στις Παραγράφους 4.2, 4.3 και 4.4. Ένας τρόπος να αποφύγουμε αυτό το πρόβλημα είναι να επιτρέψουμε στον Ορισμό 4.2.1 τον κανόνα $S \to \epsilon$ και να εξασφαλίσουμε ότι το S δεν εμφανίζεται στο δεξιό μέρος κάποιου κανόνα [1].

Παράδειγμα 4.2.5. Η γλώσσα $L = \{a^n b^n c^n \in \{a,b,c\}^* \mid n \geq 1\}$ [2] του Παραδείγματος 4.1.7 είναι γλώσσα με συμφραζόμενα [3], καθώς εύκολα μπορούμε να δούμε ότι η γραμματική $G = (V, \Sigma, R, S)$ με $V = \{B, C, T_b, T_c, S\} \cup \Sigma$, όπου $\Sigma = \{a,b,c\}$, και

$$\begin{array}{l|l} R = \{S \to aBC, & T_bC \to BC, \\ \quad S \to aSBC, & aB \to ab, \\ \quad CB \to CT_c, & bB \to bb, \\ \quad CT_c \to T_bT_c, & bC \to bc, \\ \quad T_bT_c \to T_bC, & cC \to cc\} \end{array}$$

την παράγει [4].

Ορισμός 4.2.6. *Γραμμικά φραγμένο αυτόματο (LBA)* είναι μία NTM $N = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{ναι}}, q_{\text{όχι}})$ με $\triangleleft \in \Gamma \setminus \Sigma$, όπου το $\triangleleft$ είναι ένα σύμβολο που σηματοδοτεί το τέλος της λέξης εισόδου (δες Σχήμα 4.2.1). Η N δεν μπορεί να κινήσει την κεφαλή δεξιότερα από το σύμβολο $\triangleleft$ ούτε να γράψει πάνω σε αυτό [5].

Ορίζοντας τον υπολογισμό και κατ' επέκταση την αποδοχή και την απόρριψη μίας λέξης αντίστοιχα με τον Ορισμό 1.3.8 μπορούμε να ορίσουμε τη γλώσσα που αναγνωρίζει το LBA ως εξής:

$$L(N) = \{w \in \Sigma^* \mid \exists w_1, w_2 \in \Gamma^* (\triangleright\, q_0 w \triangleleft \vdash_N^* \triangleright\, w_1 q_{\text{ναι}} w_2 \triangleleft)\}$$

[1] Έτσι όλες οι παραγωγές λέξεων από τη γραμματική θα αυξάνουν το μήκος της λέξης, εκτός φυσικά από την παραγωγή της κενής λέξης

[2] Η L ορίζεται σαν γλώσσα του $\{a,b,c\}$ για λόγους απλότητας. Θα μπορούσαμε να την ορίσουμε στο $\{0,1\}$ παραδείγματος χάρη ως εξής: $L = \{(01)^n(011)^n(0111)^n \in \{0,1\}^* \mid n \geq 1\}$.

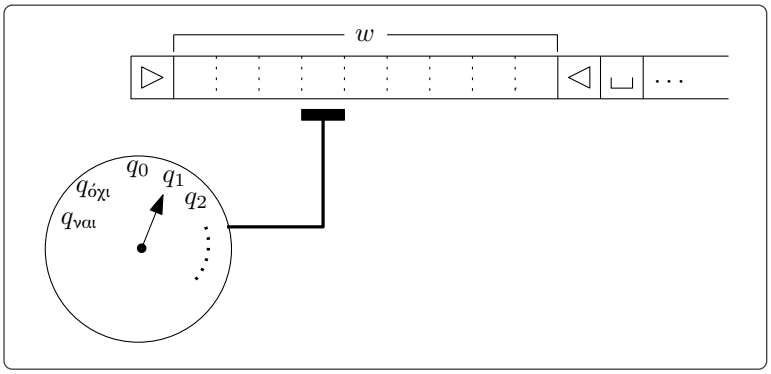
[3] Παρατηρήστε ότι η γραμματική του Παραδείγματος 4.1.7 δεν είναι γραμματική με συμφραζόμενα καθώς περιέχει τον κανόνα $T_a \to \epsilon$.

[4] Και η γραμματική με συμφραζόμενα $G = (V, \Sigma, R, S)$ με $V = \{B, C, S\} \cup \Sigma$, $\Sigma = \{a,b,c\}$, και

$$\begin{array}{l|l} R = \{S \to aBC, & bB \to bb, \\ \quad S \to aSBC, & bC \to bc, \\ \quad CB \to BC, & cC \to cc\} \\ \quad aB \to ab, & \end{array}$$

την παράγει μόνο που η γραμματική του Παραδείγματος 4.2.5 έχει την «κανονική μορφή» του Θεωρήματος 4.2.2.

[5] Συνεπώς η N έχει πρόσβαση μόνο στο κομμάτι της ταινίας που περιέχει την είσοδο.



Σχήμα 4.2.I: *Σχηματική αναπαράσταση ενός LBA.*

Παρατήρηση 4.2.7. Έστω LBA $N = (Q, \Sigma, \Gamma, \delta, q_0, q_{ναι}, q_{όχι})$. Χρησιμοποιώντας σύμβολα που αντιστοιχούν σε λέξεις μήκους το πολύ $c \in \mathbb{N}$ του Γ^* και τροποποιώντας κατάλληλα τη δ μπορούμε να «μεγαλώσουμε» τη διαθέσιμη «μνήμη» [1] από $|w|$, όπου $w \in \Sigma^*$ η είσοδος, σε $c \cdot |w|$.

Τα LBA αποτελούν έναν περιορισμό των TM. Αυτός ο περιορισμός είναι ουσιαστικός καθώς (ακόμα και διαισθητικά αντιλαμβανόμαστε ότι) τα LBA δεν είναι το ίδιο «ισχυρά» με τις TM. Για να το αποδείξουμε όμως αυτό θα χρειαστεί (για μία ακόμα φορά) να κάνουμε διαγωνιοποίηση (δες Θεώρημα 4.2.11).

Το ακόλουθο θεώρημα αποδεικνύει ότι οι γλώσσες που αναγνωρίζονται από τα LBA είναι ακριβώς οι γλώσσες με συμφραζόμενα (η απόδειξή του αφήνεται ως Άσκηση).

Θεώρημα 4.2.8. Μία γλώσσα $L \subseteq \{0,1\}^*$ είναι γλώσσα με συμφραζόμενα ανν υπάρχει LBA που την αναγνωρίζει [2].

Αν εξετάσουμε προσεκτικά την απόδειξη του Θεωρήματος 4.2.8 θα καταλήξουμε στο ακόλουθο πόρισμα.

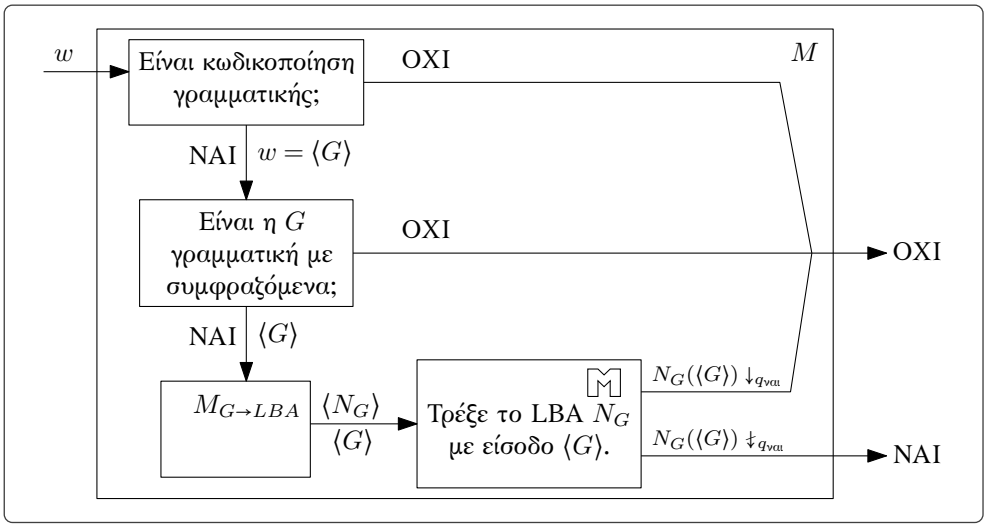
Πόρισμα 4.2.9. Έστω $L \in$ CS και έστω ότι η γραμματική G Τύπου 1 την παράγει. Υπάρχει TM $M_{G \to LBA}$ που δέχεται σαν είσοδο $\langle G \rangle$ και επιστρέφει $\langle N_G \rangle$ όπου N_G το LBA που αναγνωρίζει την L [3].

Δεν είναι ιδιαίτερα δύσκολο να αποδείξει κανείς ότι τα LBA είναι TM που «τερματίζουν πάντα» (ή τουλάχιστον, μπορούμε να εξακριβώσουμε πότε «κολλάνε», Άσκηση 4.14),

[1] Το πλήθος συμβόλων δηλαδή που μπορούμε να αποθηκεύσουμε στο κομμάτι της ταινίας που μας επιτρέπεται να τροποποιήσουμε.

[2] Δες τη Σημείωση 4.2.4.

[3] Απόρια του «διαστικού» τρόπου με τον οποίο κωδικοποιήσαμε τις γραμματικές, είναι το ακόλουθο έυλογο ερώτημα: Ποιο ακριβώς LBA θα επιστρέψει η TM $M_{G \to LBA}$, καθώς η λέξη $\langle G \rangle$ αντιστοιχεί σε πολλές γραμματικές; Η αλήθεια είναι ότι με την ίδια λέξη κωδικοποιούνται μόνο ισοδύναμες γραμματικές (που περιέχουν μη χρησιμοποιούμενα μη-τερματικά σύμβολα). Οπότε στην πραγματικότητα ένα μόνο LBA αντιστοιχεί στην $\langle G \rangle$!



Σχήμα 4.2.2: *Η TM που αποφασίζει την L στην απόδειξη του Θεωρήματος 4.2.11. $M_{G\to LBA}$ είναι η TM του Πορίσματος 4.2.9.*

επομένως μία γλώσσα με συμφραζόμενα είναι αναδρομική γλώσσα. Αυτός ο ισχυρισμός (Θεώρημα 4.2.10) μπορεί να αποδειχθεί και χωρίς τη χρήση LBA (δες Άσκηση 4.13).

Θεώρημα 4.2.10. Κάθε γλώσσα με συμφραζόμενα είναι αναδρομική (δηλαδή $\mathsf{CS} \subseteq \mathsf{REC}$).

Το αντίστροφο του Θεωρήματος 4.2.10 δεν ισχύει καθώς υπάρχουν αναδρομικές γλώσσες που δεν είναι γλώσσες με συμφραζόμενα [1].

Θεώρημα 4.2.11. Υπάρχει γλώσσα $L \in \mathsf{REC} \setminus \mathsf{CS}$.

Απόδειξη. Παρατηρήστε ότι αν μας δωθεί μια κωδικοποίηση γραμματικής στο $\{0,1\}$ (σύμφωνα με όσα είπαμε στη Σελίδα 98) μπορούμε να ελέγξουμε αν επιπλέον αντιστοιχεί σε κωδικοποίηση γραμματικής με συμφραζόμενα (ελέγχουμε αν οι κανόνες έχουν τη μορφή του Ορισμού 4.2.1). Θεωρούμε τη γλώσσα:

$$L = \{\langle G\rangle \in \{0,1\}^* \mid G \text{ γραμματική με συμφραζόμενα και } \langle G\rangle \notin L(G)\}$$

Παρατηρήστε ότι $L \in \mathsf{REC}$ καθώς η TM M του Σχήματος 4.2.2 την αποφασίζει [2]. Η L όμως δεν θα μπορούσε να είναι γλώσσα με συμφραζόμενα καθώς τότε, αν G_L ήταν η γραμματική με συμφραζόμενα που την παρήγαγε, θα ίσχυε ότι:

$$\langle G_L\rangle \in L \Leftrightarrow \langle G_L\rangle \notin L(G_L) \Leftrightarrow \langle G_L\rangle \notin L$$

που είναι άτοπο. □

[1] Πόρισμα αυτού είναι ότι τα LBA είναι ασθενέστερα από τις TM.
[2] Σύμφωνα με την Άσκηση 4.14 ο έλεγχος που κάνει η καθολική TM στο Σχήμα 4.2.2 τερματίζει πάντα.

4.3 Γραμματικές χωρίς συμφραζόμενα

Ορισμός 4.3.1. *Γραμματική χωρίς συμφραζόμενα* (ή *γραμματική Τύπου 2*) είναι μία γραμματική $G = (V, \{0,1\}, R, S)$ τέτοια ώστε $R \subseteq (V \setminus \{0,1\}) \times V^*$ [1].

Ορισμός 4.3.2. Μία γλώσσα $L \subseteq \{0,1\}^*$ ονομάζετε *γλώσσα χωρίς συμφραζόμενα* ανν υπάρχει γραμματική χωρίς συμφραζόμενα που την παράγει. Συμβολίζουμε το σύνολο των γλωσσών χωρίς συμφραζόμενα ως CF.

Σημείωση 4.3.3. Χωρίς βλάβη της γενικότητας, μπορούμε να θεωρήσουμε ότι στον Ορισμό 4.3.1 ο μόνος κανόνας που περιέχει την κενή λέξη στο δεξιό μέρος του είναι ο $S \to \epsilon$ και ότι το S δεν εμφανίζεται στο δεξιό μέρος κάποιου κανόνα. Το γεγονός αυτό θα το χρειαστούμε στην απόδειξη του Θεωρήματος 4.5.1.

Παράδειγμα 4.3.4. Η γλώσσα $L = \{0^n 1^n \in \{0,1\}^* \mid n \in \mathbb{N}\}$ είναι γλώσσα χωρίς συμφραζόμενα καθώς η γραμματική G του Παραδείγματος 4.1.6 είναι γραμματική χωρίς συμφραζόμενα.

Όπως κάναμε με τις γλώσσες με συμφραζόμενα θα ορίσουμε έναν «περιορισμό» των TM που αναγνωρίζει τις γλώσσες χωρίς συμφραζόμενα.

Ορισμός 4.3.5. *Αυτόματο στοίβας (PDA)* είναι μία NTM δύο ταινιών $N = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{ναι}}, q_{\text{όχι}})$ όπου $\delta \subseteq Q \times (\Sigma \cup \{\epsilon\}) \times (\Gamma \cup \{\epsilon\}) \times Q \times (\Gamma \cup \{\epsilon\})$ [2]. Αν έχουμε τη μετάβαση $(p, a, b, q, c) \in \delta$ τότε αν το N βρίσκεται στην κατάσταση p, διαβάζει το σύμβολο $a \in \Sigma \cup \{\epsilon\}$ στην πρώτη ταινία και το σύμβολο $b \in \Gamma \cup \{\epsilon\}$ στη δεύτερη, θα μεταβεί στην κατάσταση q και θα γράψει το σύμβολο $c \in \Gamma \cup \{\epsilon\}$ στη θέση του b (δες Σχήμα 4.3.1). Οι κεφαλές κινούνται πάντα δεξιά, εκτός αν:

- $a = \epsilon$ οπότε η κεφαλή της πρώτης ταινίας (ταινία εισόδου) δεν μετακινείται (και έτσι δεν λαμβάνουμε κάποια πληροφορία από αυτή),
- $b = \epsilon$ το N μετακινεί την κεφαλή της δεύτερης ταινίας (της «στοίβας») ένα κελί δεξιά και γράφει c στη θέση του $\sqcup$,
- $c = \epsilon$ οπότε η N αντικαθιστά το b με $\sqcup$ και κινεί την κεφαλή της δεύτερης ταινίας αριστερά [3],

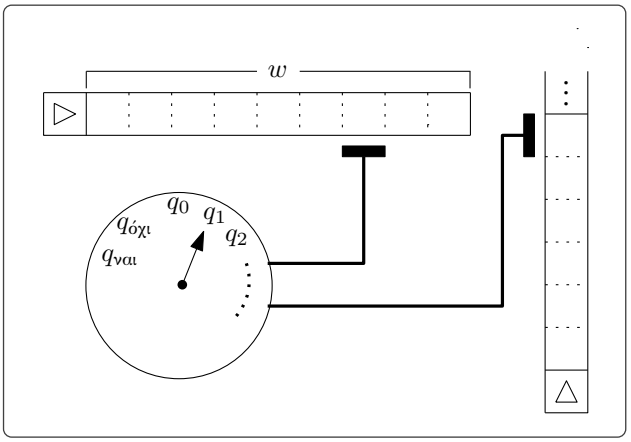
Η N τερματίζει όταν διαβαστεί όλη η είσοδος και φτάσουμε στο πρώτο $\sqcup$ (όταν συμβεί αυτό ο υπολογισμός θα πρέπει να έχει καταλλήξει σε τερματική κατάσταση).

Ένα PDA αποδέχεται/απορρίπτει μία λέξη $w \in \Sigma^*$ ανν υπάρχει λέξη $w' \in (\Sigma \cup \{\epsilon\})^*$ τέτοια ώστε $w = w'$ (δηλαδή η w' είναι στην ουσία η w όπου έχουμε προσθέσει σε κάποια σημεία το σύμβολο της κενής λέξης) και ο υπολογισμός με είσοδο την w' και κενή δεύτερη ταινία (όπως τον περιγράψαμε παραπάνω) καταλλήγει στην κατάσταση αποδοχής/απόρριψης.

[1] Δηλαδή έχουμε κανόνες της μορφής $A \to u$, όπου A μη-τερματικό σύμβολο και $u \in V^*$ (η u μπορεί να είναι και η κενή λέξη).

[2] Ναι σωστά καταλάβατε, χρησιμοποιούμε ως σύμβολο την κενή λέξη!

[3] Παρατηρήστε ότι η πρώτη ταινία περιέχει την είσοδο και δεν τροποποιείται ποτέ, το M μπορεί να διαβάσει μόνο το τελευταίο μη-κενό κελί της δεύτερης ταινίας και να γράψει μόνο στο πρώτο κενό κελί της, τη χρησιμοποιεί δηλαδή σαν μία «στοίβα» συμβόλων.



Σχήμα 4.3.1: *Σχηματική αναπαράσταση ενός PDA.*

Το παρακάτω Θεώρημα αναφέρεται χωρίς απόδειξη.

Θεώρημα 4.3.6. Μία γλώσσα $L \subseteq \{0,1\}^*$ είναι γλώσσα χωρίς συμφραζόμενα ανν υπάρχει PDA που την αναγνωρίζει.

4.4 Κανονικές γραμματικές

Ας ξεκινήσουμε ορίζοντας της γλώσσες που «προέρχονται» από κανονικές εκφράσεις του $\{0,1\}$ (θυμηθείτε τους Ορισμούς 0.2.22 και 0.2.24).

Ορισμός 4.4.1. Μία γλώσσα $L \subseteq \{0,1\}^*$ είναι *κανονική* ανν υπάρχει $\mathsf{x} \in R_{\{0,1\}}$ τέτοια ώστε $L = \mathcal{L}(\mathsf{x})$. Το σύνολο των κανονικών γλωσσών το συμβολίζουμε με R.

Ορισμός 4.4.2. *Κανονική γραμματική* (ή *αριστερο-γραμμική* [1] *γραμματική* ή *γραμματική Τύπου 3*) είναι μία γραμματική χωρίς συμφραζόμενα $G = (V, \{0,1\}, R, S)$ όπου το δεξιό μέρος των κανόνων του R περιέχει το πολύ ένα μη-τερματικό σύμβολο, το οποίο βρίσκεται στο αριστερότερο άκρο [2].

Παράδειγμα 4.4.3. Η γραμματική $G = (V, \{0,1\}, R, S)$ με $V = \{0,1,A,S\}$ και

$$R = \{S \to A, \quad S \to S1, \quad S \to \epsilon, \quad A \to A0\}$$

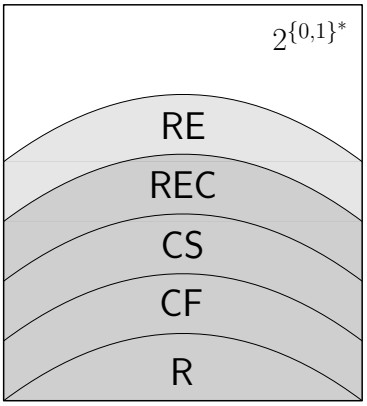
είναι κανονική γραμματική. Παρατηρήστε ότι $L(G) = \{0^n 1^m \in \{0,1\}^* \mid n,m \in \mathbb{N}\}$. Παρατηρήστε επίσης ότι $L(G) = [0^\star 1^\star]$. Όπως μας δείχνει το Θεώρημα 4.4.5, το γεγονός αυτό δεν είναι τυχαίο.

[1] Μπορούμε να ορίσουμε και *δεξιο-γραμμικές* γραμματικές με αντίστοιχο τρόπο.

[2] Δηλαδή έχουμε κανόνες της μορφής $A \to Bu$ ή $A \to u$ ή $A \to \epsilon$ όπου A, B μη-τερματικά σύμβολα και $u \in \{0,1\}^*$.

Γλώσσες	Γραμματικές	Υπολογιστικό Μοντέλο
RE	Γενικές	TM
CS	Με συμφραζόμενα	LBA
CF	Χωρίς συμφραζόμενα	PDA
R	Κανονικές	NFA

Πίνακας 4.1: *Σχέση μεταξύ κλάσεων γλωσσών, γραμματικών και μηχανών.*



Σχήμα 4.5.1: *Η Ιεραρχία Chomsky.*

Ορισμός 4.4.4. *Πεπερασμένο αυτόματο (NFA)* είναι ένα PDA $N = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{ναι}}, q_{\text{όχι}})$ που δεν έχει «στοίβα», δηλαδή η συνάρτηση μετάβασής του είναι $\delta \subseteq Q \times (\Sigma \cup \{\epsilon\}) \times Q$.

Το παρακάτω Θεώρημα αναφέρεται επίσης χωρίς απόδειξη.

Θεώρημα 4.4.5. Έστω γλώσσα $L \subseteq \{0,1\}^*$. Τα ακόλουθα είναι ισοδύναμα:

1. Η $L \in \mathsf{R}$.
2. Υπάρχει κανονική γραμματική G με $L(G) = L$.
3. Υπάρχει NFA N με $L(N) = L$.

4.5 Ιεραρχία Chomsky

Ο Πίνακας 4.1 δείχνει τη σχέση των κλάσεων γλωσσών, τύπου γραμματικής και υπολογιστικού μοντέλου που είδαμε στις προηγούμενες παραγράφους.

Θεώρημα 4.5.1 (Ιεραρχία Chomsky). Ισχύει ότι $\mathsf{R} \subset \mathsf{CF} \subset \mathsf{CS} \subset \mathsf{RE}$ (δες Σχήμα 4.5.1).

Σκιαγράφηση απόδειξης. Η συμπερίληψη προκύπτει από τους Ορισμούς, από το Θεώρημα 4.4.5 και από το γεγονός ότι:

- Μία κανονική γραμματική είναι και γραμματική χωρίς συμφραζόμενα.
- Μία γραμματική χωρίς συμφραζόμενα είναι και γραμματική με συμφραζόμενα [1].
- Μία γραμματική με συμφραζόμενα είναι και γενική γραμματική.

Για να αποδειχθεί ότι οι συμπεριλήψεις μεταξύ των R,CF και των CF,CS είναι γνήσιες πρέπει να εφαρμόσουμε τα *Λήμματα άντλησης* [2], ενώ το γνήσιο της συμπερίληψης του CS στο RE αποδείχθηκε στο Θεώρημα 4.2.11. □

Σημείωση 4.5.2. Δεν υπάρχει τύπος γραμματικής που να παράγει ακριβώς τις γλώσσες της κλάσης REC.

Οι γραμματικές που είδαμε στο κεφάλαιο αυτό στη βιβλιογραφία συνήθως αποκαλούνται *Phrase Structure*, ένα όνομα που έδωσε ο Noam Chomsky το 1957 στις «γραμματικές» που είχαν πρότερα μελετήσει οι *Emil Post* και *Axel Thue*. Σε αυτές τις γραμματικές οι παραγωγές των λέξεων βασίζονται στον μετασχηματισμό των μη-τερματικών συμβόλων. Στις λεγόμενες *Left-associative* γραμματικές οι παραγωγές των λέξεων βασίζονται στην ακόλουθη ιδέα: Ξεκινάμε από κάποιο αρχικό σύμβολο και συνεχίζουμε την παραγωγή ανάλογα με τους επιτρεπόμενους από τους κανόνες τρόπους επέκτασης της λέξης (π.χ. προσθέτοντας κάποιο σύμβολο). Η κλάση των γλωσσών που παράγεται από τις γραμματικές αυτού του είδους ταυτίζεται με τη REC [3].

Ασκήσεις

4.1 (★★☆). Αποδείξτε το Θεώρημα 4.1.13.

4.2 (★☆☆). Βρείτε γραμματική Τύπου 0 που παράγει τη γλώσσα $L = \{ww \mid w \in \{0,1\}^*\}$.

4.3 (★★☆). Αποδείξτε το Θεώρημα 4.2.8.

4.4 (★★☆). Βρείτε γραμματική Τύπου 0 που παράγει τη γλώσσα $L = \{1^{2^i} \mid i \geq 1\}$. Εξετάστε αν είναι γλώσσα με συμφραζόμενα.

4.5 (★☆☆). Βρείτε γραμματική που υπολογίζει τη συνάρτηση $f : \{0,1\}^* \to \{0,1\}^*$, με $f(x)$ να είναι η λέξη x με τα 0 να έχουν γίνει 1 και τα 1 να έχουν γίνει 0.

[1] Αυτό προκύπτει από αυτά που αναφέρονται στις Σημειώσεις 4.2.4 και 4.3.3. Ο εγκλεισμός CF ⊆ CS μπορεί επίσης να αποδειχθεί δείχνοντας ότι μπορούμε να προσομοιώσουμε τη λειτουργία ενός PDA με ένα LBA.

[2] Το Λήμμα άντλησης για κανονικές γλώσσες (με δυο λόγια) λέει ότι μία «αρκετά μεγάλη» λέξη περιέχει μία υπολέξη που επαναλαμβάνεται ένα πλήθος φορών (παρατηρήστε π.χ. ότι η γλώσσα του Παραδείγματος 4.3.4 δεν έχει αυτήν την ιδιότητα). Στις γλώσσες χωρίς συμφραζόμενα προκύπτει ότι για κάθε «αρκετά μεγάλη» λέξη υπάρχουν δύο επαναλαμβανόμενες υπολέξεις. Για περισσότερες λεπτομέρειες ανατρέξτε στα [1, 2, 3, 4, 7].

[3] Περισσότερες πληροφορίες μπορείτε να βρείτε στο [9].

4.6 (★☆☆). Βρείτε γραμματική που υπολογίζει τη συνάρτηση $f : \{0,1\}^* \to \{0,1\}^*$, με $f(x_1x_2\cdots x_n) = x_1x_1x_2x_2\cdots x_nx_n$.

4.7 (★★☆). Βρείτε γραμματική που υπολογίζει τη συνάρτηση $f : \{0,1\}^* \to \{0,1\}^*$, με:

$$f(x_1x_2\cdots x_n) = \begin{cases} x_1x_1x_2x_2\cdots x_nx_n & , \text{ Αν } x_n = 0 \\ y_1y_2\cdots y_n \text{ όπου } y_i = \begin{cases} 1 & , \text{ Αν } x_i = 0 \\ 0 & , \text{ Αλλιώς} \end{cases} & , \text{ Αλλιώς} \end{cases}$$

4.8 (★☆☆). Βρείτε γραμματική που υπολογίζει στο μοναδιαίο σύστημα τη συνάρτηση $f : \mathbb{N} \to \mathbb{N}$, με $f(x) = x \bmod 3$.

4.9 (★☆☆). Βρείτε γραμματική που υπολογίζει στο μοναδιαίο σύστημα τη συνάρτηση $f : \mathbb{N} \setminus \{0\} \to \mathbb{N}$, με $f(x) = x - 1$.

4.10 (★☆☆). Βρείτε γραμματική που υπολογίζει στο μοναδιαίο σύστημα τη συνάρτηση $f : \{x \in \mathbb{N} \mid x = 0 \bmod 2\} \to \mathbb{N}$, με $f(x) = x/2$.

4.11 (★★☆). Αποδείξτε το Θεώρημα 4.2.2 Αν αποσύρουμε τον περιορισμό $w \neq \epsilon$ ισχύει το ίδιο για κάθε γραμματική Τύπου 0;

4.12 (★★☆). Αποδείξτε το Θεώρημα 4.2.8.

4.13 (★☆☆). Αποδείξτε το Θεώρημα 4.2.10 χωρίς να χρησιμοποιήσετε LBA.

4.14 (★☆☆). Θεωρήστε τη γλώσσα $L_{\text{Αποδοχής/LBA}} = \{\langle M, w\rangle \in \{0,1\}^* \mid M \text{ είναι LBA και } M(w) \downarrow q_{\text{ναι}}\}$. Δείξτε ότι $L_{\text{Αποδοχής/LBA}} \in \mathsf{REC}$.

4.15 (☆☆☆). Δείξτε ότι η γλώσσα $L = \{ww^R \mid w \in \{0,1\}^*\}$ είναι γλώσσα χωρίς συμφραζόμενα.

ΜΕΡΟΣ ΙΙ

ΥΠΟΛΟΓΙΣΙΜΟΤΗΤΑ

ΚΕΦΑΛΑΙΟ 5

ΜΗ-ΑΠΟΦΑΝΣΙΜΟΤΗΤΑ

5.1 Θέση Church-Turing

Το 1900 ο David Hilbert δημοσίευσε μία λίστα αποτελούμενη από 23 προβλήματα που (κατά τον ίδιο) θα έπρεπε να απασχολήσουν τη Μαθηματική κοινότητα για τον (τότε) νέο αιώνα [1]. Στη δική μας αφήγηση, το δέκατο από αυτά θα μπορούσε κάλλιστα να αποτελέσει την εισαγωγή:

Το 10ο πρόβλημα του Hilbert:
Βρείτε μια διαδικασία σύμφωνα με την οποία μπορεί να εξακριβωθεί αν μία πολυωνυμική διοφαντική εξίσωση με ακέραιους συντελεστές έχει ακέραιες λύσεις, μετά από πεπερασμένο πλήθος πράξεων.

Η σπουδαιότητα αυτού του προβλήματος έγκειται στο γεγονός ότι στην ουσία ζητάει την εύρεση ενός *αλγορίθμου* που με είσοδο μία εξίσωση θα αποφασίζει αν αυτή έχει ακέραιες λύσεις ή όχι. Σίγουρα δεν είναι η πρώτη φορά που ανατέθηκε στους μαθηματικούς η εύρεση αλγορίθμου. Το σημαντικό είναι ότι πλέον ένας σύγχρονος μαθηματικός εξετάζει παράλληλα και το ενδεχόμενο μη ύπαρξης αλγορίθμου (ή έστω αποδοτικού αλγορίθμου)!

Όμως τι ακριβώς θεωρείται αλγόριθμος. Διαισθητικά θα μπορούσαμε να ορίσουμε την έννοια του αλγορίθμου ως εξής:

Ορισμός 5.1.1 (Διαισθητικός Ορισμός Αλγορίθμου). *Αλγόριθμος* είναι μία πεπερασμένη ακολουθία (αυστηρά καθορισμένων) απλών οδηγιών που διεκπεραιώνουν κάποια εργασία.

Ένα κλασικό παράδειγμα αλγόριθμου με την παραπάνω έννοια είναι ο αλγόριθμος του Ευκλείδη για την εύρεση του μέγιστου κοινού διαιρέτη (ΜΚΔ) (αποδοσμένος όπως διδάσκεται στην έκτη τάξη του Δημοτικού) [2]:

[1] Τα 10 πιο σημαντικά από αυτά τα παρουσίασε στο Παρίσι την ίδια χρονιά, στα πλαίσια του 2ου Διεθνούς Συνεδρίου Μαθηματικών.

[2] Για έναν εναλλακτικό αλγόριθμο δες τον ορισμό της συνάρτησης gcd στο Παράδειγμα 2.3.8.

Είσοδος: Μία ακολουθία από φυσικούς αριθμούς.

Βήμα 1: Γράφουμε σε μία σειρά τους αριθμούς.

Βήμα 2: Γράφουμε στην από κάτω σειρά τον μικρότερο από αυτούς και κάτω από τους άλλους το υπόλοιπο της διαίρεσης τους με αυτό τον αριθμό.

Βήμα 3: Επαναλαμβάνουμε το **Βήμα 2** έως ότου βρεθεί σειρά που περιέχει μόνο έναν αριθμό διαφορετικό του μηδενός.

Βήμα 4: Ο αριθμός αυτός είναι ο ΜΚΔ.

Όπως επίσης, αλγόριθμος μπορεί να θεωρηθεί και μία συνταγή μαγειρικής:

Είσοδος: Δύο αβγά, λάδι.

Βήμα 1: Ζεσταίνουμε το λάδι σε ένα μεγάλο τηγάνι σε μέτρια προς δυνατή φωτιά.

Βήμα 2: Σπάμε τα αυγά, ένα τη φορά, μέσα στο τηγάνι.

Βήμα 3: Γέρνουμε το τηγάνι και ρίχνουμε με ένα κουτάλι λάδι πάνω στους κρόκους.

Βήμα 4: Επαναλαμβάνουμε το **Βήμα 3** έως ότου το ασπράδι γίνει αδιαφανές.

Βήμα 5: Κατεβάζουμε τα αβγά από τη φωτιά και τα σερβίρουμε.

Φυσικά στο πλαίσιο αυτών των σημειώσεων δεν ενδιαφερόμαστε για αλγόριθμους της δεύτερης μορφής [1]. Βασικός μας σκοπός εδώ είναι, πρώτα να θεμελειώσουμε την έννοια του αλγορίθμου, έπειτα να ανακαλύψουμε προβλήματα που είναι μη-επιλύσιμα αλγοριθμικά και τέλος να κατατάξουμε αυτά τα προβλήματα ως προς τον βαθμό «μη-επιλισιμότητάς» τους.

Πόρισμα όσων δούμε στο δεύτερο μέρος των σημειώσεων είναι η διερεύνηση των δυνατοτήτων των «μηχανών υπολογισμού», όπως για παράδειγμα οι ηλεκτρονικοί υπολογιστές, και η ανακάλυψη προβλημάτων που δεν είναι επιλύσιμα από αυτές.

Προκειμένου να αποδείξουμε ότι δεν υπάρχει αλγόριθμος για κάποιο πρόβλημα θα πρέπει να τον ορίσουμε με αυστηρό τρόπο, ως μαθηματικό αντικείμενο. Έτσι, αντί να πρέπει να αποδείξουμε ότι δεν υπάρχει «πεπερασμένη ακολουθία απλών οδηγιών που διεκπεραιώνουν κάποια εργασία», θα πρέπει να αποδείξουμε την μη ύπαρξη του συγκεκριμένου μαθηματικού αντικειμένου.

Για το λόγο αυτό ασπαζόμαστε τη *Θέση Church-Turing*, οι οποίοι τη δεκαετία 1930, ανεξάρτητα ο ένας από τον άλλο, προσπάθησαν να δώσουν έναν τυπικό ορισμό του αλγορίθμου (τουλάχιστον τυπικότερο του διαισθητικού), ο μεν Church χρησιμοποιώντας ένα «συμβολικό» σύστημα τον λ-λογισμό και ο δε Turing ένα «μηχανιστικό» σύστημα τις TM. Είδαμε ότι τα δύο αυτά «μοντέλα υπολογισμού» είναι ισοδύναμα μεταξύ τους, όπως επίσης είναι

[1] Αν ο αναγώστης όμως ενδιαφέρεται, θα βρει πολλούς αλγορίθμους αυτής της μορφής εδώ: `https://akispetretzikis.com`.

ισοδύναμα και με τις ελαχιστικά αναδρομικές συναρτήσεις και τις γενικές γραμματικές [1]. Συνεπώς, χωρίς αναστολές μπορούμε να θεωρήσουμε ότι αλγόριθμος είναι, παραδείγματος χάρη, μία TM:

Θέση Church-Turing. Αλγοριθμικά υπολογίσιμες συναρτήσεις [2] είναι ακριβώς οι Turing υπολογίσιμες συναρτήσεις.

Πρωτού κλείσουμε αυτήν την εισαγωγική παράγραφο, ας αποδείξουμε ότι το $10^{ο}$ πρόβλημα του Hilbert είναι «μη επιλύσιμο» (παραθέτοντας το κεντρικό Λήμμα της απόδειξης, το Θεώρημα 5.1.6, χωρίς απόδειξη). Αυτό θα μας εισάγει στη μεθοδολογία που θα εφαρμόζουμε για να απαντάμε σε ερωτήματα που αφορούν την ύπαρξη ή όχι αλγορίθμου για κάποιο πρόβλημα.

Ξεκινάμε δίνοντας τους ορισμούς που χρειαζόμαστε για να ορίσουμε τυπικά το πρόβλημα και να το μεταφέρουμε στον δικό μας συμβολισμό.

Ορισμός 5.1.2. *Πολυωνυμική διοφαντική εξίσωση με ακέραιους συντελεστές (Π.Δ.Ε.)* είναι μία εξίσωση της μορφής:

$$P(x_1, \dots, x_n) = \sum_{i=1}^{m} a_i x_1^{k_{1_i}} \cdots x_n^{k_{n_i}} = 0$$

όπου $a_i \in \mathbb{Z}$ (οι *συντελεστές*) και $k_{1_i}, \dots, k_{n_i} \in \mathbb{N}$ (οι δυνάμεις των *μεταβλητών* $x_1, \dots, x_n$), για κάθε $i \in [m]$. *Ακέραια ρίζα* της εξίσωσης $P(x_1, \dots, x_n) = 0$ είναι μία n-άδα $(z_1, \dots, z_n) \in \mathbb{Z}^n$ τέτοια ώστε $P(z_1, \dots, z_n) = 0$.

Παράδειγμα 5.1.3. Μία Π.Δ.Ε. με τρείς μεταβλητές είναι η $3x^2 - 2xy - y^2z - 7 = 0$. Η εξίσωση αυτή έχει πολλές ακέραιες ρίζες, μία από αυτές είναι η $x = 1,\ y = 2,\ z = -2$.

Συμβολισμός 5.1.4. Έστω Π.Δ.Ε. $P(x_1, x_2, \dots, x_n) = \sum_{i=1}^{m} a_i x_1^{k_{1_i}} x_2^{k_{2_i}} \cdots x_n^{k_{n_i}} = 0$ και $s \in \mathbb{Z}$. Με P_s συμβολίζουμε την Π.Δ.Ε. $P(s, x_2, \dots, x_n) = \sum_{i=1}^{m} a_i s^{k_{1_i}} x_2^{k_{2_i}} \cdots x_n^{k_{n_i}} = 0$.

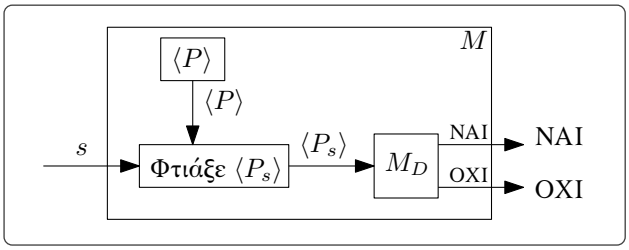
Θεωρώντας μια κωδικοποίηση των Π.Δ.Ε. σε ένα αλφάβητο, έστω το $\{0, 1\}$, μπορούμε να εκφράσουμε το $10^{ο}$ πρόβλημα του Hilbert ως εξής:

Το $10^{ο}$ πρόβλημα του Hilbert με ορολογία TM
Δείξτε (κατασκευαστικά) ότι η γλώσσα $D = \{\langle P \rangle \in \{0,1\}^* \mid P$ είναι Π.Δ.Ε. με ακέραιες ρίζες$\}$ είναι αναδρομική.

καθώς ενδιαφερόμαστε για την εύρεση ενός αλγορίθμου – δηλαδή μίας TM σύμφωνα με τη θέση Church-Turing – που δεχόμενος ως είσοδο μία Π.Δ.Ε. α) να τερματίζει πάντα και β) να μας επιστρέφει απάντηση «Ναι» ανν η εξίσωση έχει ακέραιες ρίζες.

[1] Επιπλέον έχει αποδειχθεί ότι είναι ισοδύναμα με όλα τα υπόλοιπα «ρεαλιστικά» μοντέλα υπολογισμού που έχουν προταθεί (όπως π.χ. τα προγράμματα McCarthy, το μοντέλο του Post, ακόμα και το μοντέλο RAM πάνω στο οποίο βασίζονται οι σύγχρονοι ηλεκτρονικοί υπολογιστές).

[2] Χρησιμοποιώντας οσοδήποτε μεγάλους υπολογιστικούς πόρους (χώρο, χρόνο, πλήθος παράλληλων επεξεργαστών κλπ.) αλλά πεπερασμένους.



Σχήμα 5.1.1: *Η TM M στην απόδειξη ότι $D \notin$ REC.*

Ορισμός 5.1.5. Ένα σύνολο $S \subseteq \mathbb{N}$ καλείται *διοφαντικό* ανν υπάρχει Π.Δ.Ε. $P(x_1, \ldots, x_{n+1})$ τέτοια ώστε

$$s \in S \Leftrightarrow \exists z_1, \ldots, z_n \in \mathbb{Z}\ (P(s, z_1, \ldots, z_n) = 0)$$

Το ακόλουθο Θεώρημα αποδείχθηκε το 1970 και έδωσε «αρνητική απάντηση» στο $10^{ο}$ πρόβλημα του Hilbert.

Θεώρημα 5.1.6 (Matiyasevich, Robinson, Davis, Putman). Κάθε αναδρομικά απαριθμήσιμο σύνολο είναι διοφαντικό.

Θεώρημα 5.1.7. $D \notin$ REC.

Απόδειξη. Έστω (προς άτοπο) ότι $D \in$ REC και ότι η TM M_D την αποφασίζει. Έστω επίσης $L \in$ RE $\setminus$ REC [1]. Αφού $L \in$ RE, από το Θεώρημα 5.1.6, υπάρχει Π.Δ.Ε. $P(x_1, \ldots, x_{n+1})$, για κάποιο $n \in \mathbb{N}$, τέτοια ώστε:

$$L = \{s \in \mathbb{N} \mid \exists z_1, \ldots, z_n \in \mathbb{Z}\ (P(s, z_1, \ldots, z_n) = 0)\}$$

Η TM M του Σχήματος 5.1.1 αποφασίζει την L. Άτοπο καθώς $L \notin$ REC. □

5.2 Μη-αποφανσιμότητα γλωσσών

5.2.1 Το πρόβλημα του τερματισμού

Μία γλώσσα που παρουσιάζει πολύ μεγάλο ενδιαφέρον είναι η:

$$HP = \{\langle M, w\rangle \in \{0,1\}^* \mid M(w)\downarrow\}$$ [2]

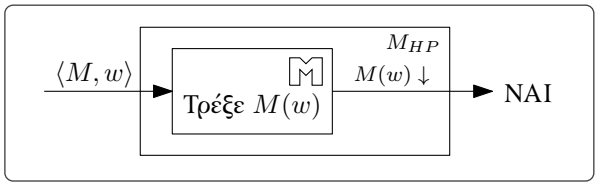
Η γλώσσα αυτή είναι γνωστή και ως *πρόβλημα του τερματισμού* καθώς περιέχει τις δυάδες κωδικοποιήσεων TM και λέξης για την οποία ο υπολογισμός τερματίζει.

[1] Εδώ χρησιμοποιούμε ανεπίσημα το γεγονός ότι REC $\subset$ RE, παρόλο που δεν το έχουμε αποδείξει ακόμα. Θα το κάνουμε όμως, με κάθε επισημότητα, στην παράγραφο που ακολουθεί. Επίσης, θεωρούμε ότι οι γλώσσες που εξετάζουμε είναι υποσύνολα του $\mathbb{N}$.

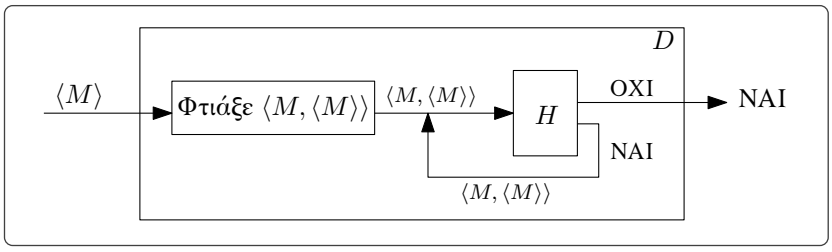
[2] Πιο τυπικά θα έπρεπε να ορίσουμε τη HP ως εξής:

$$HP = \{w \in \{0,1\}^* \mid \exists \text{ TM } M\ \exists w' \in \{0,1\}^* (w = \langle M, w'\rangle \wedge M(w')\downarrow)\}$$

Θα υποπέσουμε σε αυτή την «παρατυπία» κατ' εξακολούθηση σε όσα έπονται.



Σχήμα 5.2.1: *Η TM M_{HP} ημι-αποφασίζει την HP.*



Σχήμα 5.2.2: *Η TM D στην απόδειξη του Θεωρήματος 5.2.1.*

Μέσα από το θεώρημα που ακολουθεί θα δούμε ότι η απάντηση στο Ερώτημα 1 (Σελίδα 28) είναι καταφατική και μάλιστα μία γλώσσα που έχει αυτήν την ιδιότητα είναι η HP. Θα μπορούσαμε να πούμε ότι το πρόβλημα του τερματισμού είναι μη-επιλύσιμο καθώς δεν υπάρχει αλγόριθμος (TM δηλαδή) που να μας επιστρέφει και τις θετικές αλλά και τις αρνητικές απαντήσεις [1]. Η γλώσσα αυτή όπως θα δούμε θα ανοίξει τον ασκό του Αιόλου όσον αφορά τα μη-επιλύσιμα προβλήματα.

Θεώρημα 5.2.1. $HP \in \mathsf{RE} \setminus \mathsf{REC}$.

Απόδειξη. Η HP ανήκει στο RE καθώς η TM M_{HP} που φαίνεται στο Σχήμα 5.2.1 την ημι-αποφασίζει [2].Έστω (προς άτοπο) ότι $HP \in \mathsf{REC}$ και ότι η TM H την αποφασίζει. Θεωρούμε την TM D του Σχήματος 5.2.2 και παρατηρούμε ότι:

$$D(\langle D\rangle)\downarrow \Leftrightarrow H(\langle D, \langle D\rangle\rangle)\downarrow_{q_{\text{όχι}}} \Leftrightarrow \langle D, \langle D\rangle\rangle \notin HP \Leftrightarrow D(\langle D\rangle)\uparrow$$

Άτοπο, άρα $HP \notin \mathsf{REC}$. □

Παρατήρηση 5.2.2. Η απόδειξη του Θεωρήματος 5.2.1 αποτελεί παράδειγμα του *διαγώνιου επιχειρήματος του Cantor* [3]. Ας θεωρήσουμε την αρίθμηση των TM σύμφωνα με τον

[1] Υπάρχει αλγόριθμος που επιστρέφει τις θετικές απαντήσεις αλλά όχι (όλες) τις αρνητικές. Συνεπώς έχουμε έναν αλγόριθμο που δεν μπορεί να επιστρέψει πάντα απάντηση και, ως εκ τούτου, δεν επιλύει το πρόβλημα.

[2] Σύμφωνα με τη Σύμβαση 1.4.16 η καθολική TM για εισόδους που δεν αποτελούν κωδικοποίηση TM και λέξης απορρίπτει την είσοδό της. Επομένως οι μόνες «ενδιαφέρουσες» είσοδοι για την M_{HP} είναι οι λέξεις που αποτελούν κωδικοποίηση TM και λέξης. Συνεπώς, αντί να προσθέσουμε στην περιγραφή της M_{HP} έναν έλεγχο για το αν η είσοδος αποτελεί κωδικοποίηση TM και λέξης, θα περιγράφουμε τη λειτουργία της μόνο για εισόδους αυτής της μορφής. Αυτή την πρακτική θα την εφαρμόσουμε πολλές φορές στη συνέχεια (ακόμα και όταν περιγράφουμε TM που δεν χρησιμοποιούν την καθολική TM, δες για παράδειγμα την TM του Σχήματος 5.2.2).

[3] Έχουμε εφαρμόσει ήδη δύο φορές αυτό το επιχείρημα, στις αποδείξεις των Θεωρημάτων 0.1.17 και 4.2.11.

αριθμό Gödel τους και ας δούμε τον πίνακα που περιέχει τις τιμές της συνάρτησης ϕ_k, που υπολογίζει η TM με αριθμό Gödel k, με είσοδο τις κωδικοποιήσεις των TM (δες τους Ορισμούς 1.2.13 και 1.4.10 καθώς και τη Σύμβαση 1.2.15):

	$\langle M_1 \rangle$	$\langle M_2 \rangle$	$\langle M_3 \rangle$	$\cdots$	$\langle M_k \rangle$	$\cdots$
M_1	$\phi_1(\langle M_1 \rangle)$	$\phi_1(\langle M_2 \rangle)$	$\phi_1(\langle M_3 \rangle)$	$\cdots$	$\phi_1(\langle M_k \rangle)$	$\cdots$
M_2	$\phi_2(\langle M_1 \rangle)$	$\phi_2(\langle M_2 \rangle)$	$\phi_2(\langle M_3 \rangle)$	$\cdots$	$\phi_2(\langle M_k \rangle)$	$\cdots$
M_3	$\phi_3(\langle M_1 \rangle)$	$\phi_3(\langle M_2 \rangle)$	$\phi_3(\langle M_3 \rangle)$	$\cdots$	$\phi_3(\langle M_k \rangle)$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$
M_k	$\phi_k(\langle M_1 \rangle)$	$\phi_k(\langle M_2 \rangle)$	$\phi_k(\langle M_3 \rangle)$	$\cdots$	$\phi_k(\langle M_k \rangle)$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Φυσικά κάποιες τιμές σε αυτόν τον πίνακα δεν θα ορίζονται (θα έχουν τιμή $\perp$ δηλαδή).

Η (υποτιθέμενη) ύπαρξη της TM H (που αποφασίζει την HP) μας οδηγεί στην (υποτιθέμενη) ύπαρξη της TM D, η οποία προφανώς οφείλει να εμφανίζεται στον πίνακα, ας πούμε στη θέση d (δηλαδή $\mathsf{Gödel}(D) = d$, ή αλλιώς η D ταυτίζεται με την M_d). Όμως η συνάρτηση που υπολογίζει η D «αντιστρέφει» (υπο μία έννοια) την τιμή της διαγωνίου του πίνακα, καθώς:

$$\begin{aligned} \phi_d(\langle M_k \rangle) \neq \perp \quad &, \quad \text{αν } \phi_k(\langle M_k \rangle) = \perp \\ \phi_d(\langle M_k \rangle) = \perp \quad &, \quad \text{αν } \phi_k(\langle M_k \rangle) \neq \perp \end{aligned}$$

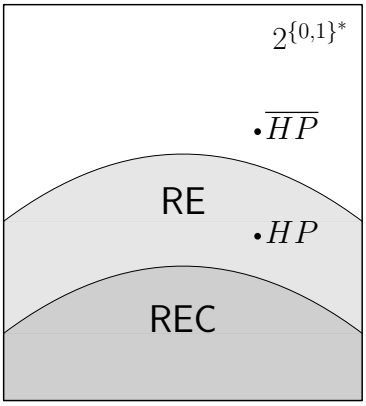
Αναπόφευκτα θα οδηγηθούμε σε άτοπο όταν εξετάσουμε την τιμή $\phi_d(\langle M_d \rangle)$.

Στοχαζόμενοι πάνω στο αποτέλεσμα του Θεωρήματος 5.2.1 μπορούμε να φέρουμε στο μυαλό μας το ακόλουθο καθημερινό σενάριο:

> *Έχουμε γράψει τον κώδικα ενός προγράμματος (στη γλώσσα προγραματισμού που προτιμούμε) και τον τρέχουμε στον υπολογιστή μας δίνοντας του κάποια είσοδο. Καθώς ο υπολογισμός αργεί να τερματίσει αρχίζουμε να αναρωτιώμαστε αν θα τερματίσει τελικά ή όχι...*

Παρόλο που τις περισσότερες φορές, όταν έχουμε να κάνουμε με απλά προγράμματα, μπορούμε με διάφορες ευρετικές μεθόδους να διαπιστώσουμε αν θα τερματίσουν για μία δεδομένη είσοδο, γενικά το μόνο που μπορούμε να κάνουμε είναι απλά να περιμένουμε να δούμε τελικά τι θα γίνει. Αυτό το συμπέρασμα προκύπτει από το Θεώρημα 5.2.1 καθώς μας αποδεικνύει ότι δεν υπάρχει αλγόριθμος που να αποφασίζει (γενικά) αν ένα πρόγραμμα θα τερματίσει για δεδομένη είσοδο.

Πόρισμα 5.2.3. $\overline{HP} \notin \mathsf{RE}$.



Σχήμα 5.2.3: *Η σχέση εγκλεισμού μεταξύ* REC *και* RE.

Πράγματι, αν υποθέσουμε (προς άτοπο) ότι $\overline{HP} \in$ RE, θα είχαμε ότι $HP, \overline{HP} \in$ RE, άρα από το Θεώρημα 1.5.4 θα έπρεπε να ίσχυε ότι $HP \in$ REC που αντιβαίνει στο Θεωρήμα 5.2.1.

Πλέον είμαστε σε θέση να εμπλουτίσουμε το Σχήμα 1.2.13 προσθέτοντας σε αυτό τις γλώσσες HP και $\overline{HP}$ (Σχήμα 5.2.3). Το παρακάτω πόρισμα προκύπτει άμεσα από την Πρόταση 1.2.38.

Πόρισμα 5.2.4. Η χαρακτηριστική συνάρτηση της γλώσσας HP δεν είναι υπολογίσιμη.

Η χ_{HP} είναι η πρώτη συνάρτηση που αποδεδειγμένα δεν είναι υπολογίσιμη. Μέχρι τώρα γνωρίζαμε ότι υπάρχουν μη-υπολογίσιμες συναρτήσεις αλλά δεν είχαμε στα χέρια μας κάποιο παράδειγμα (η απόδειξη δεν ήταν κατασκευαστική) [1].

5.2.2 Απεικονιστικές Αναγωγές

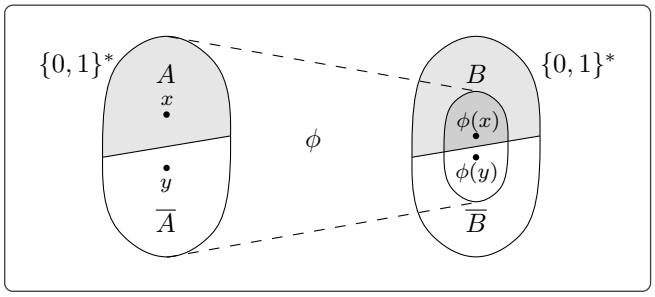
Σε αυτήν την παράγραφο θα παρουσιάσουμε τη μεθοδολογία που θα ακολουθούμε για να αποδεικνύουμε ότι μία γλώσσα δεν είναι αναδρομική (ή αναδρομικά απαριθμήσιμη). Θα μπορούσαμε φυσικά κάθε φορά να επαναλαμβάναμε την απόδειξη του Θεωρήματος 5.2.1, αυτό όμως (όπως πιθανώς να παρατηρήσατε) θα ήταν κάπως κουραστικό. Αντ' αυτού θα μημυθούμε την απόδειξη του Θεωρήματος 5.1.6.

Ορισμός 5.2.5. Έστω γλώσσες $A, B \subseteq \{0,1\}^*$. Η A *ανάγεται (απεικονιστικά) στη* B, συμβολισμός $A \leq_m B$, ανν υπάρχει συνάρτηση $\phi : \{0,1\}^* \to \{0,1\}^*$, τέτοια ώστε:

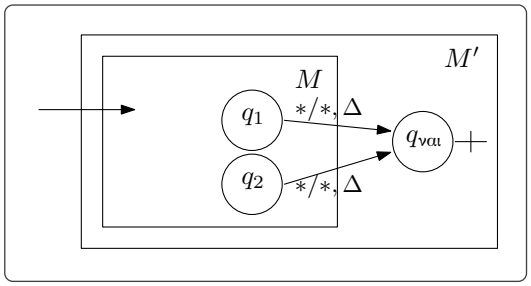
1. Η ϕ είναι πλήρης και υπολογίσιμη.
2. $\forall w \in \{0,1\}^* \ (w \in A \leftrightarrow \phi(w) \in B)$

Η συνάρτηση ϕ καλείται *(απεικονιστική ή many-one) αναγωγή της* A *στη* B (Σχήμα 5.2.4).

[1] Ενδεχομένως να προκαλεί εντύπωση το γεγονός ότι η πρώτη μη-υπολογίσιμη συνάρτηση που συναντάμε δεν είναι κάποια «περίεργη» μερική συνάρτηση. Είναι μία ολική συνάρτηση και μάλιστα αφορά ένα πολύ στοιχειώδες ερώτημα αναφορικά με τις TM.



Σχήμα 5.2.4: *Η ϕ είναι αναγωγή της A στην B.*



Σχήμα 5.2.5: *Η ΤΜ M' στην αναγωγή της HP στην $L_{Αποδοχής}$.*

Παράδειγμα 5.2.6. Θεωρούμε τη γλώσσα $L_{\text{Αποδοχής}} = \{\langle M, w\rangle \in \{0,1\}^* \mid M(w) \downarrow_{q_{\text{ναι}}}\}$. Θα ορίσουμε μία συνάρτηση $\phi : \{0,1\}^* \to \{0,1\}^*$ ως εξής:

- Για τα $x \in \{0,1\}^*$ για τα οποία υπάρχει ΤΜ M και $w \in \{0,1\}^*$ τέτοιες ώστε $x = \langle M, w\rangle$, $\phi(x) = \langle M', w\rangle$ όπου M' είναι η ΤΜ του Σχήματος 5.2.5 που:

  α) περιέχει την M σαν υπορουτίνα, έχοντας όμως «αποχαρακτηρίσει» τις τερματικές καταστάσεις της, οι οποίες πλέον είναι οι (απλές) καταστάσεις q_1, q_2 και

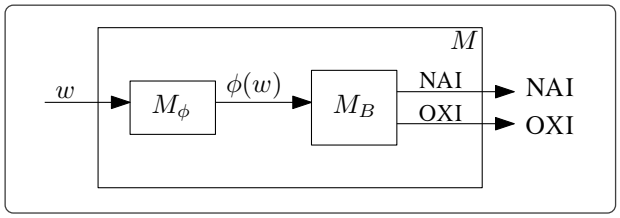
  β) μεταβαίνει στην $q_{\text{ναι}}$ (μόνο) μέσω των καταστάσεων q_1, q_2 όποιο σύμβολο και να διαβάσει.

- Σε διαφορετική περίπτωση $\phi(x) = x$.

Παρατηρούμε ότι η ϕ είναι αναγωγή της HP στην $L_{\text{Αποδοχής}}$, καθώς:

1. Η ϕ είναι πλήρης και υπολογίσιμη.

2. - $x \in HP \Rightarrow \exists$ ΤΜ M $\exists w \in \{0,1\}^*(x = \langle M, w\rangle \wedge \langle M, w\rangle \in HP) \Rightarrow M(w) \downarrow \Rightarrow M(w) \downarrow_{q_{\text{ναι}}}$ ή $M(w) \downarrow_{q_{\text{όχι}}} \Rightarrow M'(w) \downarrow_{q_1}$ ή $M'(w) \downarrow_{q_2} \Rightarrow M'(w) \downarrow_{q_{\text{ναι}}} \Rightarrow \phi(\langle M, w\rangle) \in L_{\text{Αποδοχής}}$
   - $x \notin HP \Rightarrow$ Είτε $\neg(\exists$ ΤΜ M $\exists w \in \{0,1\}^*(x = \langle M, w\rangle))$, είτε $\exists$ ΤΜ M $\exists w \in \{0,1\}^*(x = \langle M, w\rangle \wedge \langle M, w\rangle \notin HP))$:



Σχήμα 5.2.6: *Η ΤΜ στην απόδειξη του Θεωρήματος 5.2.7.*

α. Στην πρώτη περίπτωση $\phi(x) = x$ και προφανώς $x \notin L_{\text{Αποδοχής}}$.

β. Στην δεύτερη περίπτωση $\langle M, w\rangle \notin HP \Rightarrow M(w) \uparrow \Rightarrow M'(w) \uparrow \Rightarrow \phi(\langle M, w\rangle) \notin L_{\text{Αποδοχής}}$.

Συνεπώς $HP \leq_m L_{\text{Αποδοχής}}$.

Θεώρημα 5.2.7. Έστω $A, B \subseteq \{0,1\}^*$. Αν $A \leq_m B$ και $B \in$ REC ($B \in$ RE) τότε $A \in$ REC ($A \in$ RE αντίστοιχα).

Απόδειξη. Έστω ϕ η αναγωγή της A στη B, έστω M_ϕ η ΤΜ που την υπολογίζει και M_B η ΤΜ που αποφασίζει (ημι-αποφασίζει) τη B. Η ΤΜ του Σχήματος 5.2.6 αποφασίζει (ημι-αποφασίζει) την A καθώς [1]:

- $w \in A \Leftrightarrow \phi(w) \in B \Leftrightarrow M_B(\phi(w)) \downarrow_{q_{\text{ναι}}} \Leftrightarrow M(w) \downarrow_{q_{\text{ναι}}}$
- $w \notin A \Leftrightarrow \phi(w) \notin B \Leftrightarrow M_B(\phi(w)) \downarrow_{q_{\text{όχι}}} \Leftrightarrow M(w) \downarrow_{q_{\text{όχι}}}$

Συνεπώς, $A \in$ REC ($A \in$ RE). □

Για τους δικούς μας σκοπούς θα χρησιμοποιούμε κατά κύριο λόγο το ακόλουθο (άμεσο) πόρισμα του Θεωρήματος 5.2.7.

Πόρισμα 5.2.8. Έστω $A, B \subseteq \{0,1\}^*$. Αν $A \leq_m B$ και $A \notin$ REC ($A \notin$ RE) τότε $B \notin$ REC ($B \notin$ RE αντίστοιχα).

Παράδειγμα 5.2.9. Στο Παράδειγμα 5.2.6 είδαμε ότι $HP \leq_m L_{\text{Αποδοχής}}$, επομένως, αφού $HP \notin$ REC έπεται ότι $L_{\text{Αποδοχής}} \notin$ REC.

Σημείωση 5.2.10. Αν για τις γλώσσες $A, B \subseteq \{0,1\}^*$ ισχύει ότι $A \leq_m B$, διαισθητικά η B αντιστοιχεί σε πιο «δύσκολο πρόβλημα» από την A, καθώς αν υπάρχει αλγόριθμος που «λύνει» τη B τότε υπάρχει και αλγόριθμος που «λύνει» την A. Αυτή η «διαίσθηση» θα γίνει μαθηματική απόδειξη στο Κεφάλαιο 8.

Σύμβαση 5.2.11. Προκειμένου να στρέψουμε την προσοχή του αναγνώστη στην ουσία μίας συνάρτησης αναγωγής ϕ θα την παρουσιάζουμε αναλυτικά μόνο για τις εισόδους που έχουν «ενδιαφέρον» για εμάς (για τις υπόλοιπες ναι μεν θα ορίζουμε τη ϕ αλλά δεν θα ελέγχουμε αν πληρούται η δεύτερη προϋπόθεση του Ορισμού 5.2.5).

[1] Η δεύτερη παύλα είναι που διαφοροποιεί τις περιπτώσεις του REC και του RE.

Παραδείγματα μη-αναδρομικών γλωσσών

Στη συνέχεια θα δούμε μερικά ακόμα παραδείγματα γλωσσών που δεν είναι αναδρομικές (ή και αναδρομικά απαριθμήσιμες). Τα παραδείγματα αυτά θα μας αποκαλύψουν μερικά προβλήματα που είναι πέραν των «δυνατοτήτων» των ΤΜ και κατ' επέκταση (λόγω της Θέσης Church-Turing) αλγοριθμικά μη-επιλύσιμα.

Παράδειγμα 5.2.12. Θεωρούμε τη γλώσσα $L = \{\langle M, w, q\rangle \in \{0,1\}^* \mid \text{Η } M(w) \text{ μεταβαίνει στην κατάσταση } q\}$. Η συνάρτηση $\phi : \{0,1\}^* \to \{0,1\}^*$ με:

$$\phi(x) = \begin{cases} \langle M, w, q_{\text{ναι}}\rangle & , \text{ αν υπάρχει ΤΜ } M \text{ και } w \in \{0,1\}^* \text{ τέτοια ώστε } x = \langle M, w\rangle \\ \langle M_{\uparrow}, w, q_{\text{ναι}}\rangle & , \text{ αλλιώς} \end{cases}$$

όπου $M_{\uparrow}$ μία ΤΜ που δεν τερματίζει ποτέ, είναι αναγωγή της $L_{\text{Αποδοχής}}$ στην L καθώς:

1. ϕ πλήρης και υπολογίσιμη.

2. - $\langle M, w\rangle \in L_{\text{Αποδοχής}} \Rightarrow M(w) \downarrow_{q_{\text{ναι}}} \Rightarrow \langle M, w, q_{\text{ναι}}\rangle \in L$
   - $\langle M, w\rangle \notin L_{\text{Αποδοχής}} \Rightarrow M(w) \uparrow$ ή $M(w) \downarrow_{q_{\text{όχι}}} \Rightarrow M(w) \not\downarrow_{q_{\text{ναι}}} \Rightarrow \langle M, w, q_{\text{ναι}}\rangle \notin L$

Αφού $L_{\text{Αποδοχής}} \notin \mathsf{REC}$ έπεται ότι $L \notin \mathsf{REC}$.

Σημείωση 5.2.13. Από το Παράδειγμα 5.2.12 συμπεραίνουμε ότι δεν μπορούμε να γνωρίζουμε αν μία ΤΜ περνάει από κάποια συγκεκριμένη κατάσταση κατά τον υπολογισμό της με είσοδο μία (τυχούσα) λέξη w [1].

Παράδειγμα 5.2.14. Θεωρούμε τη γλώσσα $L_\epsilon = \{\langle M\rangle \in \{0,1\}^* \mid M(\epsilon) \downarrow q_{\text{ναι}}\}$. Η συνάρτηση $\phi : \{0,1\}^* \to \{0,1\}^*$ με:

$$\phi(x) = \begin{cases} \langle M_w\rangle & , \text{ αν υπάρχει ΤΜ } M \text{ και } w \in \{0,1\}^* \text{ τέτοια ώστε } x = \langle M, w\rangle \\ \langle M_{\uparrow}\rangle & , \text{ αλλιώς} \end{cases}$$

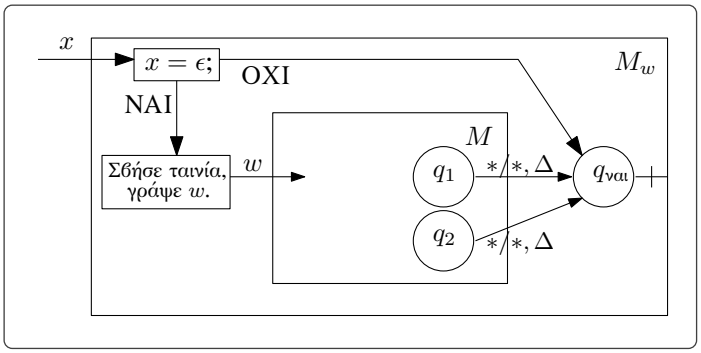
όπου M_w η ΤΜ στο Σχήμα 5.2.7 (οι q_1, q_2 έχουν αντικαταστήσει τις $q_{\text{ναι}}$, $q_{\text{όχι}}$ της M) και $M_{\uparrow}$ μία ΤΜ που δεν τερματίζει ποτέ, είναι αναγωγή της HP στην L_ϵ καθώς:

1. ϕ πλήρης και υπολογίσιμη.

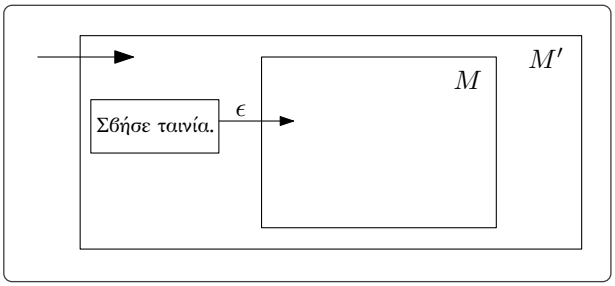
2. - $\langle M, w\rangle \in HP \Rightarrow M(w) \downarrow \Rightarrow M_w(\epsilon) \downarrow q_{\text{ναι}} \Rightarrow \langle M_w\rangle \in L_\epsilon$
   - $\langle M, w\rangle \notin HP \Rightarrow M(w) \uparrow \Rightarrow M_w(\epsilon) \uparrow \Rightarrow \langle M_w\rangle \notin L_\epsilon$

Αφού $HP \notin \mathsf{REC}$ έπεται ότι $L_\epsilon \notin \mathsf{REC}$.

[1] Σε αντίθετη περίπτωση (όπως φαίνεται από τη συνάρτησή αναγωγής) θα μπορούσαμε να ξέρουμε αν θα περάσει και από την $q_{\text{ναι}}$, πράγμα που θα καθιστούσε την $L_{\text{Αποδοχής}}$ αναδρομική γλώσσα.



Σχήμα 5.2.7: *Η TM M_w στην αναγωγή της HP στην L_ϵ.*



Σχήμα 5.2.8: *Η TM M' στην αναγωγή της L_ϵ στην L_∞.*

Παράδειγμα 5.2.15. Θεωρούμε τη γλώσσα $L_\infty = \{\langle M\rangle \in \{0,1\}^* \mid |L(M)| = \aleph_0\}$. Η συνάρτηση $\phi : \{0,1\}^* \to \{0,1\}^*$ με:

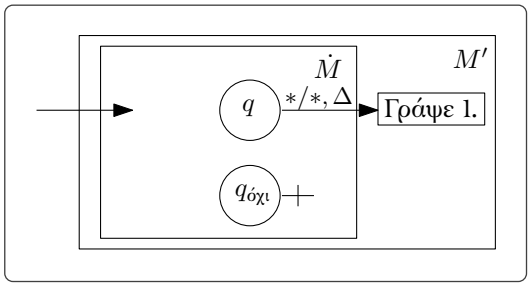
$$\phi(x) = \begin{cases} \langle M'\rangle & \text{, αν υπάρχει TM } M \text{ τέτοια ώστε } x = \langle M\rangle \\ x & \text{, αλλιώς} \end{cases}$$

όπου M' η TM στο Σχήμα 5.2.8, είναι αναγωγή της L_ϵ στην L_∞ καθώς:

1. ϕ πλήρης και υπολογίσιμη.
2. - $\langle M\rangle \in L_\epsilon \Rightarrow M(\epsilon) \downarrow_{q_{\text{ναι}}} \Rightarrow \forall w \in \{0,1\}^*(M'(w) \downarrow_{q_{\text{ναι}}}) \Rightarrow L(M') = \{0,1\}^* \Rightarrow |L(M')| = \aleph_0 \Rightarrow \langle M'\rangle \in L_\infty$
   - $\langle M\rangle \notin L_\epsilon \Rightarrow M(\epsilon) \nmid_{q_{\text{ναι}}} \Rightarrow \forall w \in \{0,1\}^*(M'(w) \nmid_{q_{\text{ναι}}}) \Rightarrow L(M') = \varnothing \Rightarrow |L(M')| = 0 \Rightarrow \langle M'\rangle \notin L_\infty$

Αφού $L_\epsilon \notin$ REC έπεται ότι $L_\infty \notin$ REC.

Παρατήρηση 5.2.16. Η συνάρτηση ϕ του Παραδείγματος 5.2.15 είναι και αναγωγή της L_ϵ στη γλώσσα $L_{\{0,1\}^*} = \{\langle M\rangle \in \{0,1\}^* \mid L(M) = \{0,1\}^*\}$. Επομένως $L_{\{0,1\}^*} \notin$ REC.



Σχήμα 5.2.9: *Η ΤΜ M' στην αναγωγή της $L_{\text{Αποδοχής}}$ στη γλώσσα του Παραδείγματος 5.2.17.*

Παράδειγμα 5.2.17. Θεωρούμε τη γλώσσα $L = \{\langle M, w\rangle \in \{0,1\}^* \mid$Η $M(w)$ γράφει 1 στην ταινία$\}$. Η συνάρτηση $\phi : \{0,1\}^* \to \{0,1\}^*$ με:

$$\phi(x) = \begin{cases} \langle M', \dot{w}\rangle & \text{, αν υπάρχει ΤΜ } M \text{ και } w \in \{0,1\}^* \text{ τέτοια ώστε } x = \langle M, w\rangle \\ x & \text{, αλλιώς} \end{cases}$$

όπου M' η ΤΜ στο Σχήμα 5.2.9, όπου η $\dot{M}$ και η $\dot{w}$ προκύπτουν αν αντικαταστήσουμε στη συνάρτηση μεταβάσεων της $\langle M\rangle$ και στη w αντίστοιχα κάθε σύμβολο $* \in \{0,1\}^*$ με το σύμβολο $\dot{*}$ [1] (η q έχει αντικαταστήσει την $q_{\text{ναι}}$ της $\dot{M}$). Η ϕ είναι αναγωγή της $L_{\text{Αποδοχής}}$ στην L καθώς:

1. ϕ πλήρης και υπολογίσιμη.
2. - $\langle M, w\rangle \in L_{\text{Αποδοχής}} \Rightarrow M(w) \downarrow_{q_{\text{ναι}}} \Rightarrow M'(\dot{w}) \downarrow_q \Rightarrow$ Η $M'(\dot{w})$ θα γράψει $1 \Rightarrow \langle M', \dot{w}\rangle \in L$
   - $\langle M, w\rangle \notin L_{\text{Αποδοχής}} \Rightarrow M(w) \nmid_{q_{\text{ναι}}} \Rightarrow$ Η $M'(\dot{w})$ δεν θα επισκεφτεί την $q \Rightarrow$ Η $M'(\dot{w})$ δεν θα γράψει 1$\Rightarrow \langle M', \dot{w}\rangle \notin L$

Αφού $L_{\text{Αποδοχής}} \notin$ REC έπεται ότι $L \notin$ REC.

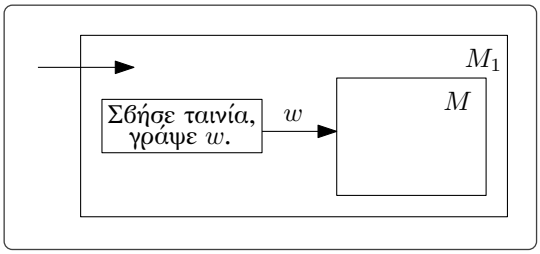
Παράδειγμα 5.2.18. Θεωρούμε τη γλώσσα $L_{\equiv} = \{\langle M_1, M_2\rangle \in \{0,1\}^* \mid L(M_1) = L(M_2)\}$. Η συνάρτηση $\phi : \{0,1\}^* \to \{0,1\}^*$ με:

$$\phi(x) = \begin{cases} \langle M_1, M_{\text{ναι}}\rangle & \text{, αν υπάρχει ΤΜ } M \text{ και } w \in \{0,1\}^* \text{ τέτοια ώστε } x = \langle M, w\rangle \\ \langle M_\uparrow, M_{\text{ναι}}\rangle & \text{, αλλιώς} \end{cases}$$

όπου M_1 η ΤΜ στο Σχήμα 5.2.10, $M_\uparrow$ μία ΤΜ που δεν τερματίζει ποτέ και $M_{\text{ναι}}$ μία ΤΜ που αποδέχεται κάθε λέξη. Η ϕ είναι αναγωγή της $L_{\text{Αποδοχής}}$ στην $L_{\equiv}$ καθώς:

1. ϕ πλήρης και υπολογίσιμη.
2. - $\langle M, w\rangle \in L_{\text{Αποδοχής}} \Rightarrow M(w) \downarrow_{q_{\text{ναι}}} \Rightarrow \forall x \in \{0,1\}^*(M_1(x) \downarrow_{q_{\text{ναι}}}) \Rightarrow L(M_1) = \{0,1\}^* = L(M_{\text{ναι}}) \Rightarrow \langle M_1, M_{\text{ναι}}\rangle \in L_{\equiv}$

[1] Τα σύμβολα $\dot{0}$ και $\dot{1}$ αποτελούν σύμβολα του αλφαβήτου ταινίας της ΤΜ M' και θεωρούμε ότι δεν υπάρχουν στο αλφάβητο ταινίας της M. Επίσης θεωρούμε ότι η $\langle M', \dot{w}\rangle$ είναι κωδικοποιημένη στο $\{0,1\}$.



Σχήμα 5.2.10: *Η ΤΜ M_1 στην αναγωγή της $L_{\text{Αποδοχής}}$ στην $L_{\equiv}$.*

- $\langle M, w\rangle \notin L_{\text{Αποδοχής}} \Rightarrow M(w) \nmid_{q_{\text{ναι}}} \Rightarrow \forall x \in \{0,1\}^*(M_1(x) \nmid_{q_{\text{ναι}}}) \Rightarrow L(M_1) = \varnothing \neq L(M_{\text{ναι}}) \Rightarrow \langle M_1, M_{\text{ναι}}\rangle \notin L_{\equiv}$

Αφού $L_{\text{Αποδοχής}} \notin \mathsf{REC}$ έπεται ότι $L_{\equiv} \notin \mathsf{REC}$.

Σημείωση 5.2.19. Από το Παράδειγμα 5.2.18 συμπεραίνουμε ότι, παρόλο που γνωρίζουμε ότι υπάρχουν (αριθμησίμως) άπειρες ΤΜ που αναγνωρίζουν την ίδια γλώσσα, αν μας δοθούν δύο ΤΜ δεν μπορούμε να αποφανθούμε αν όντως ισχύει αυτό [1].

Παράδειγμα 5.2.20. Θεωρούμε τη γλώσσα $L_{\varnothing} = \{\langle M\rangle \in \{0,1\}^* \mid L(M) = \varnothing\}$. Η συνάρτηση $\phi : \{0,1\}^* \to \{0,1\}^*$ με:

$$\phi(x) = \begin{cases} \langle M_w\rangle & , \text{ αν υπάρχει ΤΜ } M \text{ και } w \in \{0,1\}^* \text{ τέτοια ώστε } x = \langle M, w\rangle \\ \langle M_{\uparrow}\rangle & , \text{ αλλιώς} \end{cases}$$

όπου η M_w απεικονίζεται στο Σχήμα 5.2.11 και η $M_{\uparrow}$ είναι μία ΤΜ που δεν τερματίζει ποτέ, είναι αναγωγή της $\overline{L}_{\text{Αποδοχής}}$ στην $L_{\varnothing}$ καθώς [2]:

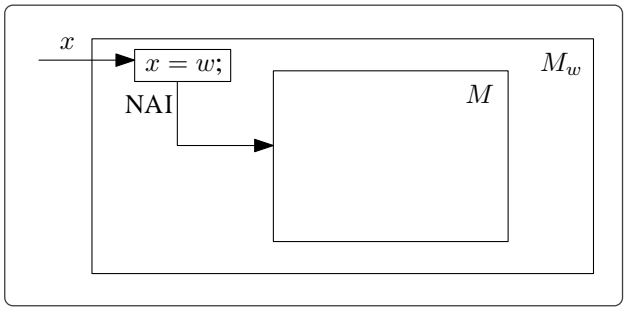
1. ϕ πλήρης και υπολογίσιμη.
2. - Αν $x \in \overline{L}_{\text{Αποδοχής}}$ τότε υπάρχουν δύο περιπτώσεις:
     α. Η x δεν έχει τη μορφή $\langle M, w\rangle$. Τότε $\phi(x) = \langle M_{\uparrow}\rangle \in L_{\varnothing}$.
     β. Η x έχει τη μορφή $\langle M, w\rangle$ και μάλιστα $M(w) \nmid_{q_{\text{ναι}}}$. Τότε $\phi(x) = \langle M_w\rangle$ και $\forall x \in \{0,1\}^*\ (M_w(x) \nmid_{q_{\text{ναι}}}) \Rightarrow L(M_w) = \varnothing \Rightarrow \langle M_w\rangle \in L_{\varnothing}$.
   - Αν $x \notin \overline{L}_{\text{Αποδοχής}}$, τότε $x = \langle M, w\rangle$ και μάλιστα $M(w) \downarrow_{q_{\text{ναι}}}$. Τότε $\phi(x) = \langle M_w\rangle$ και $M_w(w) \downarrow_{q_{\text{ναι}}} \Rightarrow L(M_w) = \{w\} \Rightarrow \langle M_w\rangle \notin L_{\varnothing}$

Εύκολα μπορούμε να δείξουμε ότι $L_{\text{Αποδοχής}} \in \mathsf{RE} \setminus \mathsf{REC}$, οπότε, από το Θεώρημα 1.5.4 έπεται ότι $\overline{L}_{\text{Αποδοχής}} \notin \mathsf{RE}$. Συνεπώς $L_{\varnothing} \notin \mathsf{RE}$.

Κλείνοντας, θα αποδείξουμε δύο προτάσεις που θα χρησιμοποιήσουμε αργότερα στο Κεφάλαιο 8.

[1] Η γλώσσα $L_{\equiv}$ δεν είναι ούτε αναδρομικά απαριθμήσιμη. Μπορείτε να δείτε το γιατί (Άσκηση 5.17);

[2] Όταν κάνουμε αναγωγή από το συμπλήρωμα μίας γλώσσας θα πρέπει να είμαστε πιο προσεκτικοί και να ελέγχουμε επιμελώς ότι η δεύτερη ιδιότητα του Ορισμού 5.2.5 πληρούται.



Σχήμα 5.2.11: *Η ΤΜ M_w στην αναγωγή της $\overline{L}_{\text{Αποδοχής}}$ στην $L_\varnothing$.*

Πρόταση 5.2.21. Η σχέση $\leq_m$ επί του συνόλου $2^{\{0,1\}^*}$ είναι μεταβατική σχέση.

Απόδειξη. Έστω γλώσσες $A, B, C \subseteq \{0,1\}^*$ τέτοιες ώστε $A \leq_m B$ και $B \leq_m C$, και έστω ϕ_1 η αναγωγή της A στην B και ϕ_2 η αναγωγή της B στη C. Θα δείξουμε ότι η $\phi_2 \circ \phi_1$ είναι αναγωγή της A στη C. Παρατηρούμε ότι:

1. Η $\phi_2 \circ \phi_1$ είναι (προφανώς) πλήρης και υπολογίσιμη από την Πρόταση 1.2.12.
2. $w \in A \Leftrightarrow \phi_1(w) \in B \Leftrightarrow \phi_2(\phi_1(w)) \in C$

Συνεπώς, $A \leq_m C$. □

Πρόταση 5.2.22. Έστω $A, B \subseteq \{0,1\}^*$. Αν $A \leq_m B$ τότε $\overline{A} \leq_m \overline{B}$.

Απόδειξη. Έστω ϕ η αναγωγή της A στη B. Αρκεί να δούμε το Σχήμα 5.2.4 και να παρατηρήσουμε ότι:

$$w \in \overline{A} \Leftrightarrow \phi(w) \in \overline{B}$$

Συνεπώς η ϕ είναι και αναγωγή της $\overline{A}$ στη $\overline{B}$. □

Ασκήσεις

5.1 (★☆☆). Δείξτε ότι $D = \{\langle P \rangle \in \{0,1\}^* \mid$ η διοφαντική εξίσωση P έχει ακέραιες ρίζες$\} \in$ RE.

5.2 (★★☆). Δείξτε ότι $D_1 = \{\langle P \rangle \in \{0,1\}^* \mid$ η διοφαντική εξίσωση P μίας μεταβλητής έχει ακέραιες ρίζες$\} \in$ REC.

5.3 (★☆☆). Έστω $L \in$ RE $\setminus$ REC και ΤΜ M τέτοια ώστε $L(M) = L$. Δείξτε ότι το σύνολο $S_L = \{w \in \{0,1\}^* \mid M(w) \uparrow\}$ είναι άπειρο.

5.4 (★☆☆). Δείξτε ότι $L_\infty \leq_m L_{\{0,1\}^*}$.

5.5 (★☆☆). Δείξτε ότι $L = \{\langle M, w\rangle \in \{0,1\}^* \mid M(w)$ περνάει από όλες τις μητερματικές καταστάσεις της $M\} \notin$ REC.

5.6 (★☆☆). Δείξτε ότι $L = \{\langle M\rangle \in \{0,1\}^* \mid \forall w \in \{0,1\}^*($η $M(w)$ γράφει κάποτε 1 και αμέσως κινεί την κεφαλή αριστερά$)\} \notin$ REC.

5.7 (★☆☆). Δείξτε ότι $L = \{\langle M\rangle \in \{0,1\}^* \mid \forall w \in \{0,1\}^*($η $M(w)$ αποδέχεται μετά από άρτιο πλήθος βημάτων$)\} \notin$ REC.

5.8 (★★☆). Δείξτε ότι $L = \{\langle M_1, M_2\rangle \in \{0,1\}^* \mid$ Υπάρχει λέξη $w \in \{0,1\}^*$ τέτοια ώστε $M_1(w) \downarrow^m_{q_{\text{ναι}}} \wedge M_2(w) \downarrow^n_{q_{\text{ναι}}}$ με $n \neq m\} \notin$ REC.

5.9 (★☆☆). Δείξτε ότι $L = \{\langle M_1, M_2, w\rangle \in \{0,1\}^* \mid$ Υπάρχει $t \in \mathbb{N}$ και $a \in \{0,1\}$ τέτοια ώστε οι M_1 και M_2 στο t-οστό βήμα της λειτουργίας τους με είσοδο την w γράφουν $a\} \notin$ REC.

5.10 (★★☆). Δείξτε ότι για κάθε $L \in$ RE ισχύει ότι $L \leq_m \{\langle M\rangle \in \{0,1\}^* \mid M(\langle M\rangle) \downarrow\}$.

5.11 (★☆☆). Δείξτε ότι $L \in$ REC ανν $L \leq_m 0^*1^*$.

5.12 (★☆☆). Δείξτε ότι αν $L_1, L_2 \in$ REC $\setminus \{\varnothing, \{0,1\}^*\}$ τότε $L_1 \leq_m L_2$.

5.13 (★★☆). Έστω K και R τα σύνολα της Άσκησης 1.16. Ισχύει ότι $R \cup K \in$ RE;

5.14 (☆☆☆). Εξετάστε αν η γλώσσα $L = \{\langle M, w\rangle \in \{0,1\}^* \mid \exists$ TM M' $(w \notin L(M) \cap L(M')\}$ είναι αναδρομική.

5.15 (★☆☆). Εξετάστε αν η γλώσσα $L = \{\langle M_1, M_2, M_3\rangle \in \{0,1\}^* \mid L(M_1) = L(M_2) \cup L(M_3)\}$ είναι αναδρομικά απαριθμήσιμη.

5.16 (★☆☆). Δείξτε ότι $L = \{\langle M_1, M_2\rangle \in \{0,1\}^* \mid \epsilon \in L(M_1) \cap L(M_2)\} \in$ RE $\setminus$ REC.

5.17 (☆☆☆). Δείξτε ότι $L_{\equiv} = \{\langle M_1, M_2\rangle \in \{0,1\}^* \mid L(M_1) = L(M_2)\} \notin$ RE.

ΚΕΦΑΛΑΙΟ 6

ΤΟ ΘΕΩΡΗΜΑ ΤΟΥ RICE

Θα ξεκινήσουμε αυτό το κεφάλαιο με τον ίδιο τρόπο που τελειώσαμε το προηγούμενο, με μια αναγωγή. Ας δείξουμε ξανά ότι η γλώσσα L_ϵ του Παραδείγματος 5.2.14 δεν ανήκει στο REC, δείχνοντας αυτήν τη φορά ότι $L_{\text{Αποδοχής}} \leq_m L_\epsilon$.

Παράδειγμα 6.0.1. Θεωρήστε TM M_ϵ που αποδέχεται τη λέξη ϵ. Η συνάρτηση $\phi : \{0,1\}^* \to \{0,1\}^*$ με:

$$\phi(x) = \begin{cases} \langle M_w \rangle & , \text{ αν υπάρχει TM } M \text{ και } w \in \{0,1\}^* \text{ τέτοια ώστε } x = \langle M, w \rangle \\ \langle M_\uparrow \rangle & , \text{ αλλιώς} \end{cases}$$

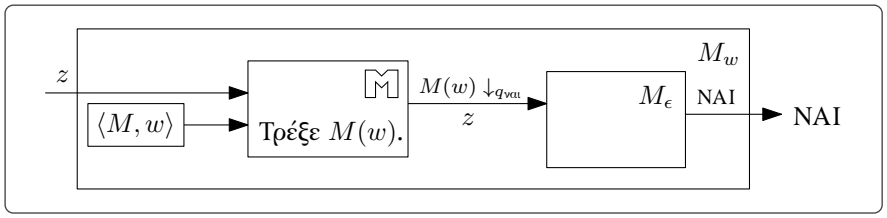
όπου M_w η TM στο Σχήμα 6.0.1 και $M_\uparrow$ μία TM που δεν τερματίζει ποτέ, είναι αναγωγή της $L_{\text{Αποδοχής}}$ στην L_ϵ καθώς:

1. ϕ πλήρης και υπολογίσιμη.

2. - $\langle M, w \rangle \in L_{\text{Αποδοχής}} \Rightarrow M(w) \downarrow_{q_{\text{ναι}}} \Rightarrow L(M_w) = L(M_\epsilon) \Rightarrow \langle M_w \rangle \in L_\epsilon$
   - $\langle M, w \rangle \notin L_{\text{Αποδοχής}} \Rightarrow M(w) \downarrow_{q_{\text{ναι}}} \Rightarrow L(M_w) = \varnothing \Rightarrow \langle M_w \rangle \notin L_\epsilon$

Η γλώσσα L_ϵ ανήκει σε μία ευρεία κλάση γλωσσών που περιέχουν (αποκλειστικά) λέξεις που αντιστοιχούν σε κωδικοποιήσεις TM των οποίων οι γλώσσες που αναγνωρίζουν πληρούν κάποιες «προδιαγραφές» (όπως για παράδειγμα στην L_ϵ περιέχει την ϵ). Για όλες αυτές τις γλώσσες μπορούμε να εφαρμόσουμε την ίδια ακριβώς αναγωγή [1]! Δεν θα μπορούσαμε να σκεφτούμε πιο χαρακτηριστικό παράδειγμα, για να περιγράψουμε τη βασική ιδέα αυτής της (μετα-)αναγωγής, από το Παράδειγμα 6.0.1:

[1] Ελέγξτε την ορθότητα αυτού του ισχυρισμού για τις γλώσσες των Παραδειγμάτων 5.2.15, 5.2.20 και της Παρατήρησης 5.2.16. Η μόνες περιπτώσεις για τις οποίες αυτός ο ισχυρισμός δεν ισχύει περιγράφονται στο Θεώρημα 6.1.1.



Σχήμα 6.0.1: *Η TM M_w στην απόδειξη του Παραδείγματος 6.0.1.*

Ορίζουμε συνάρτηση αναγωγής που «στέλνει» μία λέξη x στην κωδικοποίηση μιας TM M, έτσι ώστε:

$$L(M): \begin{cases} \textit{Πληροί τις προδιαγραφές} & , \textit{ αν } x \in L_{\textit{Αποδοχής}} \\ \textit{Δεν πληροί τις προδιαγραφές} & , \textit{ αν } x \notin L_{\textit{Αποδοχής}} \end{cases}$$

Το γεγονός αυτό παρατηρήθηκε από τον Henry Gordon Rice, ο οποίος απέδειξε το 1951 δύο Θεωρήματα που το καταδεικνύουν (τα Θεώρημα 6.1.1 και 6.2.2). Τα Θεωρήματα αυτά στη βιβλιογραφία συνήθως φέρουν το όνομά του.

Προτού δούμε το πρώτο από τα Θεωρήματα του Rice, θα χρειαστεί να δώσουμε κάποιους ορισμούς.

Ορισμός 6.0.2. *Ιδιότητα (αναδρομικά απαριθμήσιμων) γλωσσών* είναι κάθε σύνολο $\mathcal{P} \subseteq \mathsf{RE}$. Θα λέμε ότι η γλώσσα $L \in \mathsf{RE}$ έχει την ιδιότητα $\mathcal{P}$ ανν $L \in \mathcal{P}$.

Παράδειγμα 6.0.3. Τα ακόλουθα σύνολα αποτελούν ιδιότητες γλωσσών:

- $\mathcal{P}_\epsilon = \{L \in \mathsf{RE} \mid \epsilon \in L\}$
- $\mathcal{P}_\infty = \{L \in \mathsf{RE} \mid |L| = \aleph_0\}$
- $\mathcal{P}_\mathbb{N} = \{L \in \mathsf{RE} \mid |L| \in \mathbb{N}\}$
- $\mathcal{P}_{\{0,1\}^*} = \{\{0,1\}^*\}$
- $\mathcal{P}_\varnothing = \{\varnothing\}$
- $\varnothing$ (η *κενή* ιδιότητα)
- REC

Ορισμός 6.0.4. Έστω ιδιότητα $\mathcal{P} \subseteq \mathsf{RE}$. Ορίζουμε τη γλώσσα $L_\mathcal{P}$, που περιέχει τις κωδικοποιήσεις των TM που αναγνωρίζουν τις γλώσσες με την ιδιότητα $\mathcal{P}$, ως εξής:

$$L_\mathcal{P} = \{\langle M\rangle \in \{0,1\}^* \mid L(M) \in \mathcal{P}\}$$

Τα Θεωρήματα του Rice επικεντρώνονται στη γλώσσα $L_\mathcal{P}$ και καθορίζουν τις προδιαγραφές που θα πρέπει να πληροί η ιδιότητα $\mathcal{P}$ έτσι ώστε η $L_\mathcal{P}$ να είναι αναδρομική ή έστω αναδρομικά απαριθμήσιμη.

6.1 Η περίπτωση του REC

Παρατηρήστε ότι και οι τέσσερις γλώσσες που έχουμε εμμέσως παραλληλίσει σε αυτό το κεφάλαιο, οι L_ϵ, L_∞, $L_{\{0,1\}^*}$ και $L_\varnothing$, δεν είναι αναδρομικές. Εξετάζοντας τις ιδιότητες στις οποίες αντιστοιχούν ($\mathcal{P}_\epsilon$, $\mathcal{P}_\infty$, $\mathcal{P}_{\{0,1\}^*}$ και $\mathcal{P}_\varnothing$ αντίστοιχα) δεν μπορούμε να βρούμε κάτι κοινό, πέρα φυσικά από το απλό γεγονός ότι περιέχουν τουλάχιστον μία γλώσσα του RE αλλά δεν περιέχουν όλες τις γλώσσες του RE. Τέτοιου είδους ιδιότητες συνήθως τις αποκαλούμε *μη-τετριμμένες*. Το (απλό) Θεώρημα του Rice αποδεικνύει ότι η $L_\mathcal{P}$ είναι αναδρομική ανν η ιδιότητα $\mathcal{P}$ είναι τετριμμένη.

Θεώρημα 6.1.1 (Rice). Για κάθε ιδιότητα $\mathcal{P} \subseteq \mathsf{RE}$ ισχύει ότι:

$$L_\mathcal{P} \in \mathsf{REC} \Leftrightarrow \mathcal{P} = \varnothing \vee \mathcal{P} = \mathsf{RE}$$

Απόδειξη. ($\Rightarrow$) [1] Έστω ιδιότητα $\mathcal{P} \subseteq \mathsf{RE}$, με $\mathcal{P} \notin \{\varnothing, \mathsf{RE}\}$. Θεωρούμε, χωρίς βλάβη της γενικότητας, ότι $\varnothing \notin \mathcal{P}$ [2].Έστω επίσης γλώσσα $L \in \mathcal{P}$ και TM M_L που την ημι-αποφασίζει. Θα δείξουμε ότι $L_{\text{Αποδοχής}} \leq_m L_\mathcal{P}$. Θεωρούμε $\phi : \{0,1\}^* \to \{0,1\}^*$ με:

$$\phi(x) = \begin{cases} \langle M_w \rangle & , \text{ αν υπάρχει TM } M \text{ και } w \in \{0,1\}^* \text{ τέτοια ώστε } x = \langle M, w \rangle \\ \langle M_\uparrow \rangle & , \text{ αλλιώς} \end{cases}$$

όπου M_w η TM του Σχήματος 6.1.1 και $M_\uparrow$ μία TM που δεν τερματίζει ποτέ. Παρατηρούμε ότι:

1. ϕ πλήρης και υπολογίσιμη.
2. - $x \in L_{\text{Αποδοχής}}$ τότε $x = \langle M, w \rangle$ με $\langle M, w \rangle \in L_{\text{Αποδοχής}}$, οπότε $\phi(x) = \langle M_w \rangle$ και $L(M_w) = L(M_L) = L \in \mathcal{P}$ άρα $\phi(x) \in L_\mathcal{P}$.
   - $x \notin L_{\text{Αποδοχής}}$ τότε:
     α. είτε $x = \langle M, w \rangle$ με $\langle M, w \rangle \notin L_{\text{Αποδοχής}}$, οπότε $\phi(x) = \langle M_w \rangle$ και $L(M_w) = \varnothing \notin \mathcal{P}$ (αφού $M(w) \nmid_{q_{\text{ναι}}}$), άρα $\phi(x) \notin L_\mathcal{P}$,
     β. είτε $x \neq \langle M, w \rangle$ οπότε $\phi(x) = \langle M_\uparrow \rangle$ και $L(M_\uparrow) = \varnothing \notin \mathcal{P}$, άρα $\phi(x) \notin L_\mathcal{P}$.

Αφού $L_{\text{Αποδοχής}} \notin \mathsf{REC}$ έπεται ότι $L_\mathcal{P} \notin \mathsf{REC}$.

($\Leftarrow$) Παρατηρούμε ότι:

$$\text{Αν } \mathcal{P} = \varnothing \text{ τότε } L_\mathcal{P} = \{\langle M \rangle \in \{0,1\}^* \mid L(M) \in \varnothing\} = \varnothing \in \mathsf{REC}$$

και

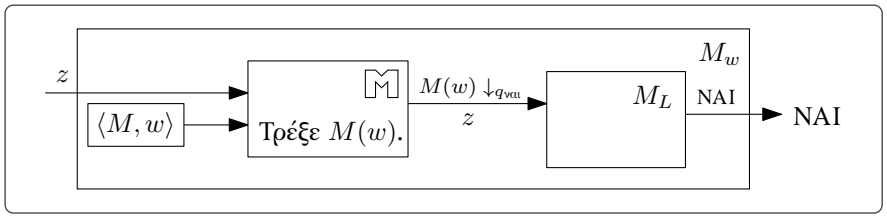
$$\text{Αν } \mathcal{P} = \mathsf{RE} \text{ τότε } L_\mathcal{P} = \{\langle M \rangle \in \{0,1\}^* \mid L(M) \in \mathsf{RE}\} = \mathcal{G} \in \mathsf{REC}$$ [3]

□

[1] Θα δείξουμε την αντιθετοαντιστροφή του.

[2] Αλλιώς θα πάρουμε την $\overline{\mathcal{P}} = \mathsf{RE} \setminus \mathcal{P}$ για την οποία επίσης ισχύει ότι $\overline{\mathcal{P}} \notin \{\varnothing, \mathsf{RE}\}$. Ολοκληρώνοντας την απόδειξη θα έχουμε δείξει ότι $L_{\overline{\mathcal{P}}} \notin \mathsf{REC}$. Για να συνάγουμε το ζητούμενο αρκεί να παρατηρήσουμε ότι $L_\mathcal{P} \in \mathsf{REC}$ ανν $L_{\overline{\mathcal{P}}} \in \mathsf{REC}$.

[3] Δες Ορισμό 1.4.10 και Παρατήρηση 1.4.11.



Σχήμα 6.1.1: *Η TM M_w στην απόδειξη του Θεωρήματος 6.1.1.*

Παράδειγμα 6.1.2 (Εφαρμογή του Θεωρήματος του Rice)**.**

- $L_{\mathbb{N}} = \{\langle M\rangle \in \{0,1\}^* \mid |L(M)| \in \mathbb{N}\} \notin \mathsf{REC}$ καθώς για την ιδιότητα $\mathcal{P}_{\mathbb{N}}$ ισχύει ότι $\mathcal{P}_{\mathbb{N}} \neq \varnothing$ (παραδείγματος χάρη $\{\epsilon\} \in \mathcal{P}_{\mathbb{N}}$) και $\mathcal{P}_{\mathbb{N}} \neq \mathsf{RE}$ ($\{0,1\}^* \notin \mathcal{P}_{\mathbb{N}}$).

- $L_{\mathsf{REC}} = \{\langle M\rangle \in \{0,1\}^* \mid L(M) \in \mathsf{REC}\} \notin \mathsf{REC}$ καθώς για την ιδιότητα REC ισχύει ότι $\mathsf{REC} \neq \varnothing$ (παραδείγματος χάρη κάθε πεπερασμένη γλώσσα ανήκει στην REC) και όπως είδαμε $\mathsf{REC} \neq \mathsf{RE}$.

- $L = \{\langle M\rangle \in \{0,1\}^* \mid L(M) = \varnothing \vee L(M) = \{(01)^n \mid n \in \mathbb{N}\} \vee L(M) = \{0,1\}^*\} \notin \mathsf{REC}$ καθώς για την ιδιότητα $\mathcal{P} = \{\varnothing, \{(01)^n \mid n \in \mathbb{N}\}, \{0,1\}^*\}$ ισχύει ότι $L = L_{\mathcal{P}}$ και προφανώς $\mathcal{P} \notin \{\varnothing, \mathsf{RE}\}$.

6.2 Η περίπτωση του RE

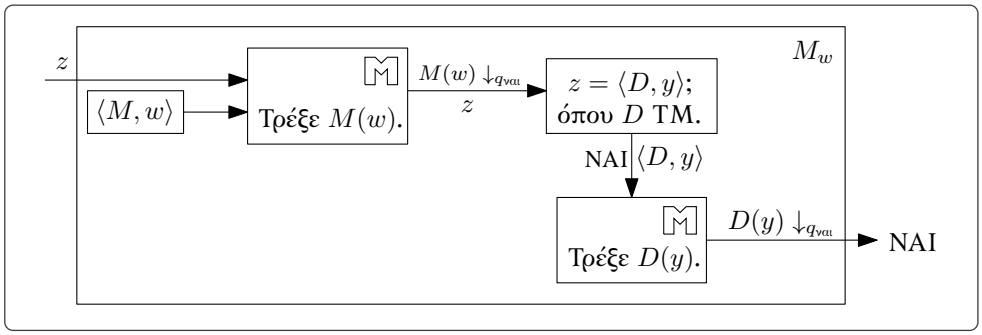
Ας δούμε μία ακόμα αναγωγή που παρουσιάζει ενδιαφέρον.

Παράδειγμα 6.2.1. Η συνάρτηση $\phi : \{0,1\}^* \to \{0,1\}^*$ με:

$$\phi(x) = \begin{cases} \langle M_w\rangle & \text{, αν υπάρχει TM } M \text{ και } w \in \{0,1\}^* \text{ τέτοια ώστε } x = \langle M, w\rangle \\ \langle M_\uparrow\rangle & \text{, αλλιώς} \end{cases}$$

όπου η $M_\uparrow$ κατά τα γνωστά δεν τερματίζει ποτέ και η M_w φαίνεται στο Σχήμα 6.2.1, είναι αναγωγή της $\overline{L}_{\text{Αποδοχής}}$ στην L_{REC} καθώς:

1. ϕ πλήρης και υπολογίσιμη.
2. - $x \in \overline{L}_{\text{Αποδοχής}}$ τότε:
     α. είτε $x = \langle M, w\rangle$ με $\langle M, w\rangle \in \overline{L}_{\text{Αποδοχής}}$, οπότε $\phi(x) = \langle M_w\rangle$ και για κάθε $x \in \{0,1\}^*$ ισχύει ότι $M_w(x) \uparrow$ (αφού $M(w) \downarrow_{q_{\text{ναι}}}$), άρα $L(M_w) = \varnothing \in \mathsf{REC}$, συνεπώς $\phi(x) \in L_{\mathsf{REC}}$,
     β. είτε $x \neq \langle M, w\rangle$, οπότε $\phi(x) = \langle M_\uparrow\rangle$ και $L(M_\uparrow) = \varnothing \in \mathsf{REC}$, άρα $\phi(x) \in L_{\mathsf{REC}}$.
   - $x \notin \overline{L}_{\text{Αποδοχής}}$ τότε $x = \langle M, w\rangle$ με $\langle M, w\rangle \in L_{\text{Αποδοχής}}$, οπότε $\phi(x) = \langle M_w\rangle$ και $L(M_w) = \{\langle D, y\rangle \in \{0,1\}^* \mid D(y) \downarrow_{q_{\text{ναι}}}\} = L_{\text{Αποδοχής}}$ (αφού $M(w) \downarrow_{q_{\text{ναι}}}$), και αφού $L_{\text{Αποδοχής}} \notin \mathsf{REC}$ έπεται ότι $\phi(x) \notin L_{\mathsf{REC}}$.



Σχήμα 6.2.1: *Η TM M_w του Παραδείγματος 6.2.1.*

Τέλος, αφού $\overline{L}_{\text{Αποδοχής}} \notin \mathsf{RE}$ έπεται ότι $L_{\mathsf{REC}} \notin \mathsf{RE}$.

Παρόλο που η ιδέα της αναγωγής του Θεωρήματος 6.1.1 (μία παραλλαγή της για την ακρίβεια) μπορεί να χρησιμοποιηθεί για να δείξουμε ότι η γλώσσα L_{REC} δεν είναι αναδρομικά απαριθμήσιμη, δυστυχώς δεν αρκεί για να επεκτείνουμε το Θεώρημα 6.1.1 στις αναδρομικά απαριθμήσιμες γλώσσες [1].

Είναι φανερό ότι η κλάση REC, ιδωμένη σαν ιδιότητα γλωσσών, ικανοποιεί πολλές και ποικίλες «προδιαγραφές». Η προδιαγραφή όμως που δεν ικανοποιεί, και ως εκ τούτου η γλώσσα L_{REC} δεν είναι αναδρομικά απαριθμήσιμη, είναι ότι υπάρχουν υπερσύνολα γλωσσών του REC που δεν ανήκουν στο REC (δες το Παράδειγμα 6.2.3 για περισσότερες λεπτομέρειες). Το δεύτερο Θεώρημα του Rice (γνωστό και ως *Γενικευμένο Θεώρημα του Rice*) καθορίζει πλήρως τις απαραίτητες προδιαγραφές μίας ιδιότητας $\mathcal{P}$ ώστε η $L_{\mathcal{P}}$ να είναι αναδρομικά απαριθμήσιμη.

Θεώρημα 6.2.2 (Γενικευμένο Θεώρημα του Rice)**.** Για κάθε ιδιότητα $\mathcal{P} \subseteq \mathsf{RE}$ ισχύει ότι:

$$L_{\mathcal{P}} \in \mathsf{RE} \Leftrightarrow ① \wedge ② \wedge ③$$

όπου:

① $\forall L \in \mathcal{P}\ \forall L' \in \mathsf{RE}\ (L \subseteq L' \rightarrow L' \in \mathcal{P})$ [2]

② $\forall L \in \mathcal{P}\ (|L| = \aleph_0 \rightarrow \exists L' \subseteq L\ (|L'| \in \mathbb{N} \wedge L' \in \mathcal{P}))$ [3]

③ $F_{\mathcal{P}} = \{w_1\#w_2\#\cdots\#w_n \in (\{0,1\} \cup \{\#\})^* \mid \{w_1, w_2, \ldots, w_n\} \in \{L \in \mathcal{P} \mid |L| \in \mathbb{N}\}\} \in \mathsf{RE}$ [4] [5]

Απόδειξη. ($\Rightarrow$) $\underline{L_{\mathcal{P}} \in \mathsf{RE} \Rightarrow ①}$: [6] Έστω γλώσσες $L_1 \in \mathcal{P}$ και $L_2 \in \mathsf{RE}$ τέτοιες ώστε $L_1 \subseteq L_2$

[1] Την παραδέτουμε όμως εδώ προς τέρψη του αναγνώστη, αλλά και για να τον προετοιμάσουμε για τις δύσκολες αναγωγές που περιέχει η απόδειξη του Θεωρήματος 6.2.2.

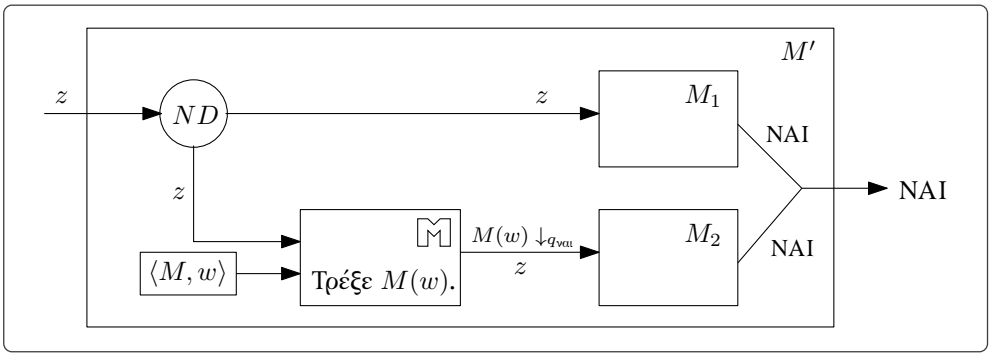
[2] Η συνθήκη αυτή «διαβάζεται»: *Κάθε αναδρομικά απαριθμήσιμο υπερσύνολο μίας γλώσσας που έχει την ιδιότητα, έχει επίσης την ιδιότητα.*

[3] *Κάθε γλώσσα που έχει την ιδιότητα έχει πεπερασμένο υποσύνολο που έχει επίσης την ιδιότητα.*

[4] Τυπικά θα πρέπει να κωδικοποιήσουμε τη γλώσσα $\{w_1, w_2, \ldots, w_n\}$ στο $\{0,1\}$. Θα χρησιμοποιήσουμε όμως άτυπα την κωδικοποίηση στο $\{0,1\} \cup \{\#\}$ καθώς είναι πιο παραστατική.

[5] *Η γλώσσα που περιέχει λέξεις που αντιστοιχούν σε πεπερασμένες γλώσσες που έχουν την ιδιότητα είναι αναδρομικά απαριθμήσιμη.*

[6] Θα δείξουμε την αντιθετοαντιστροφή του, δηλαδή ότι $\neg① \Rightarrow L_{\mathcal{P}} \notin \mathsf{RE}$.



Σχήμα 6.2.2: *Η ΤΜ M' στην απόδειξη του ότι $L_{\mathcal{P}} \in$ RE $\Rightarrow$ ① στο Θεώρημα 6.2.2.*

και $L_2 \notin \mathcal{P}$. Έστω επίσης ότι οι ΤΜ M_1, M_2 ημι-αποφασίζουν τις L_1, L_2 αντίστοιχα. Θα δείξουμε ότι $\overline{L}_{\text{Αποδοχής}} \leq_m L_{\mathcal{P}}$. Θεωρούμε συνάρτηση $\phi : \{0,1\}^* \to \{0,1\}^*$ με:

$$\phi(x) = \begin{cases} \langle M' \rangle & \text{, αν υπάρχει ΤΜ } M \text{ και } w \in \{0,1\}^* \text{ τέτοια ώστε } x = \langle M, w\rangle \\ \langle M_1 \rangle & \text{, αλλιώς} \end{cases}$$

όπου M' η ΤΜ του Σχήματος 6.2.2. Παρατηρούμε ότι:

1. ϕ πλήρης και υπολογίσιμη.

2. - $x \in \overline{L}_{\text{Αποδοχής}}$ τότε
   α. είτε $x = \langle M, w\rangle$ με $\langle M, w\rangle \in \overline{L}_{\text{Αποδοχής}}$, οπότε $\phi(x) = \langle M'\rangle$ και $L(M') = L(M_1) = L_1 \in \mathcal{P}$ άρα $\phi(x) \in L_{\mathcal{P}}$,
   β. είτε $x \neq \langle M, w\rangle$, οπότε $\phi(x) = \langle M_1\rangle$ και $L_1 \in \mathcal{P}$ άρα $\phi(x) \in L_{\mathcal{P}}$.
   - $x \notin \overline{L}_{\text{Αποδοχής}}$ τότε $x = \langle M, w\rangle$ με $\langle M, w\rangle \in L_{\text{Αποδοχής}}$, οπότε $\phi(x) = \langle M'\rangle$ και $L(M') = L(M_2) = L_2 \notin \mathcal{P}$ (αφού $M(w)\downarrow_{q_{\text{ναι}}}$ και $L_1 \subseteq L_2$), άρα $\phi(x) \notin L_{\mathcal{P}}$.

Αφού $\overline{L}_{\text{Αποδοχής}} \notin$ RE έπεται ότι $L_{\mathcal{P}} \notin$ RE.

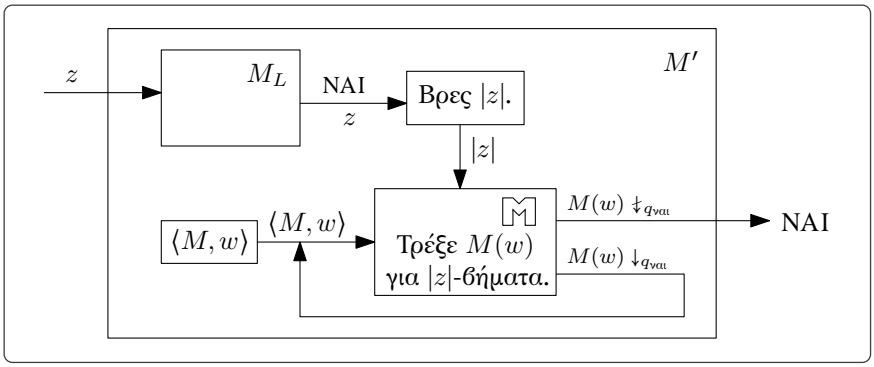
$L_{\mathcal{P}} \in$ RE $\Rightarrow$ ②: [1] Έστω γλώσσα $L \in \mathcal{P}$ τέτοια ώστε $|L| = \aleph_0$ και κάθε πεπερασμένο υποσύνολό της δεν ανήκει στην $\mathcal{P}$. Έστω επίσης M_L η ΤΜ που ημι-αποφασίζει την L. Θα δείξουμε ότι $\overline{L}_{\text{Αποδοχής}} \leq_m L_{\mathcal{P}}$. Θεωρούμε συνάρτηση $\phi : \{0,1\}^* \to \{0,1\}^*$ με:

$$\phi(x) = \begin{cases} \langle M' \rangle & \text{, αν υπάρχει ΤΜ } M \text{ και } w \in \{0,1\}^* \text{ τέτοια ώστε } x = \langle M, w\rangle \\ \langle M_L \rangle & \text{, αλλιώς} \end{cases}$$

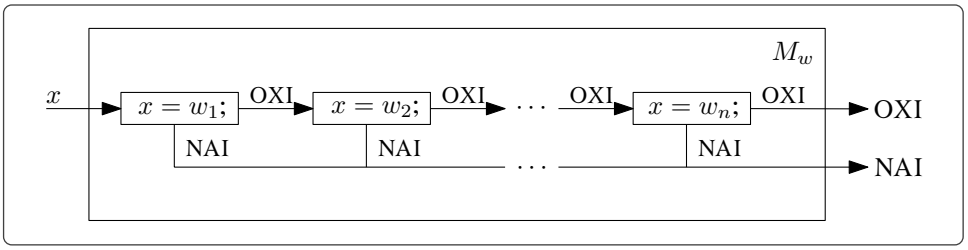
όπου M' η ΤΜ του Σχήματος 6.2.3. Παρατηρούμε ότι:

1. ϕ πλήρης και υπολογίσιμη.

[1] Θα δείξουμε την αντιθετοαντιστροφή του, δηλαδή ότι $\neg$② $\Rightarrow L_{\mathcal{P}} \notin$ RE.



Σχήμα 6.2.3: *Η ΤΜ M' στην απόδειξη του ότι $L_{\mathcal{P}} \in$ RE $\Rightarrow$ ② στο Θεώρημα 6.2.2.*



Σχήμα 6.2.4: *Η ΤΜ M_w στην απόδειξη του ότι $L_{\mathcal{P}} \in$ RE $\Rightarrow$ ③ στο Θεώρημα 6.2.2.*

2. - $x \in \overline{L}_{\text{Αποδοχής}}$ τότε
     α. είτε $x = \langle M, w\rangle$ με $\langle M, w\rangle \in \overline{L}_{\text{Αποδοχής}}$, οπότε $\phi(x) = \langle M'\rangle$ και $L(M') = L(M_L) = L \in \mathcal{P}$ άρα $\phi(x) \in L_{\mathcal{P}}$,
     β. είτε $x \neq \langle M, w\rangle$, οπότε $\phi(x) = \langle M_L\rangle$ και $L \in \mathcal{P}$ άρα $\phi(x) \in L_{\mathcal{P}}$.
   - $x \notin \overline{L}_{\text{Αποδοχής}}$ τότε $x = \langle M, w\rangle$ με $\langle M, w\rangle \in L_{\text{Αποδοχής}}$, οπότε $\phi(x) = \langle M'\rangle$. Παρατηρούμε ότι για κάποιο $t \in \mathbb{N}$ ισχύει ότι $M(w) \downarrow^t_{q_{\text{ναι}}}$, οπότε $L(M') = \{z \in L \mid |z| < t\}$. Συνεπώς $|L(M')| \in \mathbb{N}$ και $L(M') \subseteq L$ άρα $L(M') \notin \mathcal{P}$, οπότε $\phi(x) \notin L_{\mathcal{P}}$.

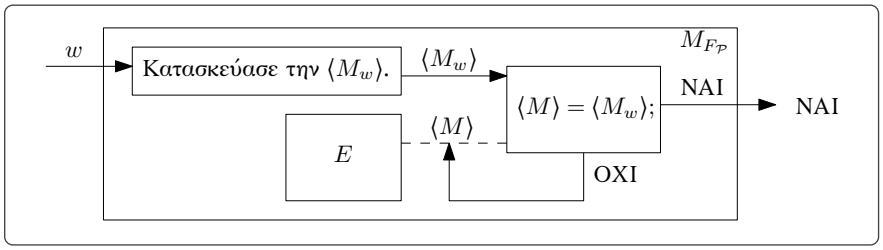
Αφού $\overline{L}_{\text{Αποδοχής}} \notin$ RE έπεται ότι $L_{\mathcal{P}} \notin$ RE.

$L_{\mathcal{P}} \in$ RE $\Rightarrow$ ③: Για κάθε λέξη του $(\{0,1\} \cup \{\#\})^*$, έστω τη $w = w_1\#w_2\#\cdots\#w_n$ όπου $w_i \in \{0,1\}^*$ για $i \in [n]$ [1], θεωρούμε τη λέξη $\langle M_w\rangle \in \{0,1\}^*$, όπου M_w η ΤΜ του Σχήματος 6.2.4 που αποφασίζει την γλώσσα $\{w_1, w_2, \ldots, w_n\}$.

Αφού $L_{\mathcal{P}} \in$ RE υπάρχει απαριθμητής, έστω E, που απαριθμεί την $L_{\mathcal{P}}$. Θεωρούμε την ΤΜ $M_{F_{\mathcal{P}}}$ του Σχήματος 6.2.5 και παρατηρούμε ότι:

- Αν $w \in F_{\mathcal{P}}$, τότε $w = w_1\#w_2\#\cdots\#w_n$ για κάποιες λέξεις $w_1, w_2, \ldots, w_n \in \{0,1\}^*$, όπου η $L = \{w_1, w_2, \ldots, w_n\} \in \mathcal{P}$. Αφού η M_w αποφασίζει την L ο E κάποια στιγμή θα τυπώσει $\langle M_w\rangle$. Άρα $M_{F_{\mathcal{P}}}(w) \downarrow q_{\text{ναι}}$.

[1] Ενδεχομένως κάποια από τις w_i, $i \in [n]$, να είναι η κενή λέξη και να έχουμε και επαναλήψεις.



Σχήμα 6.2.5: *Η ΤΜ $M_{F_\mathcal{P}}$ στην απόδειξη του ότι $L_\mathcal{P} \in$ RE $\Rightarrow$ ③ στο Θεώρημα 6.2.2.*

- Αν $w \notin F_\mathcal{P}$, τότε $w = w_1\#w_2\#\cdots\#w_n$ για κάποιες λέξεις $w_1, w_2, \ldots, w_n \in \{0,1\}^*$ [1], όπου $\{w_1, w_2, \ldots, w_n\} \notin \mathcal{P}$. Ο E δεν θα τυπώσει ποτέ $\langle M_w \rangle$. Άρα $M_{F_\mathcal{P}}(w) \uparrow$.

Επομένως η $M_{F_\mathcal{P}}$ ημι-αποφασίζει την $F_\mathcal{P}$.

($\Leftarrow$): [2] Από το ③ υπάρχει απαριθμητής E που απαριθμεί την $F_\mathcal{P}$. Θα δείξουμε ότι η ΤΜ D του Σχήματος 6.2.6 ημι-αποφασίζει την $L_\mathcal{P}$ [3].

$L_\mathcal{P} \subseteq L(D)$:Έστω $\langle M \rangle \in L_\mathcal{P}$ δηλαδή $L(M) \in \mathcal{P}$. Από το ② έπεται ότι

$$\exists L \subseteq L(M)\ (|L| \in \mathbb{N} \wedge L \in \mathcal{P}),$$

έστω ότι $L = \{w_1, \ldots, w_n\}$. Από το ③ έπεται ότι ο E κάποια στιγμή θα τυπώσει $w_1\#\cdots\#w_n$, έστω μετά από i-βήματα, και αφού $L \subseteq L(M)$, έπεται ότι

$$\exists j \in \mathbb{N}\ \forall s \in [n]\ (M(w_s) \downarrow^j_{q_{\text{ναι}}}),$$

οπότε για το ζευγάρι (i,j) ισχύει ότι $D(\langle M \rangle) \downarrow_{q_{\text{ναι}}}$, άρα $\langle M \rangle \in L(D)$.

$L(D) \subseteq L_\mathcal{P}$:Έστω $\langle M \rangle \in L(D)$, δηλαδή υπάρχει $(i,j) \in \mathbb{N}^2$ τέτοιο ώστε

$$\forall s \in [n]\ (M(w_s) \downarrow^j_{q_{\text{ναι}}}),$$

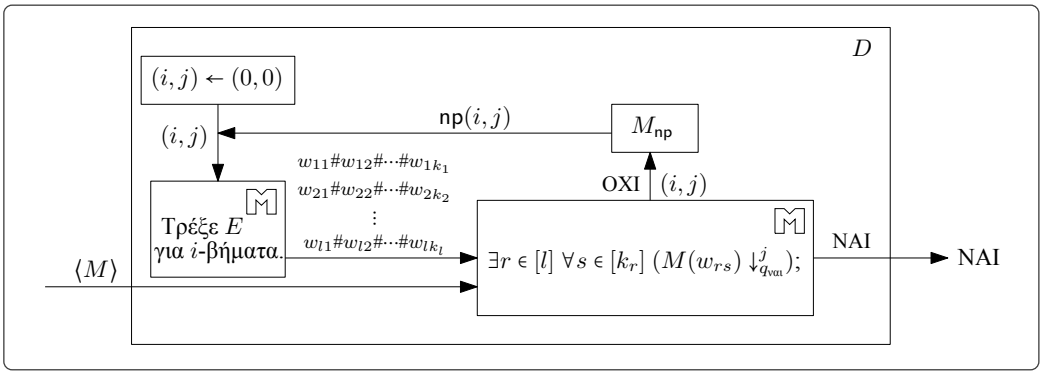
όπου $w_1\#\cdots\#w_n$ είναι μία από τις λέξεις που τύπωσε ο E σε i-βήματα. Συνεπώς ισχύει ότι η $L = \{w_1, \ldots, w_n\}$ είναι υποσύνολο της $L(M)$ και, αφού ο E απαριθμεί την $F_\mathcal{P}$, ισχύει ότι η L έχει την ιδιότητα $\mathcal{P}$. Από το ① έπεται ότι $L(M) \in \mathcal{P}$, άρα $\langle M \rangle \in L_\mathcal{P}$. □

Στη συνέχεια θα δούμε μερικά παραδείγματα εφαρμογής του Γενικευμένου Θεωρήματος του Rice.

[1] Ακόμα και αν τετριμμένα ισχύει ότι $n = 1$.

[2] Εδώ θα φανεί ο λόγος που οι ①, ② και ③ είναι ικανές να μας εξασφαλίσουν ότι η $L_\mathcal{P}$ θα είναι αναδρομικά απαριθμήσιμη: Δοσμένης μιας ΤΜ M η ③ μας δίνει το δικαίωμα να ελέγξουμε μόνο ένα πεπερασμένο κομμάτι της $L(M)$ για να εξακριβώσουμε αν $L(M) \in \mathcal{P}$, καθώς από τη ② αν $L(M) \in \mathcal{P}$ θα υπάρχει πεπερασμένο υποσύνολό της που έχει την ιδιότητα $\mathcal{P}$ (και κάποια στιγμή ο απαριθμητής για την $F_\mathcal{P}$ θα το τυπώσει), και αντίστροφα, αν κάποιο πεπερασμένο κομμάτι της $L(M)$ έχει την $\mathcal{P}$ τότε και η $L(M)$ οφείλει να έχει την $\mathcal{P}$, λόγω του ①.

[3] Η ΤΜ $M_{\text{πρ}}$ που χρησιμοποιεί σαν υπορουτίνα η D είναι μία παραλλαγή της ΤΜ της Παρατήρησης 1.4.18.



Σχήμα 6.2.6: *Η TM D στην απόδειξη του Θεωρήματος 6.2.2.*

Παράδειγμα 6.2.3. Θα αποδείξουμε ξανά ότι η γλώσσα L_{REC} δεν είναι αναδρομικά απαριθμήσιμη, χωρίς να χρησιμοποιήσουμε αναγωγή (όπως κάναμε στο Παράδειγμα 6.2.1). Θεωρούμε την ιδιότητα $\mathcal{P} = \mathsf{REC}$ και παρατηρούμε ότι για τη γλώσσα $\varnothing$ (που προφανώς έχει την ιδιότητα $\mathcal{P}$) υπάρχει γλώσσα L' με $\varnothing \subseteq L'$ που δεν έχει την ιδιότητα $\mathcal{P}$, παραδείγματος χάρη η $L_{\text{Αποδοχής}}$. Συνεπώς παραβιάζεται η συνθήκη (1) του Θεωρήματος 6.2.2, άρα $L_{\mathsf{REC}} \notin \mathsf{RE}$.

Παράδειγμα 6.2.4. Παρατηρήστε ότι για την ιδιότητα $\mathcal{P}_\infty$ δεν ισχύει η συνθήκη (2) καθώς δεν υπάρχει πεπερασμένη γλώσσα με την ιδιότητα $\mathcal{P}_\infty$. Συνεπώς $L_\infty \notin \mathsf{RE}$.

Παράδειγμα 6.2.5. Έστω η ιδιότητα $\mathcal{P} = \{L \in \mathsf{RE} \mid L \setminus L_{\text{Αποδοχής}} \neq \varnothing\}$. Παρατηρούμε ότι αν η L έχει την ιδιότητα $\mathcal{P}$ τότε $L \setminus L_{\text{Αποδοχής}} \neq \varnothing$, οπότε:

$$\forall L' \in \mathsf{RE}\ (L \subseteq L' \to L' \setminus L_{\text{Αποδοχής}} \neq \varnothing)$$

Άρα η $\mathcal{P}$ ικανοποιεί τη συνθήκη (1) του Θεωρήματος 6.2.2.

Επίσης, αφού $L \setminus L_{\text{Αποδοχής}} \neq \varnothing$, υπάρχει $w \in L \setminus L_{\text{Αποδοχής}}$. Θεωρούμε τη γλώσσα $\{w\} \subseteq L$ για την οποία ισχύει επίσης ότι $\{w\} \setminus L_{\text{Αποδοχής}} \neq \varnothing$, άρα $\{w\} \in \mathcal{P}$. Συνεπώς η $\mathcal{P}$ ικανοποιεί και τη συνθήκη (2) του Θεωρήματος 6.2.2.

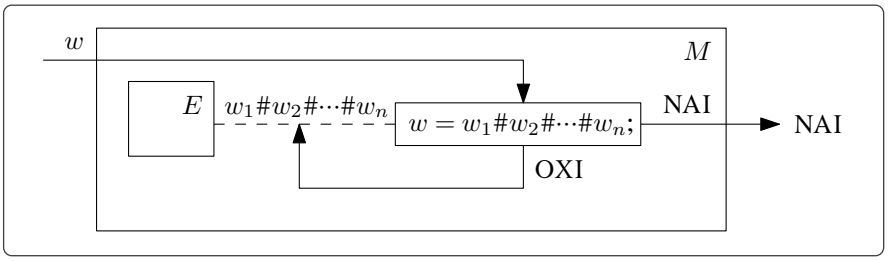
Έστω (προς άτοπο) ότι ικανοποιεί και τη συνθήκη (3), δηλαδή υπάρχει απαριθμητής E που απαριθμεί την $F_{\mathcal{P}}$. Η TM M του Σχήματος 6.2.7 ημι-αποφασίζει την $\overline{L}_{\text{Αποδοχής}}$, καθώς αν $w \in \overline{L}_{\text{Αποδοχής}}$ τότε $\{w\} \in \mathcal{P}$ άρα ο E κάποια στιγμή θα τυπώσει τη w. Άτοπο. Συνεπώς $L_{\mathcal{P}} \notin \mathsf{RE}$.

Παράδειγμα 6.2.6. Έστω η ιδιότητα $\mathcal{P} = \{L \in \mathsf{RE} \mid |L| \geq 10\}$. Παρατηρούμε ότι αν η L έχει την ιδιότητα $\mathcal{P}$ τότε $|L| \geq 10$, οπότε:

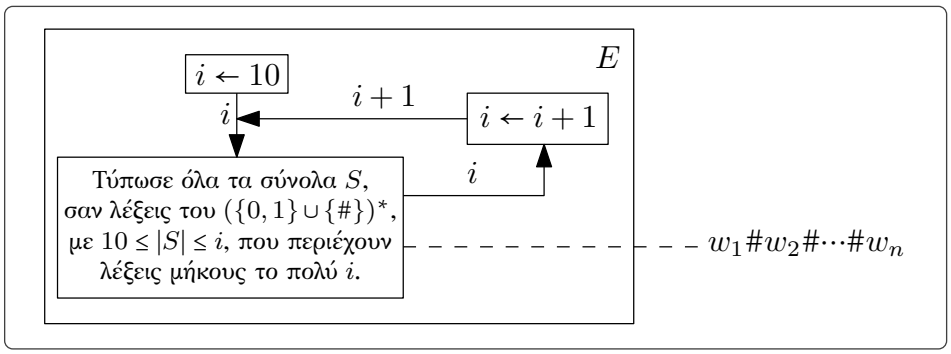
$$\forall L' \in \mathsf{RE}\ (L \subseteq L' \to |L'| \geq |L| \geq 10)$$

Άρα η $\mathcal{P}$ ικανοποιεί τη συνθήκη (1) του Θεωρήματος 6.2.2.

Επίσης, αφού $|L| \geq 10$, υπάρχουν διακεκριμένες $w_1, \ldots, w_{10} \in L$. Θεωρούμε τη γλώσσα $L' = \{w_1, \ldots, w_{10}\} \subseteq L$ η οποία έχει 10 στοιχεία, άρα $L' \in \mathcal{P}$. Συνεπώς η $\mathcal{P}$ ικανοποιεί και τη συνθήκη (2) του Θεωρήματος 6.2.2.



Σχήμα 6.2.7: *Η ΤΜ M που (υποθετικά) ημι-αποφασίζει την $\overline{L}_{\text{Αποδοχής}}$ στο Παράδειγμα 6.2.5.*



Σχήμα 6.2.8: *Ο απαριθμητής E στο Παράδειγμα 6.2.6.*

Τέλος, ο απαριθμητής E του Σχήματος 6.2.8 απαριθμεί την $F_{\mathcal{P}}$. Συνεπώς η $\mathcal{P}$ ικανοποιεί και τη συνθήκη ③ του Θεωρήματος 6.2.2, άρα έπεται ότι $L_{\mathcal{P}} \in$ RE [1].

Ασκήσεις

6.1 (☆☆☆). Έστω $L \in$ RE. Εκφράστε σαν γλώσσα το ακόλουθο πρόβλημα:

Είσοδος:	Κωδικοποίηση μίας ΤΜ M
Έξοδος:	Ναι αν η M αναγνωρίζει την L και όχι αλλιώς.

Και ελέγξτε αν ανήκει στο REC.

6.2 (★☆☆). Θεωρήστε τη γλώσσα $L = \{\langle M\rangle \in \{0,1\}^* \mid L(M) = HP\}$. Δείξτε ότι:

1. Η L δεν είναι αναδρομική, χωρίς να χρησιμοποιήσετε το (απλό) Θεώρημα του Rice (και το δεύτερο υποερώτημα).

[1] Φυσικά στην προκειμένη περίπτωση θα ήταν λιγότερο κουραστικό να κατασκευάσουμε κατευθείαν μία ΤΜ που να ημι-αποφασίζει την $L_{10} = \{\langle M\rangle \in \{0,1\}^* \mid |L(M)| \geq 10\}$. Η κατασκευή αυτής της ΤΜ αφήνεται ως άσκηση.

2. Η L δεν είναι αναδρομικά απαριθμήσιμη, χωρίς να χρησιμοποιήσετε το (γενικευμένο) Θεώρημα του Rice.

6.3 (★☆☆). Εξετάστε αν η γλώσσα $L = \{\langle M\rangle \in \{0,1\}^* \mid$ Υπάρχει ΤΜ M' με άρτιο πλήθος καταστάσεων τέτοια ώστε $L(M') = L(M)\}$ είναι αναδρομική.

6.4 (★☆☆). Δείξτε ότι $L = \{\langle M\rangle \in \{0,1\}^* \mid \exists w \in \Sigma^* : |w| = 1871 \wedge w \in L(M)\} \in \mathsf{RE}$. Ισχύει ότι $\overline{L} \in \mathsf{RE}$;

6.5 (★☆☆). Εξετάστε αν οι γλώσσες:

- $L_{\mathsf{RE}} = \{\langle M\rangle \in \{0,1\}^* \mid L(M) \in \mathsf{RE}\}$
- $L_{\mathsf{CS}} = \{\langle M\rangle \in \{0,1\}^* \mid L(M) \in \mathsf{CS}\}$
- $L_{\mathsf{CF}} = \{\langle M\rangle \in \{0,1\}^* \mid L(M) \in \mathsf{CF}\}$
- $L_{\mathsf{R}} = \{\langle M\rangle \in \{0,1\}^* \mid L(M) \in \mathsf{R}\}$

είναι αναδρομικά απαριθμήσιμες.

6.6 (★☆☆). Δώστε παράδειγμα ιδιότητας που ικανοποιεί τα ① και ③ στην εκφώνηση του Θεωρήματος 6.2.2, αλλά δεν ικανοποιεί το ②.

6.7 (☆☆☆). Εξετάστε αν οι γλώσσες:

- $L_1 = \{\langle M\rangle \in \{0,1\}^* \mid L(M) \cap \{0^{2^n} \in \{0,1\}^* \mid n \in \mathbb{N}\} = \varnothing\}$
- $L_2 = \{\langle M\rangle \in \{0,1\}^* \mid L(M) \cap \{0^{2^n} \in \{0,1\}^* \mid n \in \mathbb{N}\} \neq \varnothing\}$

είναι αναδρομικά απαριθμήσιμες.

6.8 (☆☆☆). Εξετάστε αν οι γλώσσες:

- $L_1 = \{\langle M\rangle \in \{0,1\}^* \mid$ Υπάρχουν τουλάχιστον δύο λέξεις w_1, w_2, με $|w_1| \neq |w_2|$, για τις οποίες η M τερματίζει$\}$
- $L_2 = \{\langle M\rangle \in \{0,1\}^* \mid$ Υπάρχουν ακριβώς δύο λέξεις w_1, w_2, με $|w_1| \neq |w_2|$, για τις οποίες η M τερματίζει$\}$

είναι αναδρομικά απαριθμήσιμες.

6.9 (★☆☆). Εξετάστε αν οι γλώσσες:

- $L_1 = \{\langle M\rangle \in \{0,1\}^* \mid |L(M)| \leq 68\}$
- $L_2 = \{\langle M\rangle \in \{0,1\}^* \mid |L(M)| \geq 68\}$

είναι αναδρομικά απαριθμήσιμες.

6.10 (★☆☆). Εξετάστε αν οι γλώσσες:

- $L_1 = \{\langle M\rangle \in \{0,1\}^* \mid \text{Η } M \text{ τερματίζει για όλες τις λέξεις με άρτιο μήκος}\}$
- $L_2 = \{\langle M\rangle \in \{0,1\}^* \mid \text{Υπάρχει λέξη αρτίου μήκους για την οποία η } M \text{ τερματίζει}\}$

είναι αναδρομικά απαριθμήσιμες.

6.11 (★☆☆). Εξετάστε αν η γλώσσα $L = \{\langle M\rangle \in \{0,1\}^* \mid |L(M)| \text{ είναι πρώτος αριθμός}\}$ είναι αναδρομικά απαριθμήσιμη.

6.12 (★☆☆). Εξετάστε αν η γλώσσα $L = \{\langle M\rangle \in \{0,1\}^* \mid \text{Η } M \text{ τερματίζει για όλα τα παλίνδρομα του } \{0,1\}^*\}$ είναι αναδρομικά απαριθμήσιμη.

6.13 (★☆☆). Εξετάστε αν η γλώσσα $L = \{\langle M\rangle \in \{0,1\}^* \mid |L(M)| = |\overline{L(M)}| = \aleph_0\}$ είναι αναδρομικά απαριθμήσιμη.

ΚΕΦΑΛΑΙΟ 7

ΤΟ ΘΕΩΡΗΜΑ ΑΝΑΔΡΟΜΗΣ

7.1 Μπορούν οι μηχανές να αυτοαναπαράγονται;

Προτού απαντήσουμε σε αυτό το ερώτημα ας παρακολουθήσουμε τον ακόλουθο συλλογισμό:

1. *Οι ζωντανοί οργανισμοί είναι μηχανές.*

   Η πρόταση αυτή είναι αληθής και αποτελεί θεμελιώδες δόγμα της σύγχρονης Βιολογίας. Οι ζωντανοί οργανισμοί λειτουργούν με «μηχανιστικό» τρόπο.

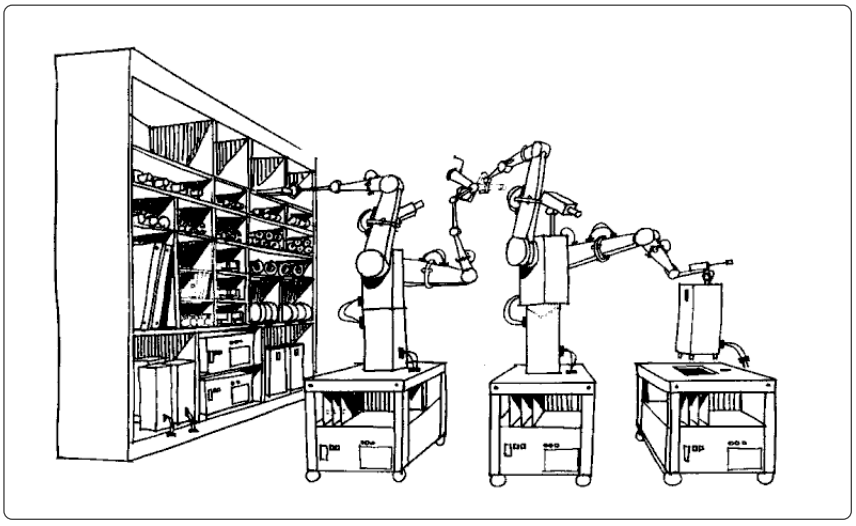
2. *Οι ζωντανοί οργανισμοί μπορούν να αυτοαναπαράγονται.*

   Η πρόταση αυτή είναι επίσης αληθής. Είναι ουσιώδες γνώρισμα των ζωντανών οργανισμών να μπορούν να παράξουν, μέσω κάποιας διαδικασίας γονιμοποίησης και γέννησης, έναν ζωντανό οργανισμό του ίδιου είδους.

Μπορούν λοιπόν οι μηχανές να αυτοαναπαράγονται, όπως θα έκανε ένας ζωντανός οργανισμός;

Μιλώντας γενικά για «μηχανές», ίσως απαντούσαμε αρνητικά, καθώς αν η μηχανή A παράγει τη μηχανή B λογικά θα πρέπει να είναι «πιο πολύπλοκη» (σε επίπεδο σχεδίασης και περιγραφής) από τη B. Συνεπώς η A δεν θα μπορούσε να παράξει την A. Με ορισμότερη σκέψη όμως, μάλλον θα καταλήγαμε σε καταφατική απάντηση (δες Σχήμα 7.1.1). Αυτό που καθοδηγεί σε λάθος δρόμο τη διαίσθησή μας είναι το γεγονός ότι σχεδιάζουμε μία μηχανή με σκοπό να πράξει μία συγκεκριμένη διαδικασία, και συνήθως αυτή η διαδικασία δεν είναι η αναπαραγωγή! Αυτό δεν σημαίνει όμως ότι δεν μπορούμε να σχεδιάσουμε μία μηχανή που (αν την τροφοδοτήσουμε με τα απαραίτητα υλικά) να μπορεί να κατασκευάσει μία μηχανή του ίδιου τύπου [1].

[1] Ενδιαφέρον παρουσιάζει η ιδέα των αυτοαναπαραγόμενων διαστημοπλοίων (γνωστά και ως *Von Neumann probes*) και τα διάφορα φιλοσοφικά εωτήματα που εγείρουν όσον αφορά την ύπαρξη εξωγήινων πολιτισμών (*Παράδοξο του Fermi*).



Σχήμα 7.1.1: *Καλλιτεχνική αναπαράσταση μίας μηχανής που αυτοαναπαράγεται.*

Ας επικεντρωθούμε όμως στις μηχανές που μας ενδιαφέρουν, τις ΤΜ, και ας μεταφέρουμε το ερώτημα στα πλαίσιά τους. Τι σημαίνει όμως αυτοαναπαραγωγή για έναν αλγόριθμο; Η πιο συνετή προσέγγιση θα ήταν η εξής:

> *Ένας αλγόριθμος αυτοαναπαράγεται αν έχει ως έξοδο κάποια κωδικοποίηση του ίδιου του εαυτού!*

Σκοπός της παραγράφου αυτής είναι να αποδείξουμε ότι και οι ΤΜ μπορούν να αυτοαναπαράγονται με την παραπάνω έννοια: *Μπορεί μία ΤΜ M να έχει σαν έξοδο την $\langle M \rangle$.* Μπορούμε να φανταστούμε τις ΤΜ σαν ένα πρόγραμμα (δες Σελίδα 19) και ξέρουμε ότι ένα πρόγραμμα μπορεί να έχει σαν έξοδο τον ίδιο τον κώδικα του. Για παράδειγμα ας δούμε το ακόλουθο πρόγραμμα σε ψευδογλώσσα [1]:

```
 Γράψε 2 αντίγραφα του παρακάτω μηνύματος το 2ο σε εισαγωγικά.
"Γράψε 2 αντίγραφα του παρακάτω μηνύματος το 2ο σε εισαγωγικά."
```

Σε φυσική γλώσσα αυτό θα το γράφαμε απλούστατα ως εξής:

```
Γράψε αυτήν την πρόταση.
```

[1] Σε Python θα γράφαμε π.χ.:

```
a = ['print("a =", a)','for s in a:','    print(s)']
print("a =", a)
for s in a:
    print(s)
```

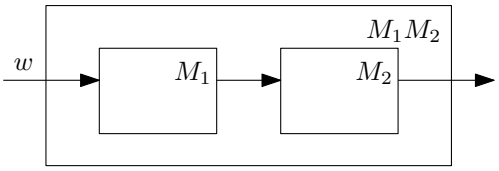
Παραδείγματα για άλλες γλώσσες προγραμματισμού υπάρχουν εδώ: `http://www.nyx.net/~gthompso/quine.htm`.

όμως μία γλώσσα προγραμματισμού δεν μπορεί να καταλάβει την *αυτοαναφορά* (την λέξη «αυτήν» δηλαδή).

Μιμούμενοι την παραπάνω υλοποίηση της αυτοαναπαραγωγής αλγορίθμων, μέσω της αυτοαναφοράς, θα αποδείξουμε ότι υπάρχουν ΤΜ με έξοδο την κωδικοποίησή τους (οι λεγόμενες *αυτογραφικές ΤΜ*). Μάλιστα θα προχωρήσουμε την ιδέα αυτή περεταίρω και θα αποδείξουμε κάτι ακόμα πιο εντυπωσιακό: *Μία ΤΜ M μπορεί να χρησιμοποιεί κατά τη λειτουργία της την $\langle M\rangle$*. Μπορεί να έχει δηλαδή «επίγνωση» του «εαυτού» της και να εκμεταλευτεί αυτό το γεγονός κατά τον υπολογισμό.

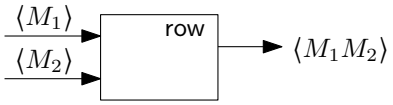
Είναι πια καιρός να αφήσουμε τη φιλοσοφία και να επανέλθουμε στον κόσμο των μαθηματικών. Θα ξεκινήσουμε εισάγοντας τον συμβολισμό που θα διευκολύνει την περιγραφή ΤΜ που θα ορίσουμε στη συνέχεια.

Συμβολισμός 7.1.1. Έστω ΤΜ M_1, M_2. Θεωρούμε την ΤΜ M_1M_2:



που τρέχει την M_1 με είσοδο w και όταν αυτή τερματίσει (αν τερματίσει) τρέχει την M_2 με είσοδο το περιεχόμενο της ταινίας της $M_1(w)$ κατά τον τερματισμό της. Στην περίπτωση όπου η M_2 δέχεται δύο εισόδους (όπως στην απόδειξη του Θεωρήματος 7.2.1), η πρώτη θα είναι το περιεχόμενο της ταινίας της $M_1(w)$ και η δεύτερη η w.

Θεωρούμε επίσης την ΤΜ row:



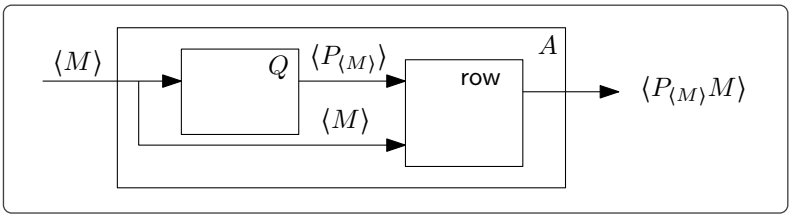
που δέχεται ως είσοδο τις κωδικοποιήσεις των ΤΜ M_1 και M_2 και επιστρέφει την κωδικοποίηση της ΤΜ M_1M_2 (και όχι την παράθεση των λέξεων $\langle M_1\rangle, \langle M_2\rangle$).

Θεώρημα 7.1.2. Υπάρχει ΤΜ M που («αγνοεί» την είσοδό της και) επιστρέφει $\langle M\rangle$.

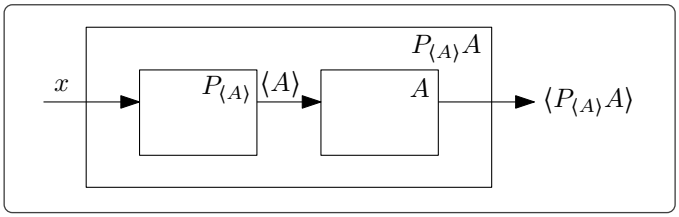
Απόδειξη. Θεωρούμε την ΤΜ P_w που «αγνοεί» την είσοδό της και επιστρέφει τη λέξη w και την ΤΜ Q που παίρνει μία λέξη w σαν είσοδο και επιστρέφει την $\langle P_w\rangle$. Τέλος, θεωρούμε την ΤΜ A του Σχήματος 7.1.2 και παρατηρούμε ότι η ΤΜ $P_{\langle A\rangle}A$ του Σχήματος 7.1.3 («αγνοεί» την είσοδό της και) επιστρέφει $\langle P_{\langle A\rangle}A\rangle$, άρα είναι η ΤΜ που αναζητούσαμε. □

Όμως σε ποιο σημείο εφαρμόζεται η αυτοαναφορά στην παραπάνω απόδειξη; Τυπικά η αυτοαναφορά στα μαθηματικά εκφράζεται μέσω κάποιου *Θεωρήματος Σταθερού Σημείου* (δες Θεώρημα 7.3.4). Οι λεπτομέρειες θα αφεθούν ως άσκηση (Άσκηση 7.9[1])...

[1] Ίσως μια μικρή βοήθεια: Θεωρήστε τον μετασχηματισμό ΤΜ $t : \mathcal{G} \to \mathcal{G}$ με $t(\langle M\rangle) = \langle P_{\langle M\rangle}\rangle$.



Σχήμα 7.1.2: *Η TM A στην απόδειξη του Θεωρήματος 7.1.2.*



Σχήμα 7.1.3: *Η TM $P_{\langle A \rangle} A$ στην απόδειξη του Θεωρήματος 7.1.2.*

7.2 Το Θεώρημα Αναδρομής

Θεώρημα 7.2.1 (Θεώρημα Αναδρομής[1])**.** Για κάθε υπολογίσιμη συνάρτηση $t : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ υπάρχει TM R τέτοια ώστε για κάθε $x \in \{0,1\}^*$:

$$\phi_R(x) = t(\langle R \rangle, x)$$

όπου ϕ_R είναι η συνάρτηση που υπολογίζει η TM R (δες Ορισμό 1.2.13).

Απόδειξη. Έστω T η TM που υπολογίζει τη συνάρτηση t (η T δέχεται σαν είσοδο δύο λέξεις). Παρατηρούμε ότι η TM $P_{\langle AT \rangle} AT$ του Σχήματος 7.2.1, με είσοδο $x \in \{0,1\}^*$ επιστρέφει την τιμή $t(\langle P_{\langle AT \rangle} AT \rangle, x)$, άρα είναι η TM R που αναζητούσαμε. □

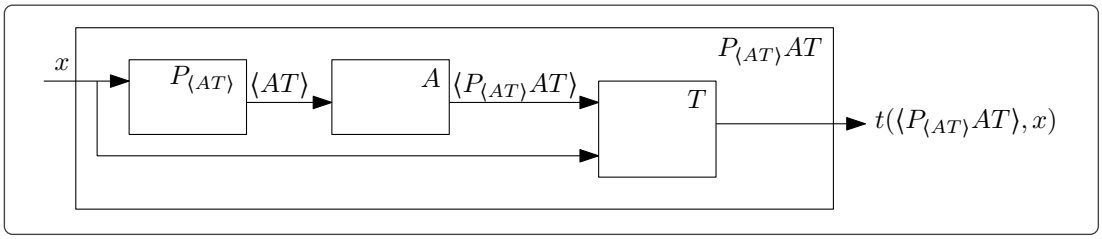
Ως πρώτο παράδειγμα εφαρμογής του Θεωρήματος Αναδρομής θα αποδείξουμε ξανά το γεγονός ότι $HP \notin \mathsf{REC}$.

Παράδειγμα 7.2.2. Έστω (προς άτοπο) ότι η TM H αποφασίζει την HP. Θεωρούμε τη συνάρτηση $t : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$, με:

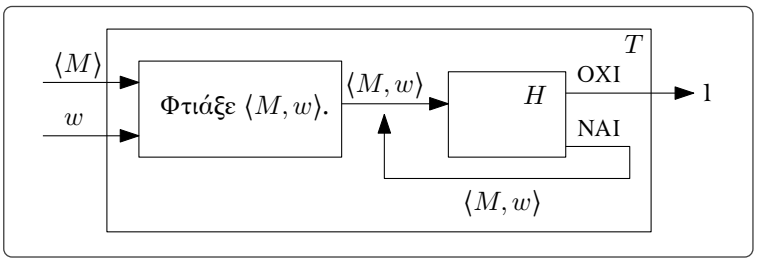
$$t(x,w) = \begin{cases} 1 & , \text{ αν υπάρχει TM } M \text{ τέτοια ώστε } x = \langle M \rangle \text{ και } M(w) \uparrow \\ \perp & , \text{ αλλιώς} \end{cases}$$

Αυτή η (μερική) συνάρτηση είναι υπολογίσιμη (π.χ. από την TM του Σχήματος 7.2.2), άρα από το Θεώρημα 7.2.1 υπάρχει TM R τέτοια ώστε για κάθε $w \in \{0,1\}^*$:

[1] Στη βιβλιογραφία το Θεώρημα αυτό αναφέρεται ως *Δεύτερο Θεώρημα Αναδρομής του Kleene* και δεν θα πρέπει να συγχέεται με το Θεωρήμα Ανδρομής που συναντάμε στην *Αξιωματική Θεωρία Συνόλων* (το δεύτερο αποδεικνύει την ύπαρξη των συναρτήσεων που ορίζονται αναδρομικά, ενώ το πρώτο αποδεικνύει ότι οι συναρτήσεις που ορίζονται αναδρομικά μέσω υπολογισμών συναρτήσεων είναι υπολογίσιμες, δες Άσκηση 7.7).



Σχήμα 7.2.1: *Η ΤΜ $P_{\langle AT\rangle}AT$ στην απόδειξη του Θεωρήματος 7.2.1.*



Σχήμα 7.2.2: *Η ΤΜ του Παραδείγματος 7.2.2 (αν η πρώτη είσοδος δεν είναι κωδικοποίηση ΤΜ η T θα κολλήσει).*

$$\phi_R(w) = t(\langle R\rangle, w) = \begin{cases} 1 & , \text{ αν } R(w)\uparrow \\ \perp & , \text{ αν } R(w)\downarrow \end{cases} = \begin{cases} 1 & , \text{ αν } \phi_R(w) = \perp \\ \perp & , \text{ αν } \phi_R(w) \neq \perp \end{cases}$$

πράγμα που φυσικά είναι άτοπο.

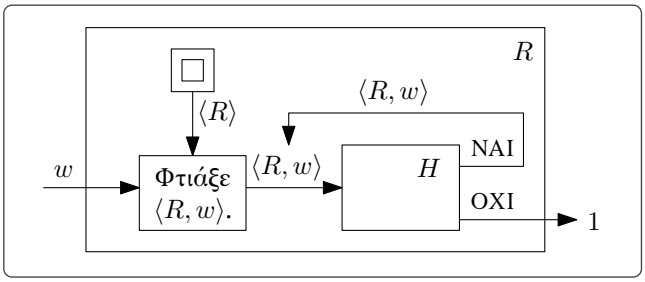
Το Παράδειγμα 7.2.2 είναι ενδεικτικό της δύναμης του Θεωρήματος Αναδρομής, καθώς μας δείχνει ότι μπορεί να χρησιμοποιηθεί για να αποδείξουμε ότι η HP δεν ανήκει στο REC, χωρίς να χρειαστεί να κάνουμε διαγωνιοποίηση! Βέβαια στην πραγματικότητα, αντί για διαγωνιοποίηση χρησιμοποιήσαμε αυτοαναφορά, μία έννοια που στη λογική ταυτίζεται συχνά με το διαγώνιο επιχείρημα του Cantor (και όπως προείπαμε με τα Θεωρήματα Σταθερού Σημείου).

Πόρισμα 7.2.3. Έστω υπολογίσιμη συνάρτηση $f : \{0,1\}^* \to \{0,1\}^*$. Υπάρχει ΤΜ R που υπολογίζει την f και «χρησιμοποιεί [1]» κατά τον υπολογισμό την $\langle R\rangle$.

Πράγματι, αρκεί να θεωρήσουμε τη συνάρτηση $t : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ με $t(x, y) = f(y)$, καθώς από το Θεώρημα 7.2.1 (αφού η t προφανώς είναι υπολογίσιμη) παίρνουμε ΤΜ R τέτοια ώστε για κάθε $y \in \{0,1\}^*$ να ισχύει ότι $\phi_R(y) = t(\langle R\rangle, y) = f(y)$ [2].

[1] Χρησιμοποιούμε τον όρο «χρησιμοποιεί» για να εκφράσουμε το γεγονός ότι η R κατά την διάρκεια του υπολογισμού της παράγει την $\langle R\rangle$.

[2] Πιο αναλυτικά: Έστω M_f η ΤΜ που υπολογίζει την f και T η ΤΜ που υπολογίζει την t (απλά τρέχει την M_f για τη δεύτερη είσοδο). Τότε η ζητούμενη R είναι η $P_{\langle AT\rangle}AT$ (η υπορουτίνα $P_{\langle AT\rangle}A$ παράγει την $\langle R\rangle$).



Σχήμα 7.2.3: *Η ΤΜ του Παραδείγματος 7.2.5, όπου H η ΤΜ που (υποθετικά) αποφασίζει την HP.*

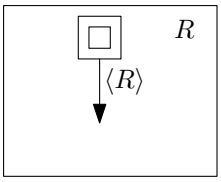
Στην απόδειξη του παραπάνω Πορίσματος η συνάρτηση t (και κατεπέκταση η ΤΜ T που την υπολογίζει) στην ουσία δεν εκμεταλευόταν την $\langle R\rangle$. Τίποτα δεν μας εμποδίζει φυσικά να ορίσουμε πιο σύνθετες συναρτήσεις t έτσι ώστε να γίνει ουσιαστική εφαρμογή του Θεωρήματος Αναδρομής.

Πόρισμα (του Πορίσματος 7.2.3). Έστω γλώσσα $L \in \mathsf{RE}$. Υπάρχει ΤΜ R με $L(R) = L$ που «χρησιμοποιεί» στον υπολογισμό της την $\langle R\rangle$ [1].

Αν κοιτάξουμε προσεκτικά την απόδειξη του Θεωρήματος 7.2.1 θα δούμε ότι η ΤΜ R (με άλλα λόγια η $P_{\langle AT\rangle}AT$) πρώτα δημιουργεί την $\langle R\rangle$ (δηλαδή την $\langle P_{\langle AT\rangle}AT\rangle$, μέσω της υπορουτίνας $P_{\langle AT\rangle}A$) και έπειτα τη χρησιμοποιεί για να υπολογίσει την $t(\langle R\rangle, x)$ (δίνοντάς την ως είσοδο στην T μαζί με την x). Το γεγονός αυτό αποτελεί την έμπνευση του ακόλουθου συμβολισμού.

Συμβολισμός 7.2.4 (Κουτάκια συνέχεια...).

8. Όταν χρησιμοποιούμε το Θεώρημα Αναδρομής κατά τον σχεδιασμό μίας ΤΜ θα γράφουμε:

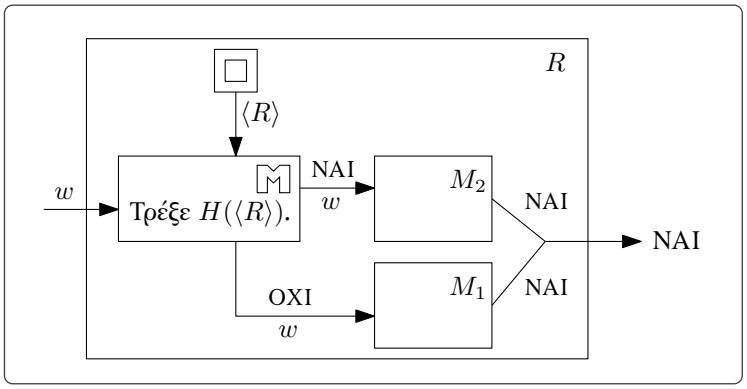


Παράδειγμα 7.2.5 (Το Παράδειγμα 7.2.2 με τον παραπάνω συμβολισμό). Θωρούμε την ΤΜ R του Σχήματος 7.2.3 και παρατηρούμε ότι για $w \in \{0,1\}^*$:

$$R(w)\downarrow \Leftrightarrow H(\langle R, w\rangle)\downarrow_{q_{\text{όχι}}} \Leftrightarrow R(w)\uparrow$$

που είναι άτοπο.

[1] Δες Άσκηση 7.1.



Σχήμα 7.2.4: *Η ΤΜ του Παραδείγματος 7.2.6.*

Εδώ ίσως πρέπει να τονίσουμε το γεγονός ότι για την παραπάνω απόδειξη (και για όσες ακολουθούν) δεν χρησιμοποιούμε το Πόρισμα 7.2.3 (και το πόρισμά του) αλλά κατευθείαν την απόδειξη του Θεωρήματος Αναδρομής: Ορίζουμε την ΤΜ T του Σχήματος 7.2.2 και έπειτα παίρνουμε ως R τη μηχανή $P_{\langle AT\rangle}AT$ (το διπλό κουτάκι του Συμβολισμού 7.2.4 στην πραγματικότητα είναι η υπορουτίνα $P_{\langle AT\rangle}A$).

Οι αποδείξεις των Παραδειγμάτων 7.2.2 και 7.2.5 βασίζονται σε ακριβώς τα ίδια επιχειρήματα, όμως ο Συμβολισμός 7.2.4 απλοποιεί αρκετά την παρουσίαση.

Παράδειγμα 7.2.6 (Εναλλακτική απόδειξη του Θεωρήματος 6.1.1).
($\Rightarrow$) Έστω ιδιότητα $\mathcal{P} \subseteq \mathsf{RE}$ με $\mathcal{P} \notin \{\varnothing, \mathsf{RE}\}$ και γλώσσες $L_1 \in \mathcal{P}$ και $L_2 \in \mathsf{RE} \setminus \mathcal{P}$. Έστω επίσης ότι οι ΤΜ M_1, M_2 ημι-αποφασίζουν τις L_1 και L_2 αντίστοιχα και (προς άτοπο) ότι η H αποφασίζει την $L_{\mathcal{P}}$. Παρατηρούμε ότι για την ΤΜ του Σχήματος 7.2.4 ισχύει ότι:

- $\langle R\rangle \in L_{\mathcal{P}} \Rightarrow H(\langle R\rangle) \downarrow_{q_{\text{ναι}}} \Rightarrow L(R) = L(M_2) = L_2 \notin \mathcal{P} \Rightarrow \langle R\rangle \notin L_{\mathcal{P}}$

- $\langle R\rangle \notin L_{\mathcal{P}} \Rightarrow H(\langle R\rangle) \downarrow_{q_{\text{όχι}}} \Rightarrow L(R) = L(M_1) = L_1 \in \mathcal{P} \Rightarrow \langle R\rangle \in L_{\mathcal{P}}$

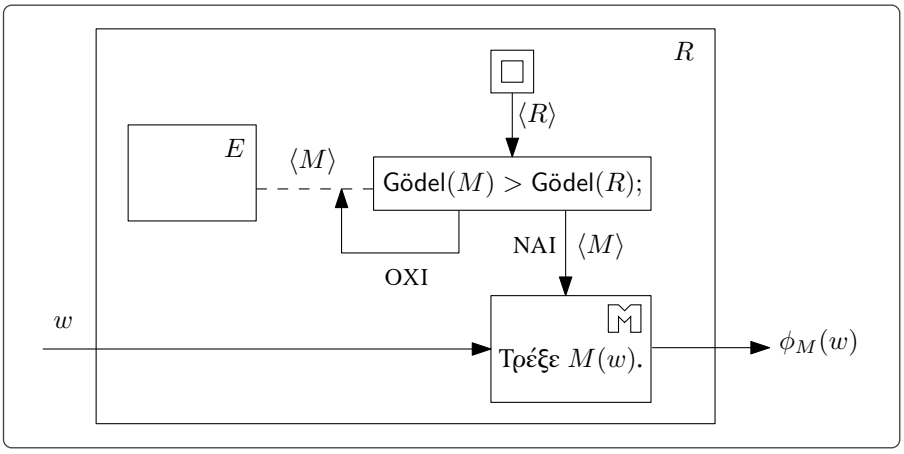
που είναι άτοπο.

Θα κλείσουμε τα παραδείγματα εφαρμογών του Θεωρήματος Αναδρομής ορίζοντας μία πολύ ενδιαφέρουσα κλάση ΤΜ. Υπάρχουν αριθμησίμως άπειρες ΤΜ που αναγνωρίζουν μια γλώσσα $L \in \mathsf{RE}$, απ' όλες αυτές, ακριβώς μία έχει τη *βραχύτερη-συντομότερη «περιγραφή»*.

Ορισμός 7.2.7. Μία ΤΜ M καλείται *βραχύτατη ΤΜ* ανν για κάθε $i \in \mathbb{N}$ με $i < \mathsf{Gödel}(M)$ ισχύει ότι $\phi_{M_i} \neq \phi_M$, όπου M_i η ΤΜ με αριθμό Gödel i. Ορίζουμε επίσης τη γλώσσα $L_{\text{Βραχύτατες}} = \{\langle M\rangle \in \{0,1\}^* \mid M \text{ βραχύτατη ΤΜ}\}$.

Παρατηρήστε ότι η $L_{\text{Βραχύτατες}}$ περιέχει τις βραχύτερες κωδικοποιήσεις ΤΜ που αναγνωρίζουν τις γλώσσες στο RE. Θα δείξουμε ότι αυτή η γλώσσα δεν είναι αναδρομικά απαριθμήσιμη.

Λήμμα 7.2.8. Η γλώσσα $L_{\text{Βραχύτατες}}$ είναι άπειρη.



Σχήμα 7.2.5: *Η ΤΜ της Πρότασης 7.2.9.*

Απόδειξη. Έστω (προς άτοπο) ότι $L_{\text{Βραχύτατες}} = \{\langle M_1\rangle, \langle M_2\rangle \dots, \langle M_n\rangle\}$ για κάποιο $n \in \mathbb{N}$. Παρατηρούμε ότι υπάρχει πεπερασμένη γλώσσα $L \notin \{L(M_1), L(M_2), \dots, L(M_n)\}$ [1]. Συνεπώς η βραχύτατη ΤΜ που αποφασίζει την L θα έπρεπε να είναι μία εκ των $M_1, M_2, \dots, M_n$. Άτοπο. □

Πρόταση 7.2.9. $L_{\text{Βραχύτατες}} \notin \mathsf{RE}$.

Απόδειξη. Έστω (προς άτοπο) ότι $L_{\text{Βραχύτατες}} \in \mathsf{RE}$ και ότι ο απαριθμητής E την απαριθμεί. Θεωρούμε την ΤΜ R του Σχήματος 7.2.5 και παρατηρούμε ότι ο E κάποτε θα επιστρέψει μία ΤΜ M με $\mathsf{Gödel}(M) > \mathsf{Gödel}(R)$, καθώς η $L_{\text{Βραχύτατες}}$ είναι άπειρη (Λήμμα 7.2.8). Οπότε θα έχουμε:

$$\left.\begin{array}{l}\phi_R = \phi_M \\ \langle M\rangle \in L_{\text{Βραχύτατες}}\end{array}\right\} \Rightarrow \mathsf{Gödel}(M) \leq \mathsf{Gödel}(R)$$

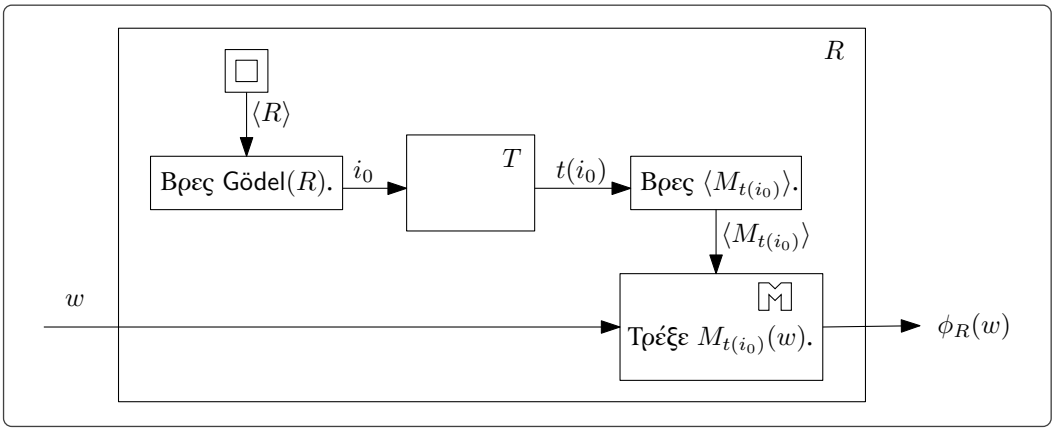
που είναι άτοπο. □

7.3 Το Πρώτο Θεώρημα Μη-πληρότητας του Gödel

Ορισμός 7.3.1. *Μετασχηματισμός ΤΜ* είναι οποιαδήποτε συνάρτηση $t : \mathcal{G} \to \mathcal{G}$ (δες Ορισμό 1.4.10).

Για τους σκοπούς αυτής της παραγράφου μας βολεύει να περάσουμε πάλι στον «κόσμο» των φυσικών αριθμών και των υπολογίσιμων αριθμητικών συναρτήσεων. Για παράδειγμα ο παραπάνω ορισμός μπορεί να εκφραστεί πιο απλά, αν αντί για την κωδικοποίηση μιας ΤΜ χρησιμοποιήσουμε τον αριθμό Gödel της.

[1] Παρατηρήστε ότι ακριβώς μία από τις $L(M_1), \dots, L(M_n)$ μπορεί να είναι η $\{0,1\}^*$, έστω χωρίς βλάβη της γενικότητας ότι είναι η M_1 (η περίπτωση όπου καμία από τις $L(M_1), \dots, L(M_n)$ δεν είναι η $\{0,1\}^*$ καλύπτεται από τα επιχειρήματα που θα ακολουθήσουν). Συνεπώς υπάρχουν λέξεις $w_2 \notin L(M_2), \dots, w_n \notin L(M_n)$. Παρατηρήστε ότι $L = \{w_2, \dots, w_n\} \notin \{L(M_1), L(M_2), \dots, L(M_n)\}$.



Σχήμα 7.3.1: *Η ΤΜ που «αποτελεί» σταθερό σημείο για τον μετασχηματισμό t.*

Ορισμός 7.3.2. *Μετασχηματισμός ΤΜ* είναι οποιαδήποτε συνάρτηση $t : \mathbb{N} \to \mathbb{N}$.

Ορισμός 7.3.3. Έστω μετασχηματισμός $t : \mathbb{N} \to \mathbb{N}$. Το $i_0 \in \mathbb{N}$ είναι *σταθερό σημείο του* t ανν οι ΤΜ με αριθμούς Gödel i_0 και $t(i_0)$ είναι ισοδύναμες (δες Ορισμό 1.2.14).

Χάριν συντομίας σε όσα έπονται θα συμβολίζουμε με M_i την ΤΜ με αριθμό Gödel i και με ϕ_i τη συνάρτηση που υπολογίζει (την ϕ_{M_i} δηλαδή). Συνεπώς, μπορούμε πιο απλά να πούμε ότι το i_0 θα είναι σταθερό σημείο του μετασχηματισμού t ανν $\phi_{i_0} = \phi_{t(i_0)}$.

Θεώρημα 7.3.4 (Θεώρημα Σταθερού Σημείου)**.** Κάθε πλήρης και υπολογίσιμος μετασχηματισμός ΤΜ έχει σταθερό σημείο.

Απόδειξη. Έστω T η ΤΜ που υπολογίζει τον μετασχηματισμό t. Παρατηρούμε ότι αν η ΤΜ R του Σχήματος 7.3.1 έχει αριθμό Gödel i_0 τότε $\phi_R = \phi_{i_0} = \phi_{t(i_0)}$. □

Το Θεώρημα 7.3.4 θα το συνατήσετε στη βιβλιογραφία ως *Θεώρημα Σταθερού Σημείου του Rogers*. Ας δούμε ένα παράδειγμα εφαρμογής του.

Πρόταση 7.3.5. Για κάθε πλήρη, υπολογίσιμο, 1-1 και επί μετασχηματισμό $t : \mathbb{N} \to \mathbb{N}$ υπάρχει $i_0 \in \mathbb{N}$ τέτοιο ώστε $\phi_{t(i_0)} = \phi_{t(i_0+1)}$ [1].

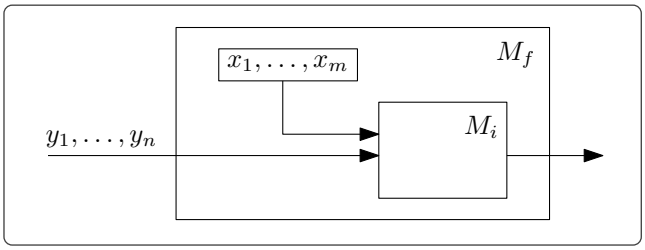
Απόδειξη. Αφού η t είναι 1-1 και επί έπεται ότι αντιστρέφεται. Θεωρούμε τη συνάρτηση $\sigma : \mathbb{N} \to \mathbb{N}$ με $\sigma(x) = t(t^{-1}(x) + 1)$. Από την Πρόταση 1.2.12 προκύπτει ότι η σ είναι υπολογίσιμη ως σύνθεση υπολογίσιμων συναρτήσεων και (προφανώς) πλήρης, άρα μπορούμε να εφαρμόσουμε το Θεώρημα 7.3.4 και να πάρουμε $j_0 \in \mathbb{N}$ τέτοιο ώστε:

$$\phi_{j_0} = \phi_{\sigma(j_0)} \tag{7.1}$$

Παρατηρούμε ότι το $i_0 = t^{-1}(j_0)$ έχει τη ζητούμενη ιδιότητα καθώς:

$$\phi_{\sigma(j_0)} = \phi_{t(t^{-1}(j_0)+1)} = \phi_{t(i_0+1)}$$

[1] Δηλαδή οι ΤΜ με αριθμούς Gödel $t(i_0)$ και $t(i_0 + 1)$ είναι ισοδύναμες.



Σχήμα 7.3.2: *Η TM M_f στην απόδειξη του Θεωρήματος 7.3.7.*

και

$$\phi_{j_0} = \phi_{t(t^{-1}(j_0))} = \phi_{t(i_0)}$$

άρα από την (7.1) έπεται ότι $\phi_{t(i_0)} = \phi_{t(i_0+1)}$. □

Fun fact: Το Θεώρημα Σταθερού Σημείου είναι ισοδύναμο με το Θεώρημα Αναδρομής (δες Ασκήσεις 7.8 και 7.10). Για λόγους πληρότητας θα ξαναδιατυπώσουμε το Θεώρημα 7.2.1 χρησιμοποιώντας τον συμβολισμό αυτής της παραγράφου.

Θεώρημα 7.3.6. Για κάθε υπολογίσιμη συνάρτηση $t : \mathbb{N}^2 \to \mathbb{N}$ υπάρχει $i \in \mathbb{N}$ (αριθμός Gödel TM δηλαδή) τέτοιο ώστε για κάθε $x \in \mathbb{N}$:

$$\phi_i(x) = t(i, x)$$

Θεώρημα 7.3.7 (Θεώρημα S-m-n [1]). Για κάθε υπολογίσιμη συνάρτηση $g : \mathbb{N}^{m+n} \to \mathbb{N}$ και $x_1, \ldots, x_m \in \mathbb{N}$ υπάρχει υπολογίσιμη συνάρτηση $f : \mathbb{N}^n \to \mathbb{N}$ τέτοια ώστε:

$$\forall y_1, \ldots, y_n \in \mathbb{N}\ (f(y_1, \ldots, y_n) = g(x_1, \ldots, x_m, y_1, \ldots, y_n))$$

Επιπλέον, υπάρχει πλήρης και υπολογίσιμη συνάρτηση $\mathsf{S}^{\mathsf{m}}_{\mathsf{n}} : \mathbb{N}^{m+1} \to \mathbb{N}$ τέτοια ώστε, αν $\phi_i = g$ τότε:

$$\phi_{\mathsf{S}^{\mathsf{m}}_{\mathsf{n}}(i, x_1, \ldots, x_m)} = f \text{ [2]}$$

Απόδειξη. Έστω M_i η TM που υπολογίζει την g. Παρατηρούμε ότι η TM M_f του Σχήματος 7.3.2 υπολογίζει την f.

Τέλος, ορίζουμε τη συνάρτηση $\mathsf{S}^{\mathsf{m}}_{\mathsf{n}}(i, x_1, \ldots, x_m) = \mathsf{Gödel}(M_f)$. Η συνάρτηση αυτή είναι προφανώς υπολογίσιμη [3] και πλήρης. □

Πλέον έχουμε τα δύο βασικά λήμματα που χρειαζόμαστε για να αποδείξουμε το Θεώρημα Μη-πληρότητας του Gödel. Ο αναγνώστης που δεν είναι εξοικειωμένος με την πρωτοβάθμια λογική θα πρέπει να ανατρέξει στο Παράρτημα Α προτού συνεχίσει τη μελέτη του.

[1] Το θεώρημα αυτό πολλές φορές στη βιβλιογραφία αναφέρετε και ως *Θεώρημα Παραμετροποίησης*.

[2] Με λόγια: Υπάρχει πλήρης και υπολογίσιμη συνάρτηση $\mathsf{S}^{\mathsf{m}}_{\mathsf{n}}$ τέτοια ώστε αν η TM με αριθμό Gödel i υπολογίζει την g τότε η TM με αριθμό Gödel $\mathsf{S}^{\mathsf{m}}_{\mathsf{n}}(i, x_1, \ldots, x_m)$ υπολογίζει την f.

[3] Αφού υπολογίσουμε την κωδικοποίηση της M_i, έχοντας τις «σταθερές» $x_1, \ldots, x_m$, μπορούμε να φτιάξουμε την κωδικοποίηση της M_f και έπειτα να βρούμε τον αριθμό Gödel της.

Θεώρημα 7.3.8 ($1^ο$ Θεώρημα Μη-πληρότητας Gödel). Υπάρχει πρόταση φ της $\Gamma_1^{\partial\alpha}$ τέτοια ώστε αν το P είναι συνεπές τότε $P \nvdash \varphi$ και $P \nvdash \neg\varphi$ [1].

Απόδειξη. Έστω ότι το P είναι συνεπές και έστω (προς άτοπο) ότι για κάθε πρόταση φ της $\Gamma_1^{\partial\alpha}$ ισχύει ότι είτε $P \vdash \varphi$ είτε $P \vdash \neg\varphi$.

Θυμηθείτε ότι η συνάρτηση που υπολογίζει μία ΤΜ είναι ελαχιστικά αναδρομική (Θεώρημα 2.5.1). Θα συμβολίζουμε με f_i την ελαχιστικά αναδρομική συνάρτηση που ορίζει η ϕ_i (η συνάρτηση δηλαδή που υπολογίζει η ΤΜ με αριθμό Gödel i). Από το Θεώρημα Α.5.6 η f_i είναι αναπαραστάσιμη στο P, δηλαδή υπάρχει τύπος $\varphi_i(x, y)$ τέτοιος ώστε για κάθε $x \in \mathbb{N}$:

$$\begin{aligned} f_i(x) = y &\Rightarrow P \vdash \varphi_i(\underline{x}, \underline{y}) \\ f_i(x) \neq y &\Rightarrow P \vdash \neg\varphi_i(\underline{x}, \underline{y}) \end{aligned}$$

Θεωρούμε συνάρτηση $g : \mathbb{N}^2 \to \mathbb{N}$ με:

$$g(i,j) = \begin{cases} 1 & , \text{ αν } P \vdash \forall y\ \neg\varphi_i(\underline{j}, y) \\ \perp & , \text{ αλλιώς} \end{cases}$$

(Παρατηρήστε ότι αν $P \vdash \forall y\ \neg\varphi_i(\underline{j}, y)$, αφού η πρόταση φ_i στην ουσία αναπαριστά τη ϕ_i, τότρε δεν υπάρχει η τιμή $\phi_i(j)$ και κατ' επέκταση ο υπολογισμός $M_i(j)$ δεν τερματίζει. Το γεγονός αυτό θα το αποδείξουμε και τυπικά σε λίγο.)

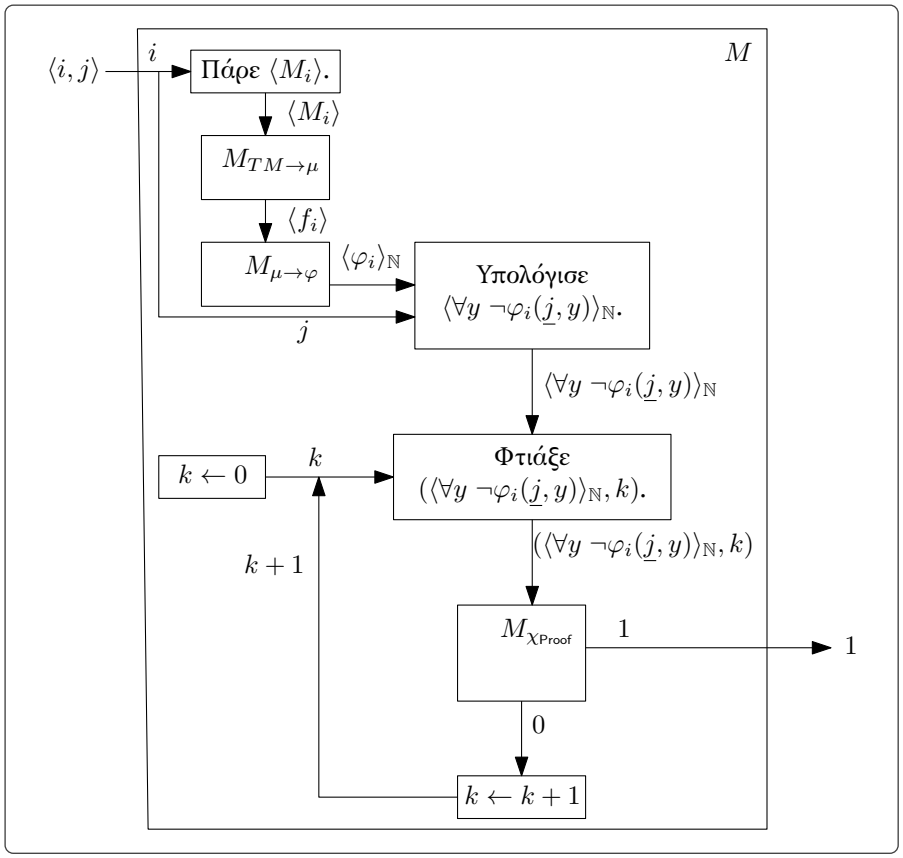
Η συνάρτηση g είναι υπολογίσιμη [2] από την ΤΜ M του Σχήματος 7.3.3, όπου $M_{\chi_{\mathsf{Proof}}}$ η ΤΜ που υπολογίζει τη χαρακτηριστική συνάρτηση της σχέσης Proof (δες Πρόταση Α.5.9 και φυσικά το Θεώρημα 2.5.1) και $M_{TM\to\mu}$, $M_{\mu\to\varphi}$ οι ΤΜ των Παρατηρήσεων 2.5.3 και Α.5.8 αντίστοιχα [3].

Έστω ότι $\text{Gödel}(M) = l$. Από το Θεώρημα 7.3.7 προκύπτει ότι αν θεωρήσουμε το i σαν παράμετρο τότε υπάρχει υπολογίσιμη συνάρτηση f_i τέτοια ώστε για κάθε $j \in \mathbb{N}$ ισχύει ότι

[1] Στην κλασική απόδειξη ο Gödel κατασκεύασε μια πρόταση φ που έφερε το νόημα «Εγώ δεν αποδεικνύομαι στο P», βασιζόταν δηλαδή στην αυτοαναφορά (εκφρασμένη φυσικά μέσω ενός Θεωρήματος Σταθερού Σημείου). Για να ορίσει ο Gödel αυτήν την πρόταση χρειάστηκε να κωδικοποιήσει τους λογικούς τύπους (και τις ακολουθίες αυτών) σε φυσικούς αριθμούς, πράγμα απαραίτητο για να ορίσει την ελαχιστικά αναδρομική σχέση Proof (δες Πρόταση Α.5.9). Η σχέση αυτή περιέχει τα ζευγάρια φυσικών αριθμών που αντιστοιχούν σε τυπική απόδειξη από το P και στην πρόταση που αποδεικνύει αυτή η απόδειξη. Με αυτόν τον τρόπο μπορούμε να μιλάμε για τυπικές αποδείξεις τύπων με κάτι πιο εύκολα «διαχειρίσιμο»: με φυσικούς αριθμού αντί για πεπερασμένες ακολουθίες τύπων. Οπότε για να δείξουμε ότι η αυτοαναφορική πρόταση φ (που αναφέρθηκε πριν) δεν έχει απόδειξη θα πρέπει απλά να δείξουμε ότι δεν υπάρχει φυσικός αριθμός που να αντιστοιχεί σε απόδειξή της. Το επόμενο και τελευταίο βήμα είναι να δείξουμε ότι οι ελαχιστικά αναδρομικές σχέσεις είναι αναπαραστάσιμες (Ορισμός Α.5.5) στο P, μπορούν δηλαδή να «εκφραστούν» με λογικούς τύπους.

[2] Το βασικό συστατικό για να το πετύχουμε αυτό είναι η «κωδικοποίηση».

[3] Κάποιος υποψιασμένος αναγνώστης θα έχει σοβαρές ενστάσεις στο γεγονός αυτό: Εν ολίγης, αν μπορούμε να υπολογίσουμε την g τότε μπορούμε να αναγνωρίσουμε πότε μία ΤΜ τερματίζει για δοσμένη είσοδο (ελέγχωντας αν η τιμή της g είναι 1)! Σε αυτόν τον συλλογισμό όμως θεωρούμε δεδομένο ότι αν για κάποια i, j είναι αληθής η πρόταση $\forall y\ \neg\varphi_i(\underline{j}, y)$ τότε θα ισχύει ότι $P \vdash \forall y\ \neg\varphi_i(\underline{j}, y)$, και ο λόγος φυσικά είναι η υπόθεσή μας (προς άτοπο) ότι για κάθε πρόταση φ ισχύει είτε $P \vdash \varphi$ είτε $P \vdash \neg\varphi$. Ας παρακολουθήσουμε όμως τη συνέχεια της απόδειξης για να οδηγηθούμε και επισίμως στο άτοπο...



Σχήμα 7.3.3: *Η TM M που υπολογίζει τη συνάρτηση g στην απόδειξη του Θεωρήματος 7.3.8 (με $\langle\varphi_i\rangle_{\mathbb{N}}$ συμβολίζουμε τον αριθμό Gödel της πρόταση φ_i, δες Παράγραφο A.5.1).*

$f_i(j) = g(i, j)$ και ότι $f_i = \phi_{\mathsf{S}^1_1(l,i)}$. Επιπλέον, ο μετασχηματισμός t με $t(i) = \mathsf{S}^1_1(l, i)$ είναι πλήρης και υπολογίσιμος, άρα από το Θεώρημα 7.3.4 έχει σταθερό σημείο, έστω $i_0 \in \mathbb{N}$ [1]. Οπότε για κάθε $j \in \mathbb{N}$ ισχύει ότι:

$$g(i_0, j) = f_{i_0}(j) = \phi_{\mathsf{S}^1_1(l,i_0)}(j) = \phi_{t(i_0)}(j) = \phi_{i_0}(j) \tag{7.2}$$

Αφού το P έχει υποτεθεί συνεπές μπορεί να ισχύει ακριβώς ένα από τα ακόλουθα:

1. $P \vdash \forall y\ \neg\varphi_{i_0}(\underline{j}, y)$,
2. $P \vdash \neg\forall y\ \neg\varphi_{i_0}(\underline{j}, y)$

Σκοπός μας είναι να οδηγηθούμε σε άτοπο και στις δύο περιπτώσεις.

[1] Εδώ προσθέτουμε και την αυτοαναφορά στο μείγμα της απόδειξης.

1. Έστω ότι $P \vdash \forall y\ \neg\varphi_{i_0}(\underline{j}, y)$. Από το Θεώρημα Εγκυρότητας (Θεώρημα Α.4.1) προκύπτει ότι $P \vDash \forall y\ \neg\varphi_{i_0}(\underline{j}, y)$ και αφού $\mathfrak{N} \vDash P$, εφαρμόζοντας τον ορισμό του Tarski, προκύπτει ότι για κάθε $n \in \mathbb{N}$ ισχύει ότι $\mathfrak{N} \nvDash \varphi_{i_0}(\underline{j}, y/n)$. Αν ίσχυε ότι $\phi_{i_0}(j) = n$, αφού η φ_{i_0} αναπαριστά την f_{i_0}, θα έπρεπε να ισχύει ότι $P \vdash \varphi_{i_0}(\underline{j}, \underline{n})$, άρα (από το Θεώρημα Εγκυρότητας) ότι $\mathfrak{N} \vDash \varphi_{i_0}(\underline{j}, \underline{n})$ [1]. Συνεπώς ισχύει ότι $\phi_{i_0}(j) \neq n$ για κάθε $n \in \mathbb{N}$, ή αλλιώς ότι $\phi_{i_0}(j) = \perp$.

   Όμως, αφού $P \vdash \forall y\ \neg\varphi_{i_0}(\underline{j}, y)$ έπεται ότι $g(i_0, j) = 1$ και από την (7.2) έπεται ότι $\phi_{i_0}(j) = 1$, που είναι άτοπο.

2. Έστω ότι $P \vdash \neg\forall y\ \neg\varphi_{i_0}(\underline{j}, y)$. Τότε θα είχαμε ότι $g(i_0, j) = \perp$ [2]. Οπότε λόγω της (7.2) θα ισχύει επίσης ότι $\phi_{i_0}(j) = \perp$. Θα δείξουμε, αντίστοιχα με πριν, ότι υπάρχει $n \in \mathbb{N}$ τέτοιο ώστε $\phi_{i_0}(j) = n$, δηλαδή ότι $\phi_{i_0}(j) \neq \perp$, που είναι άτοπο.

   Επικαλούμενοι το Θεώρημα Εγκυρότητας και εφαρμόζοντας τον ορισμό του Tarski καταλήγουμε ότι υπάρχει $n \in \mathbb{N}$ τέτοιο ώστε $\mathfrak{N} \vDash \varphi_{i_0}(\underline{j}, y/n)$. Αν ίσχυε ότι $\phi_{i_0}(j) \neq n$ τότε θα είχαμε $P \vdash \neg\varphi_{i_0}(\underline{j}, \underline{n})$, άρα $\mathfrak{N} \vDash \neg\varphi_{i_0}(\underline{j}, \underline{n})$. Συνεπώς υπάρχει $n \in \mathbb{N}$ τέτοιο ώστε $\phi_{i_0}(j) = n$. □

Παρατήρηση 7.3.9. Η απόδειξη του Θεωρήματος 7.3.8 μας δείχνει ότι υπάρχει ΤΜ Μ (η M_{i_0}) για την οποία δεν μπορούμε να αποδείξουμε (στην $\Gamma_1^{\text{θα}}$) ότι για δεδομένη είσοδο τερματίζει ούτε να αποδείξουμε ότι δεν τερματίζει.

Παρατήρηση 7.3.10. Έστω φ η πρόταση του Θεωρήματος 7.3.8. Αφού προφανώς μία εκ των $\varphi, \neg\varphi$ είναι αληθής στην προτιθέμενη ερμηνεία $\mathfrak{N}$ της $\Gamma_1^{\text{θα}}$, το Θεώρημα 7.3.8 αποδεικνύει ότι υπάρχουν αληθείς προτάσεις των μαθηματικών που χρησιμοποιούμε (που φυσικά εμπεριέχουν την αριθμητική Peano) οι οποίες δεν μπορούν να αποδειχτούν. Μία πιθανή λύση σε αυτό το «πρόβλημα» θα ήταν να διαλέξουμε μία εκ των $\varphi, \neg\varphi$ και να την εντάξουμε ως αξίωμα στο P. Και πάλι όμως θα μπορούσαμε να επαναλάβουμε την απόδειξη του Θεωρήματος 7.3.8 και να βρούμε άλλη πρόταση με αυτήν την ιδιότητα...

Παρόλο που η πρόταση φ του Θεωρήματος 7.3.8 φαίνεται να είναι «κατασκευασμένη» και δε μοιάζει στις προτάσεις των μαθηματικών που έχουμε συνηθίσει, η Μη-πληρότητα της αριθμητικής Peano (και κατ' επέκταση όλων των μαθηματικών που την περιέχουν) δεν αφορά μόνο κατασκευασμένες προτάσεις. Δυστυχώς υπάρχουν προτάσεις με καθαρά «μαθηματικό περιεχόμενο», όχι προτάσεις που προέκυψαν από μια διαδικασία παρόμοια με την απόδειξη του Θεωρήματος Μη-πληρότητας, που απασχολούσαν τους μαθηματικούς καιρό και τελικά αποδείχθηκαν «μη αποδείξιμες».

Σημείωση 7.3.11. Το Θεώρημα 7.3.8 στην ουσία αποδεικνύει ότι το P (που περιέχει μόνο τα στοιχειώδη αξιώματα της αριθμητικής) δεν είναι *τυπικά πλήρες*. Σε αυτήν τη διαπίστωση οδηγούμαστε αν υποθέσουμε ότι το P είναι συνεπές [2]. Είναι όμως το P τελικά συνεπές; Σε

[1] Το οποίο σημαίνει ότι $\mathfrak{N} \vDash \varphi_{i_0}(\underline{j}, y/n)$ αφού το ψηφίο $\underline{n}$ ερμηνεύεται στη $\mathfrak{N}$ ως $n \in \mathbb{N}$.

[2] Παρατηρήστε ότι αφού $P \vdash \neg\forall y\ \neg\varphi_{i_0}(\underline{j}, y)$ και το P έχει υποτεθεί συνεπές δεν μπορεί να ισχύει παράλληλα ότι $P \vdash \forall y\ \neg\varphi_{i_0}(\underline{j}, y)$.

[2] Αν δεν είναι συνεπές τότε προφανώς είναι τυπικά πλήρες: Αφού θα μπορούμε να αποδείξουμε έναν τύπο και την άρνησή του θα μπορούμε να αποδείξουμε μία αντίφαση και ως συνέπεια θα μπορούμε να αποδείξουμε όλους τους λογικούς τύπους.

αυτό το ερώτημα ο Kurt Gödel έδωσε (πάλι) μία «δυσάρεστη» απάντηση για τους μαθηματικούς. Το $2^ο$ *Θεώρημα Μη-πληρότητας* δείχνει ότι δεν μπορεί να αποδειχθεί από το P η συνέπειά του. Αυτό σημαίνει ότι δεν μπορούμε (με στοιχειώδεις μεθόδους) να αποδείξουμε τη συνέπεια του P.

Ασκήσεις

7.1 (★☆☆). Αποδείξτε τυπικά ότι αν $L \in \mathsf{RE}$, υπάρχει TM R με $L(R) = L$ που «χρησιμοποιεί» στον υπολογισμό της την $\langle R \rangle$. Θα σας φανεί χρήσιμος ο Ορισμός 1.2.19, η Πρόταση 1.2.39 και το Πόρισμα 7.2.3.

7.2 (★☆☆). Βρείτε δύο διαφορετικές TM M και N τέτοιες ώστε για κάθε $x \in \{0,1\}^*$ να ισχύει ότι $\phi_M(x) = \langle N \rangle$ και $\phi_N(x) = \langle M \rangle$.

7.3 (★★☆). Θεωρήστε τη γλώσσα:

$$L = \{\langle M \rangle \in \{0,1\}^* \quad | \quad \text{Για κάθε Τ.Μ. } M' \text{ ισχύει ότι αν } L(M) = L(M') \\ \text{τότε } |\langle M \rangle| \leq |\langle M' \rangle|\}$$

Δείξτε ότι δεν υπάρχει άπειρο αναδρομικά απαριθμήσιμο υποσύνολο της L.

7.4 (★★☆). Μια TM M ονομάζεται *ελαχιστική* αν κάθε TM M' με $L(M') = L(M)$ έχει περισσότερες καταστάσεις από την M (θεωρούμε χωρίς βλάβη της γενικότητας ότι όλες οι TM έχουν ως αλφάβητο ταινίας το $\{\triangleright, \sqcup, 0, 1\}$). Υπάρχει άπειρο, Αναδρομικά Απαριθμήσιμο σύνολο κωδικοποιήσεων ελαχιστικών TM;

7.5 (★☆☆). Έστω $d(x)$ η βραχύτερη λέξη της μορφής $\langle M, w \rangle$ όπου η TM M με είσοδο w τερματίζει γράφοντας x στην ταινία της. Δείξτε ότι η συνάρτηση $K : \{0,1\}^* \to \mathbb{N}$, με $K(x) = |d(x)|$, δεν είναι υπολογίσιμη.

7.6 (★★★). Υπάρχει 1-1 και επί, πλήρης υπολογίσιμος μετασχηματισμός TM $t : \mathbb{N} \to \mathbb{N}$ για τον οποίο δεν υπάρχει $i \in \mathbb{N}$ τέτοιο ώστε $\phi_{t(i)} = \phi_{t(i+1)} = \phi_{t(i+2)}$;

7.7 (★★☆). Έστω υπολογίσιμη συνάρτηση $h : \mathbb{N}^2 \to \mathbb{N}$ και $q \in \mathbb{N}$. Δείξτε χρησιμοποιώντας το Θεώρημα 7.3.6 ότι υπάρχει συνάρτηση που ορίζεται μέσω της αναδρομικής εξίσωσης:

$$\begin{cases} f(0) = q \\ f(y+1) = \mathsf{h}(f(y), y) \end{cases}$$

που είναι υπολογίσιμη.

7.8 (★★★). Αποδείξτε το Θεώρημα 7.3.4 χωρίς να χρησιμοποιήσετε το Θεώρημα 7.2.1.

7.9 (★☆☆). Αποδείξτε το Θεώρημα 7.1.2 χρησιμοποιώντας το Θεώρημα 7.3.4.

7.10 (★★☆). Αποδείξτε το Θεώρημα 7.2.1 χρησιμοποιώντας το Θεώρημα 7.3.4.

ΚΕΦΑΛΑΙΟ 8

ΑΡΙΘΜΗΤΙΚΗ ΙΕΡΑΡΧΙΑ

Η απάντηση των ερωτημάτων της Σελίδας 28 μας έδειξε ότι υπάρχουν γλώσσες (ή προβλήματα αν προτιμάτε) τριών κατηγοριών: οι αναδρομικές, οι αναδρομικά απαριθμήσιμες και οι άλλες. Το «οι άλλες» προφανώς δεν μπορεί γίνει ανεκτό σε ένα επιστημονικό κείμενο. Η περιέργειά μας αναπόφευκτα καλλιεργεί την ανάγκη να κατατάξουμε *όλες* [1] τις γλώσσες ως προς τον «βαθμό δυσκολίας» τους. Ας καταπιαστούμε λοιπόν με αυτό το εγχείρημα.

Υπό ποία έννοια «δυσκολίας» όμως θα γίνει αυτή η κατάταξη; Η δυσκολία στο να αποφασίσουμε μία γλώσσα (ή να υπολογίσουμε μία συνάρτηση) δεν θα οφείλεται στο πλήθος των υπολογιστικών πόρων που θα χρειαστεί να δαπανήσουμε προς αυτό, όπως γίνεται π.χ. στη Θεωρία της Υπολογιστικής Πολυπλοκότητας (ούτως ή άλλως έχουμε αποφασίσει ότι έχουμε στη διάθεσή μας οσοδήποτε μεγάλους αλλά πεπερασμένους πόρους). Εμάς μας ενδιαφέρει πόσο «ισχυρές» παραδοχές θα χρειαστεί να κάνουμε για να αποφασίσουμε τη γλώσσα. Για τον λόγο αυτό θα εισάγουμε τον λεγόμενο *σχετικό υπολογισμό*, τον υπολογισμό δηλαδή που εξαρτάται από κάποιες (κατά κανόνα πολύ ισχυρές) παραδοχές.

8.1 Σχετικός υπολογισμός

Θα θέσουμε δύο ακόμα υποθετικά ερωτήματα τα οποία θα προσπαθήσουμε να απαντήσουμε:

> **Ερώτημα 3:** Ας κάνουμε την υπόθεση εργασίας ότι η γλώσσα HP (που άνοιξε τον ασκό του Αιόλου) είναι αναδρομική γλώσσα. Είναι τότε και κάθε άλλη γλώσσα αναδρομική ή έστω αναδρομικά απαριθμήσιμη [2];

[1] Δυστυχώς –στα πλαίσια αυτών των σημειώσεων– δεν θα μπορέσουμε να καθορίσουμε τη δυσκολία όλων των γλωσσών. Η μελέτη μας σταματάει σε μία γλώσσα την οποία αδυνατούμε μέσω της θεωρία που θα αναπτύξουμε να την κατατάξουμε σε κάποια κλάση δυσκολίας. Ο φιλομαθής αναγνώστης θα χρειαστεί να συνεχίσει την αναζήτησή του στο πεδίο της *Περιγραφικής Συνολοθεωρίας*.

[2] Προσοχή! Δεν θα δεχθούμε σαν αληθή πρόταση μία αντίφαση γιατί τότε όλες οι προτάσεις θα ήταν αληθείς. Το ερώτημα θα γίνει πιο ξεκάθαρο στη συνέχεια.

Μιλώντας πιο χαλαρά, το ερώτημα θα διατυπωνόταν ως εξής: *Αν ξέραμε για ποιες εισόδους τερματίζει μία ΤΜ και για ποιες όχι θα μπορούσαμε να αποφασίσουμε όλες τις γλώσσες, ή έστω να τις αναγνωρίσουμε;*Ένα πιο γενικό ερώτημα είναι το εξής:

Ερώτημα 4: Είναι όλες οι γλώσσες στο $2^{\{0,1\}^*} \setminus \mathsf{RE}$ το ίδιο «μη αποφάνσιμες»;

Προκειμένου να ορίσουμε ένα μέτρο «μη αποφανσιμότητας» θα εισάγουμε τον *σχετικό υπολογισμό*, δηλαδή τον υπολογισμό μίας συνάρτησης ή την αποφανσιμότητα μίας γλώσσας σε σχέση με κάποια άλλη συνάρτηση ή γλώσσα. Ακολουθώντας την ιδέα του σχετικού υπολογισμού, θα θεωρούμε ότι μία γλώσσα B είναι «δυσκολότερη» από μία γλώσσα A αν η (υποθετική στις περισσότερες περιπτώσεις) ύπαρξη ενός αλγόριθμου που αποφασίζει τη B μπορεί να χρησιμοποιηθεί για να αποφασίσουμε ή να αναγνωρίσουμε την A [1].

Κεντρικό ρόλο στον σχετικό υπολογισμό παίζει η έννοια του *μαντείου για μία γλώσσα* και το μοντέλο ΤΜ που μπορεί να αξιοποιήσει τους «χρησμούς» του μαντείου. Ας περάσουμε στις λεπτομέρειες αυτών των εννοιών.

Ορισμός 8.1.1. *Χρησμοδότης (ή μαντείο) για μία γλώσσα* $L \subseteq \{0,1\}^*$ είναι μία *εξωτερική μηχανή* (όχι ΤΜ) που δέχεται σαν είσοδο μία λέξη $w \in \{0,1\}^*$ και επιστέφει 1 αν $w \in L$ και 0 αν $w \notin L$.

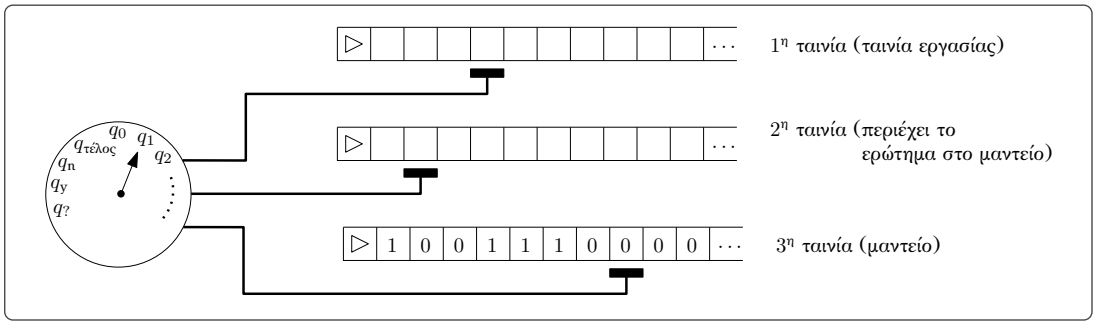
Ο παραπάνω Ορισμός είναι ο συνηθέστερος στη βιβλιογραφία. Για να μπορέσουμε να συνδέσουμε το ασαφές «εξωτερική μηχανή» με τις αυστηρά ορισμένες ΤΜ οφείλουμε να ορίσουμε τα μαντεία με πιο τυπικό τρόπο. Θα θεωρήσουμε λοιπόν ως μαντείο για τη γλώσσα $L \subseteq \{0,1\}^*$ μία άπειρη ταινία (από τα δεξιά) που περιέχει τη χαρακτηριστική συνάρτηση της L. Πιο συγκεκριμένα, τα κελιά αυτής της ταινίας αντιστοιχούν στις λέξεις του $\{0,1\}^*$ (το αριστερότερο αντιστοιχεί στην ϵ και τα υπόλοιπα ακολουθούν τη λεξικογραφική διάταξη του $\{0,1\}^*$) και αναγράφουν 1 αν η λέξη του κελιού ανήκει στη γλώσσα και 0 αν δεν ανήκει. Σύμφωνα με αυτήν τη σύμβαση μπορούμε να ορίσουμε ΤΜ που χρησιμοποιούν μαντεία ως εξής:

Ορισμός 8.1.2. Έστω γλώσσα $L \subseteq \{0,1\}^*$. *Χρησμοληπτική ΤΜ ως προς την* L *(ή ΤΜ με μαντείο για την* L *ή, εν συντομία, ΟΤΜ)* είναι μία ΤΜ $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{τέλος}})$ τριών ταινιών, όπου η 3^{η} ταινία είναι το μαντείο για την L (δες Σχήμα 8.1.1). Επιπλέον το Q περιέχει τρεις ειδικές, μη τερματικές καταστάσεις, τις $q_?$, q_{y} και q_{n}, οι οποίες σταματούν την κανονική ροή του υπολογισμού και ξεκινούν τη διαδικασία «ερώτησης» προς το μαντείο. Η M όταν μεταβαίνει στην $q_?$ κάνει τα ακόλουθα:

1. Υπολογίζει τη σειρά στη λεξικογραφική διάταξη της λέξης που περιέχει η 2^{η} ταινία, έστω ότι είναι η i-οστή λέξη,

2. κινεί την κεφαλή της $3^{\eta\varsigma}$ ταινίας στο κελί i και διαβάζει το περιεχόμενό του. Αν αυτό είναι 1 μεταβαίνει στην κατάσταση q_{y} και αν αυτό είναι 0 στην κατάσταση q_{n}.

[1] Κάτι αντίστοιχο είχαμε κάνει και στο Κεφάλαιο 5 με τις απεικονιστικές αναγωγές. Στην Παράγραφο 8.3 θα γίνει αυτή η συσχέτιση και θα δούμε τις διαφορές που υπάρχουν.



Σχήμα 8.1.1: *Σχηματική αναπαράσταση μίας OTM.*

Έχοντας πάρει θετική ή αρνητική απάντηση από το μαντείο ο υπολογισμός συνεχίζει κατά τα γνωστά [1].

Παρατήρηση 8.1.3. Κατ' αντιστοιχία με τον Ορισμό 1.2.23, μπορούμε να ορίσουμε τις χρησμοληπτικές TM με δύο τερματικές καταστάσεις (τις $q_{\text{ναι}}$ και $q_{\text{όχι}}$), αν το ενδιαφέρον μας στρέφεται προς την αποφανσιμότητα γλωσσών.

Δεν θα ήταν παράλογο κάποιος να ενίσταται στην ύπαρξη OTM. Το πρόβλημα φυσικά είναι ότι το μαντείο μπορεί να είναι οποιαδήποτε γλώσσα (ακόμα και μία γλώσσα που δεν ανήκει στο RE) και η χαρακτηριστική συνάρτηση αυτής της γλώσσας μπορεί να μην είναι υπολογίσιμη. Τα δύο σημεία που θα πρέπει να αναλογιστούμε για να ξεπεράσουμε αυτήν την ανασφάλεια είναι, πρώτον, ότι μία OTM είναι μια καθ' όλα νόμιμη TM με τρεις ταινίες (το μαντείο είναι μια «εξωτερική μηχανή» και όχι κάποια υπορουτίνα της), και κανένας φαντάζομαι δεν αμφισβητεί την ύπαρξη 3-ταινιακών TM. Η δεύτερη και πιο σημαντική σκέψη (που πάντα θα πρέπει να μένει στο πίσω μέρος του μυαλού μας σε αυτό το κεφάλαιο) είναι ότι μελετάμε τον σχετικό υπολογισμό, αναπτύσσουμε δηλαδή μία θεωρία βασισμένη σε υποθέσεις. Για παράδειγμα μπορεί να χρειαστεί να υποθέσουμε ότι η χαρακτηριστική συνάρτηση της HP είναι υπολογίσιμη και έτσι υπάρχει μαντείο για αυτήν [2]. Οπότε, συνοψίζοντας, η απάντηση είναι *ναι* υπάρχουν OTM και, όσον αφορά τα μαντεία τους, δεχόμαστε σαν υπόθεση εργασίας ότι η χαρακτηριστική συνάρτησή τους είναι υπολογίσιμη και μελετάμε τις συνέπειες αυτής της παραδοχής.

Συμβολισμός 8.1.4. Έστω OTM $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{τέλος}})$ και γλώσσα $L \subseteq \{0,1\}^*$. Θα γράφουμε M^L όταν θέλουμε να τονίσουμε το μαντείο το οποίο προτιθέμεθα να χρησιμοποιούμε για την M.

[1] Ο υπολογισμός ναι μεν διεξάγεται «κατά τα γνωστά» αλλά η γνώση που αποκομίσαμε από το μαντείο κάνει τις OTM πολύ πιο «ισχυρές» από τις TM (τυπικά δεν μπορούμε να συγκρίνουμε τη δύναμη αυτών των δύο υπολογιστικών μοντέλων όπως εξηγεί η Παρατήρηση 8.1.15). Ο λόγος φυσικά είναι ότι με το μαντείο μπορούμε να γνωρίζουμε αν μία λέξη ανήκει σε μία γλώσσα ή όχι, ακόμα και για γλώσσες που είναι μη αποφάνσιμες, για τις οποίες δηλαδή δεν θα μπορούσαμε να αποκτήσουμε αυτήν τη γνώση με κάποιον υπολογιστικό τρόπο.

[2] Είναι νομίζω εμφανές ότι δεν μας χρειάζεται η a priori γνώση όλης της χαρακτηριστικής συνάρτησης της γλώσσας μαντείου. Μας χρειάζεται μόνο η τιμή της για το εκάστοτε ερώτημα προς το μαντείο την κάθε φορά.

Στη συνέχεια θα γίνει αντιληπτό ότι ανάλογα με το μαντείο που χρησιμοποιεί η M θα αλλάξει (συνήθως ριζικά) και η «συμπεριφορά» της. Έτσι, όταν μας ενδιαφέρει η συμπεριφορά της σε σχέση με τη γλώσσα L θα την τρέχουμε με αυτήν την γλώσσα ως μαντείο.

Ορισμός 8.1.5. Έστω γλώσσα $A \subseteq \{0,1\}^*$ και συνάρτηση $f : \{0,1\}^* \to \{0,1\}^*$. Μία ΟΤΜ M που χρησιμοποιεί μαντείο για την A *υπολογίζει* την f ανν:

$$\forall w \in \mathsf{dom}(f)(\triangleright\, q_0 w \vdash^*_{M^A} \triangleright\, q_{\text{τέλος}} f(w)) \text{ και } \forall w \notin \mathsf{dom}(f)(M^A(w)\uparrow)$$

Ορισμός 8.1.6. Έστω γλώσσα $A \subseteq \{0,1\}^*$ και συνάρτηση $f : \{0,1\}^* \to \{0,1\}^*$. Αν υπάρχει ΟΤΜ M που υπολογίζει την f αν χρησιμοποιήσουμε μαντείο για την A θα λέμε ότι η f είναι *υπολογίσιμη ως προς την A*.

Ορισμός 8.1.7. Έστω γλώσσες $A, B \subseteq \{0,1\}^*$. Μία ΟΤΜ M που χρησιμοποιεί μαντείο για την A *αναγνωρίζει* (ή *ημι-αποφασίζει*) την B ανν:

(A) $w \in B \Leftrightarrow M^A(w)\downarrow_{q_{\text{ναι}}}$

Ορισμός 8.1.8. Έστω γλώσσες $A, B \subseteq \{0,1\}^*$. Αν υπάρχει ΟΤΜ M που ημι-αποφασίζει την B αν χρησιμοποιήσουμε μαντείο για την A θα λέμε ότι η B είναι *αναδρομικά απαριθμήσιμη ως προς την A*.

Ορισμός 8.1.9. Έστω γλώσσες $A, B \subseteq \{0,1\}^*$. Μία ΟΤΜ M που χρησιμοποιεί μαντείο για την A *αποφασίζει* την B ανν:

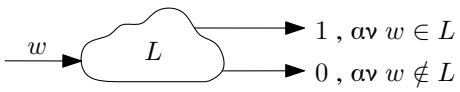
(A) $w \in B \Leftrightarrow M^A(w)\downarrow_{q_{\text{ναι}}}$

(B) $w \notin B \Leftrightarrow M^A(w)\downarrow_{q_{\text{όχι}}}$

Ορισμός 8.1.10. Έστω γλώσσες $A, B \subseteq \{0,1\}^*$. Αν υπάρχει ΟΤΜ M που αποφασίζει την B αν χρησιμοποιήσουμε μαντείο για την A θα λέμε ότι η B είναι *αναδρομική ως προς την A*.

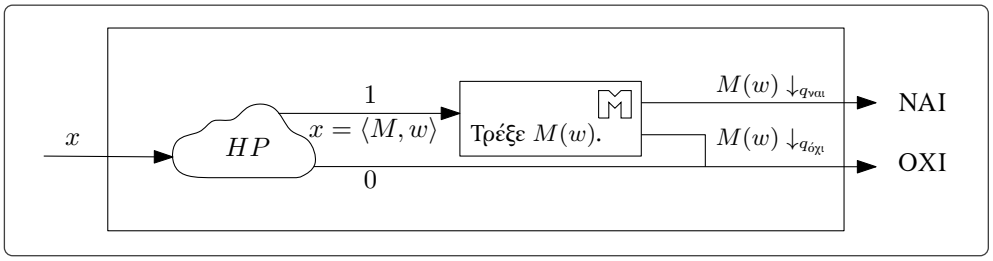
Συμβολισμός 8.1.11 (Κουτάκια συνέχεια...).

9. Θα συμβολίζουμε το μαντείο για τη γλώσσα $L \subseteq \{0,1\}^*$ ως εξής:



(Στην απεικονιζόμενη περίπτωση γίνεται ερώτημα στο μαντείο για τη λέξη w.)

Παράδειγμα 8.1.12. Η $L_{\text{Αποδοχής}}$ είναι αναδρομική ως προς την HP καθώς η ΟΤΜ του Σχήματος 8.1.2 την αποφασίζει.



Σχήμα 8.1.2: *Η ΟΤΜ που αποφασίζει την* $L_{\text{Αποδοχής}}$.

Παρατήρηση 8.1.13. Παρατηρήστε ότι αν είχαμε εφοδιάσει την ΟΤΜ του παραπάνω παραδείγματος με μαντείο για τη $\overline{HP}$ (αντί για το μαντείο για την HP), τότε θα αποφάσιζε την κενή γλώσσα [1]. Ακόμα και αν η ΟΤΜ αποφασίζει (ημι-αποφασίζει) μία συγκεκριμένη γλώσσα (ή υπολογίζει μία συγκεκριμένη συνάρτηση), αν το μαντείο αλλάξει τότε αλλάζει και η γλώσσα που αποφασίζει (ημι-αποφασίζει, ή η συνάρτηση που υπολογίζει). Μπορούμε να αντιστοιχήσουμε σε μία ΟΤΜ μία γλώσσα (ή μία συνάρτηση) μόνο *εν σχέσει* με τη γλώσσα που χρησιμοποιούμε ως μαντείο [2].

Συμβολισμός 8.1.14. Έστω ΟΤΜ $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{τέλος}})$ και γλώσσα $L \subseteq \{0,1\}^*$. Χάριν συντομίας σε όσα ακολουθούν θα γράφουμε «υπάρχει ΟΤΜ M^L...» αντί για την πρόταση «υπάρχει ΟΤΜ M που αν χρησιμοποιήσουμε ως μαντείο την L ...».

Παρατήρηση 8.1.15. Οι ΟΤΜ είναι επέκταση των ΤΜ. Θα μπορούσαμε να το φανταστούμε αυτό ως εξής: Μία ΤΜ θεωρείται ΟΤΜ που δεν χρησιμοποιεί ποτέ το μαντείο της [3]. Η επέκταση αυτή, σε αντίθεση με τις επεκτάσεις που είδαμε στην Παράγραφο 1.3, δείχνει (εσφαλμένα) ισχυρότερη από τις ΤΜ [4], καθώς για παράδειγμα η ΟΤΜ του Παραδείγματος 8.1.12 αποφασίζει μία μη αναδρομική γλώσσα. Εδώ όμως έχουμε να κάνουμε με σχετικό υπολογισμό (καθώς κάνουμε την παραδοχή ότι μπορούμε να γνωρίζουμε αν μια λέξη ανήκει στην HP ή όχι) και όχι με απόλυτο υπολογισμό (όπου δεν κάνουμε καμία παραδοχή).

Ένας πιο τυπικός τρόπος να δούμε ότι οι ΟΤΜ είναι επέκταση των ΤΜ, ή, σωστότερα, ότι οι ΤΜ είναι περιορισμός των ΟΤΜ, δίνεται στη Σύμβαση 8.1.16.

Σύμβαση 8.1.16. Για λόγους «συμβατότητας» θα θεωρήσουμε ότι μία ΤΜ $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{τέλος}})$ είναι μία ΟΤΜ στην οποία έχουμε θέσει τον ακόλουθο έξτρα περιορισμό για τη συνάρτηση μετάβασης:

$$\forall a, b \in \Gamma \ \forall q, p \in Q \ \forall x \in \{\text{A}, \Delta\}(\delta(q, a) = (p, b, x) \to p \neq q_?) \tag{8.1}$$

[1] Εδώ υποθέτουμε ότι αν δώσουμε στην καθολική ΤΜ ως είσοδο λέξη που δεν αποτελεί κωδικοποίηση ΤΜ και λέξης, αυτή θα κολλήσει.

[2] Θυμηθείτε ότι έως τώρα σε κάθε ΤΜ αντιστοιχούσαμε ακριβώς μία συνάρτηση και ακριβώς μία γλώσσα. Στον σχετικό υπολογισμό αυτό γενικά δεν ισχύει. Ισχύει μόνο όταν δηλώσουμε ρητά το μαντείο που θα χρησιμοποιήσουμε στην ΟΤΜ. Υπό μία έννοια ο σχετικός υπολογισμός ταυτίζεται με τον υπολογισμό που μελετούσαμε έως τώρα αν επικεντρωθούμε σε μία συγκεκριμένη γλώσσα μαντείου. Φυσικά η χρήση μαντείου μας οδηγεί σε αποτελέσματα που είναι αντίθετα με αυτά που θεωρούσαμε αλγοριθμικά εφικτά.

[3] Έχει φυσικά τη δυνατότητα να το χρησιμοποιήσει, απλά δεν το κάνει.

[4] Πράγμα που θα κλόνιζε την εμπιστοσύνη μας στη Θέση Church-Turing!

δηλαδή, κατά τη λειτουργία της δεν μεταβαίνουν ποτέ στην κατάσταση $q_?$.

Η παραπάνω σύμβαση μας δίνει εν ολίγης το δικαίωμα να τρέχουμε τις ΟΤΜ που ικανοποιούν την προϋπόθεση (8.1) «χωρίς να χρησιμοποιούμε μαντείο» [1], όπως δηλαδή κάναμε έως τώρα.

Συνδυάζοντας τη Σύμβαση 8.1.16 με τους Ορισμούς 1.2.28 και 1.2.29 οδηγούμαστε στην ακόλουθη παρατήρηση.

Παρατήρηση 8.1.17. *Μία γλώσσα $L \subseteq \{0,1\}^*$ είναι αναδρομική (ή αναδρομικά απαριθμήσιμη) ανν υπάρχει ΟΤΜ που την αποφασίζει (ημι-αποφασίζει αντίστοιχα) ασχέτως με ποια γλώσσα θα χρησιμοποιήσουμε ως μαντείο. Επομένως, οι κλάσεις* REC *και* RE *αφορούν απόλυτο υπολογισμό* [2].

Χρησμοληπτική Καθολική Μηχανή Turing

Στην Παράγραφο 1.4 κωδικοποιήσαμε τη συνάρτηση μεταβάσεων μίας ΤΜ στο $\{0,1\}$, με απώτερο σκοπό να ορίσουμε την καθολική ΤΜ. Η καθολική ΤΜ μπορεί να δεχθεί σαν είσοδο την κωδικοποίηση μίας ΤΜ και μίας λέξης και να προσομοιώσει τη λειτουργία της με είσοδο αυτήν τη λέξη. Όσον αφορά τις ΟΤΜ δεν έχουμε πολλά να προσθέσουμε ως προς την κωδικοποίησή τους, καθώς τις ορίσαμε σαν ΤΜ 3-ταινιών και (όπως στις ΤΜ δεν κωδικοποιούσαμε το περιεχόμενο της ταινίας, έτσι και για τις ΟΤΜ) κωδικοποιούμε μόνο τη συνάρτηση μετάβασης (και όχι την «προβληματική» ταινία του μαντείου). Αυτό που θέλει προσοχή είναι το εξής: Δεν θα ήταν σωστό να πάρουμε πρώτα ισοδύναμη μονοταινιακή ΤΜ και έπειτα να κωδικοποιήσουμε αυτήν. Ο λόγος είναι ότι σε μία μονοταινιακή ΟΤΜ θα έπρεπε κάπως να «τοποθετήσουμε» την ταινία του μαντείου στη μοναδική ταινία της (κάτι αντίστοιχο με την απόδειξη του Θεωρήματος 1.3.3) ή, έστω, να χρησιμοποιούμε τη χαρακτηριστική συνάρτηση της γλώσσας μαντείου σαν υπορουτίνα! Αντ' αυτού, κωδικοποιούμε κατευθείαν τη συνάρτηση μεταβάσεων όπως στην Παράγραφο 1.4, μόνο που θα αλλάξουμε τις κωδικοποιήσεις των μεταβάσεων καθώς τώρα έχουμε τρεις ταινίες [3]. Μετά από αυτήν τη διευκρίνιση. μπορούμε πλέον να περάσουμε στον ορισμό της *Χρησμοληπτικής Καθολικής ΤΜ*.

Ορισμός 8.1.18. Έστω γλώσσα $L \subseteq \{0,1\}^*$. *Χρησμοληπτική Καθολική ΤΜ ως προς την L*, συμβολισμός $\mathbb{M}^L$, είναι μία ΟΤΜ που δέχεται ως είσοδο την κωδικοποίηση μίας ΟΤΜ M και μίας λέξης w και μπορεί να προσομοιώσει την $M(w)$ με τον ίδιο τρόπο όπως μία (απλή) Καθολική ΤΜ (δες Ορισμό 1.4.14), μόνο που χρησιμοποιεί το μαντείο για την L όποτε η προσομοίωση της $M(w)$ πηγαίνει στην κατάσταση $q_?$.

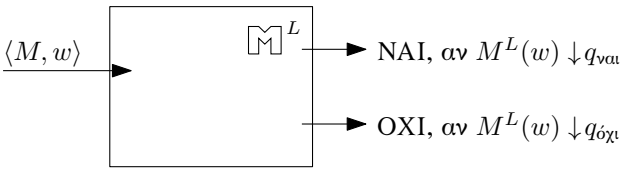
Συμβολισμός 8.1.19 (Κουτάκια συνέχεια...).

[1] Αν το κάναμε αυτό σε μία ΟΤΜ που δεν ικανοποιεί την (8.1) τότε αυτή θα κόλλαγε όταν έφτανε στην κατάσταση $q_?$ καθώς θα περίμενε για πάντα έναν «χρησμό».

[2] Η Σύμβαση 8.1.16 δεν είναι απαραίτητη για να ισχύει αυτή η παρατήρηση (δες Άσκηση 8.2).

[3] Στην ταινία του μαντείου θα χρειαστεί να κάνουμε σε κάθε βήμα υπολογισμού και μία άσκοπη κίνηση της κεφαλής.

10. Έστω γλώσσα $L \subseteq \{0,1\}^*$, ΟΤΜ M και $w \in \{0,1\}^*$. Θα γράφουμε: [1]



Παρατηρήστε ότι ανάλογα με το μαντείο που χρησιμοποιεί η καθολική ΟΤΜ μπορεί να αποδεχθεί ή να απορρίψει την είσοδό της. Για παράδειγμα αν προσομοιώσουμε την ΟΤΜ του Παραδείγματος 8.1.12 με είσοδο $\langle M, w\rangle \in L_{\text{Αποδοχής}}$, χρησιμοποιώντας για μαντείο την HP, η καθολική ΟΤΜ θα αποδεχθεί την είσοδο, ενώ αν χρησιμοποιήσουμε για μαντείο τη $\overline{HP}$ θα απορρίψει την είσοδο.

Κλάσεις σχετικού υπολογισμού

Ορισμός 8.1.20. Έστω γλώσσα $A \subseteq \{0,1\}^*$. Ορίζουμε τις ακόλουθες *κλάσεις γλωσσών ως προς την* A:

- $\mathsf{RE}^A = \{L \subseteq \{0,1\}^* \mid$ υπάρχει ΟΤΜ M^A που ημι-αποφασίζει την $L\}$
- $\mathsf{REC}^A = \{L \subseteq \{0,1\}^* \mid$ υπάρχει ΟΤΜ M^A που αποφασίζει την $L\}$

Θεώρημα 8.1.21. Έστω γλώσσα $A \subseteq \{0,1\}^*$. Αν $A \in \mathsf{REC}$ τότε $\mathsf{RE}^A = \mathsf{RE}$ και $\mathsf{REC}^A = \mathsf{REC}$.

Απόδειξη. [2] Έστω M_A η ΤΜ που αποφασίζει την A και έστω γλώσσα $L \in \mathsf{RE}^A$, δηλαδή υπάρχει ΟΤΜ M_L^A που την ημι-αποφασίζει. «Αντικαθιστούμε» το μαντείο για την A με την M_A στην M_L^A και παίρνουμε ΤΜ M ως εξής:

> *Η M προσομοιώνει με μία (απλή) καθολική ΤΜ την M_L^A. Όταν η M_L^A «ρωτάει» το μαντείο για μία λέξη w η M τρέχει την M_A με είσοδο w και αν αυτή αποδεχτεί γράφει 1 στην τρίτη ταινία (την ταινία του μαντείου) στο κελί $|w|+1$, ενώ αν απορρίψει γράφει 0* [3].

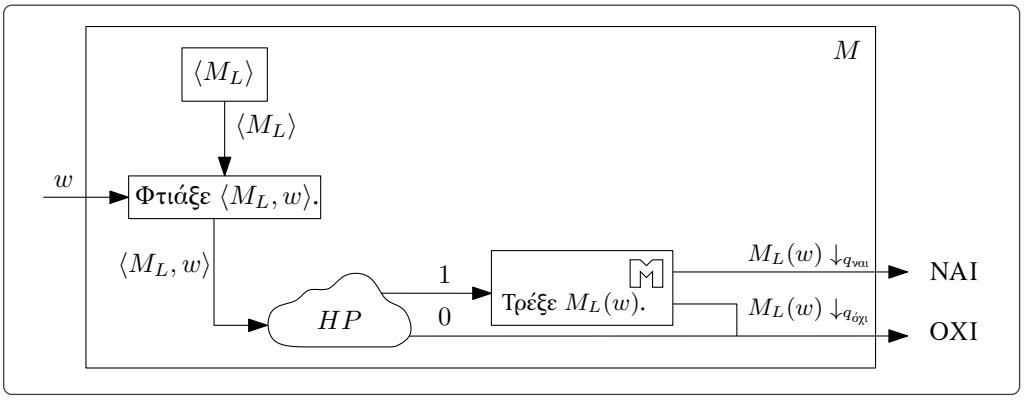
Κατά αυτόν τον τρόπο μπορούμε να «ξεγελάσουμε» την M_L^A και να λειτουργεί όπως θα έκανε αν χρησιμοποιούσε μαντείο για την A, αλλά στην ουσία τους «χρησμούς» τους υπολογίζουμε χρησιμοποιώντας την M_A [4].Έτσι κατασκευάσαμε μία ΤΜ M που ημι-αποφασίζει την L και άρα $L \in \mathsf{RE}$. Συνεπώς $\mathsf{RE}^A \subseteq \mathsf{RE}$.

[1] Γράφουμε $\boxed{M}^L$ αντί για $\boxed{M}$ θέλοντας να τονίσουμε το μαντείο που προτιθέμεθα να χρησιμοποιήσουμε στην προσομοίωση. Μην παρεξηγηθεί αυτός ο συμβολισμός και θεωρηθεί ότι η γλώσσα L έχει συγκεκριμενοποιηθεί. Ανάλογα με τον σκοπό που χρησιμοποιούμε τη χρησμοληπτική καθολική μηχανή η γλώσσα μαντείο μπορεί να αλλάξει.

[2] Θα δείξουμε μόνο την πρώτη περίπτωση. Η δεύτερη είναι εντελώς αντίστοιχη.

[3] Η ταινία του μαντείου δεν χρειάζεται να περιέχει ολόκληρη τη χ_A. Αρκεί τα κελιά που αντιστοιχούν στις λέξεις για τις οποίες γίνεται το κάθε ερώτημα να περιέχουν τη σωστή τιμή.

[4] Τυπικά, για να συμμορφωθούμε απόλυτα με τη Σύμβαση 8.1.16, θα πρέπει να παρακάμψουμε την κατάσταση $q_?$ της M_L^A έτσι ώστε η ΤΜ που κατασκευάζουμε να μην μεταβαίνει ποτέ σε αυτήν.



Σχήμα 8.1.3: *Η ΟΤΜ M στην απόδειξη της Πρότασης 8.1.22.*

Έστω τώρα γλώσσα $L \in \mathsf{RE}$ και ΤΜ M_L που την ημι-αποφασίζει. Από τη Σύμβαση 8.1.16 προκύπτει ότι η M_L αποτελεί ΟΤΜ που δεν «ρωτάει» ποτέ το μαντείο. Συνεπώς $L \in \mathsf{RE}^A$ και έτσι $\mathsf{RE} \subseteq \mathsf{RE}^A$. □

Σύμφωνα με το Θεώρημα 8.1.21 η θεωρία του σχετικού υπολογισμού δεν παρουσιάζει «ενδιαφέρον» όταν χρησιμοποιούμε ως μαντείο μία αναδρομική γλώσσα. Ας δούμε λοιπόν τι συμβαίνει όταν χρησιμοποιήσουμε μια αναδρομικά απαριθμήσιμη γλώσσα $A \subseteq \{0,1\}^*$ που δεν είναι αναδρομική. Από το δεύτερο σκέλος της απόδειξης του Θεωρήματος 8.1.21 προκύπτει ότι $\mathsf{RE} \subseteq \mathsf{RE}^A$. Για μερικές γλώσσες-μαντεία ισχύει ότι $\mathsf{RE} \subseteq \mathsf{REC}^A$, όπως για παράδειγμα την HP.

Πρόταση 8.1.22. Ισχύει ότι $\mathsf{RE} \subseteq \mathsf{REC}^{HP}$.

Απόδειξη. Έστω γλώσσα $L \in \mathsf{RE}$ και έστω M_L η ΤΜ που την ημι-αποφασίζει. Παρατηρούμε ότι η ΟΤΜ M του Σχήματος 8.1.3 αποφασίζει την L, άρα $L \in \mathsf{REC}^{HP}$. □

Συνεπώς η απάντηση στο Ερώτημα 3 (σελίδα 157) είναι καταφατική, αλλά μόνο όσον αφορά τις αναδρομικά απαριθμήσιμες γλώσσες:

Πρόταση 8.1.23. Υπάρχει γλώσσα $L \subseteq \{0,1\}^*$ που δεν ανήκει στο REC^{HP}.

Απόδειξη. Θεωρούμε τη γλώσσα:

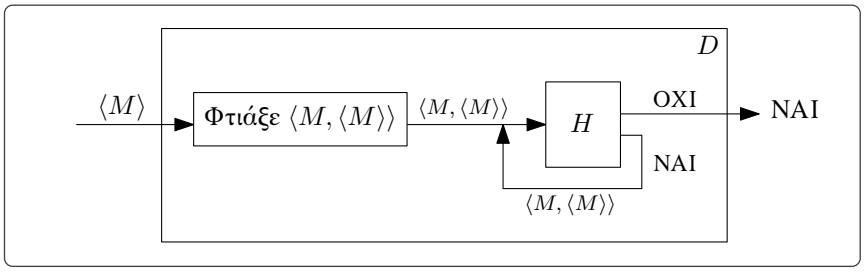
$$HP_2 = \{\langle M, w\rangle \in \{0,1\}^* \mid M^{HP}(w)\downarrow\}\ ^1$$

Θα δείξουμε ότι $HP_2 \notin \mathsf{REC}^{HP}$. Έστω (προς άτοπο) ότι $HP_2 \in \mathsf{REC}^{HP}$ και έστω ότι η ΟΤΜ H^{HP} την αποφασίζει. Θεωρούμε την ΟΤΜ D του Σχήματος 8.1.4 και παρατηρούμε ότι:

$$D^{HP}(\langle D\rangle)\downarrow \Leftrightarrow H^{HP}(\langle D, \langle D\rangle\rangle)\downarrow_{q_{\text{όχι}}} \Leftrightarrow \langle D, \langle D\rangle\rangle \notin HP_2 \Leftrightarrow D^{HP}(\langle D\rangle)\uparrow$$

Άτοπο, άρα $HP_2 \notin \mathsf{REC}^{HP}$. □

[1] Το «2» στο HP_2 προκύπτει από τον Ορισμό 8.2.4 που ακολουθεί.



Σχήμα 8.1.4: *Η OTM D στην απόδειξη της Πρότασης 8.1.23. Παρατηρήστε ότι είναι ακριβώς ίδια με την TM στην απόδειξη του Θεωρήματος 5.2.1.*

Η Πρόταση 8.1.23 ρίχνει λίγο φως στο Ερώτημα 4: Υπάρχουν γλώσσες που ακόμα και η γνώση του πότε ο υπολογισμός μίας TM τερματίζει δεν αρκεί για να τις αποφασίσουμε. Ο «βαθμός» μη αποφανσιμότητάς τους συνεπώς οφείλει να είναι μεγαλύτερος από τον βαθμό π.χ. των γλωσσών στην κλάση RE. Αυτό ισχύει φυσικά αν πάρουμε την HP ως γλώσσα αναφοράς. Στην επόμενη παράγραφο θα προχωρήσουμε την ιδέα του σχετικού υπολογισμού ακόμα πιο πέρα, εξετάζοντας σε γενικότερο πλαίσιο τη μη αποφανσιμότητα όπου θα λαμβάνουμε ως αναφορά ολόκληρες κλάσεις γλωσσών.

Κλείνουμε αυτήν την παράγραφο αποδεικνύοντας μερικές χρήσιμες ιδιότητες των κλάσεων σχετικού υπολογισμού.

Θεώρημα 8.1.24. Έστω γλώσσα $A \subseteq \{0,1\}^*$. $L \in \mathsf{REC}^A$ ανν $\overline{L} \in \mathsf{REC}^A$.

Απόδειξη. Η απόδειξη είναι ίδια με την απόδειξη του Θεωρήματος 1.5.3, μόνο που σε αυτή την περίπτωση έχουμε OTM. □

Ορισμός 8.1.25. Εστω κλάση γλωσσών $\mathcal{C}$. Ορίζουμε την κλάση γλωσσών co-$\mathcal{C}$ $= \{L \subseteq \{0,1\}^* \mid \overline{L} \in \mathcal{C}\}$.

Θεώρημα 8.1.26. Έστω γλώσσα $A \subseteq \{0,1\}^*$. Ισχύει ότι $\mathsf{RE}^A \cap \text{co-}\mathsf{RE}^A = \mathsf{REC}^A$.

Απόδειξη. Έστω γλώσσα $L \in \mathsf{REC}^A$. Κατά ήσσονα λόγο ισχύει ότι $L \in \mathsf{RE}^A$. Από το Θεώρημα 8.1.24 προκύπτει ότι $\overline{L} \in \mathsf{REC}^A$ και αντίστοιχα ότι $\overline{L} \in \mathsf{RE}^A$. Άρα $L \in \mathsf{RE}^A \cap \text{co-}\mathsf{RE}^A$.

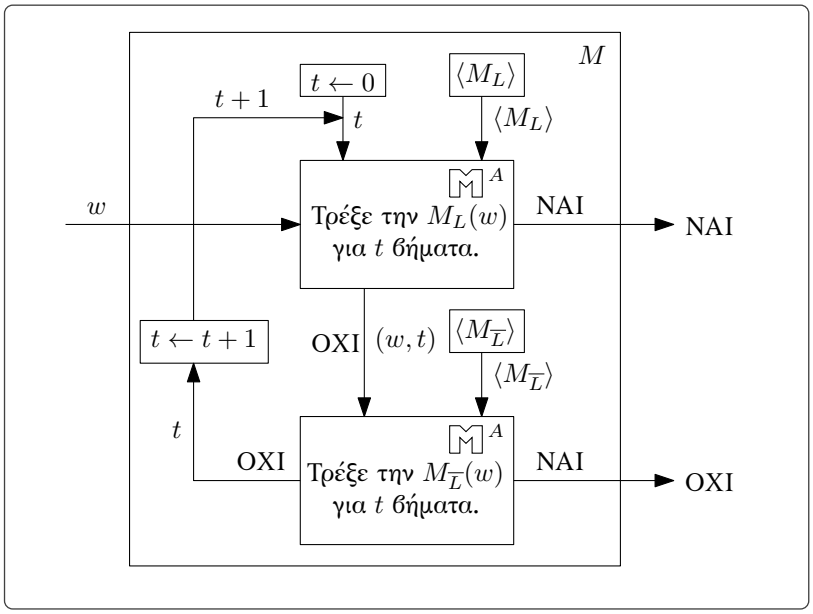
Έστω τώρα γλώσσα $L \in \mathsf{RE}^A \cap \text{co-}\mathsf{RE}^A$ δηλαδή υπάρχουν OTM M_L^A και $M_{\overline{L}}^A$ που ημιαποφασίζουν τις L και $\overline{L}$ αντίστοιχα. Κατασκευάζουμε την OTM M του Σχήματος 8.1.5 και παρατηρούμε ότι αποφασίζει την L. Άρα $L \in \mathsf{REC}^A$. □

Το ακόλουθο Θεώρημα είναι πάρα πολύ χρήσιμο καθώς μας δίνει το δικαίωμα να αλλάξουμε τη «γλώσσα αναφοράς».

Θεώρημα 8.1.27. Έστω γλώσσες $A, B, C \subseteq \{0,1\}^*$. Ισχύει ότι:

i. Αν $A \in \mathsf{RE}^B$ και $B \in \mathsf{REC}^C$ τότε $A \in \mathsf{RE}^C$.

ii. Αν $A \in \mathsf{REC}^B$ και $B \in \mathsf{REC}^C$ τότε $A \in \mathsf{REC}^C$.



Σχήμα 8.1.5: *Η TM M που αποφασίζει την L όταν $L \in \mathsf{RE}^A \cap \text{co-}\mathsf{RE}^A$ (ο λόγος που χρησιμοποιούμε τον συμβολισμό $\boxed{\mathsf{M}}^A$ αναφέρεται στην Υποσημείωση 1 στη Σελίδα 163).*

Απόδειξη. [1] i. Έστω M_A^B η TM που ημι-αποφασίζει την A και M_B^C η TM που αποφασίζει την B. Αρκεί να «αντικαταστήσουμε» το μαντείο για τη B στην M_A με την M_B (όπως κάναμε στην απόδειξη του Θεωρήματος 8.1.21). Η «αντικατάσταση» αυτή θα γίνει ως εξής:

> *Προσομοιώνουμε με μία χρησμοληπτική καθολική TM την M_A και όταν η M_A «ρωτάει» το μαντείο αν μία λέξη w ανήκει στη γλώσσα B, αντί αυτού τρέχουμε την M_B με είσοδο w.*

Έτσι παίρνουμε μία OTM που, αν χρησιμοποιήσουμε μαντείο για τη C, θα ημι-αποφασίζει την A. □

Θεώρημα 8.1.28. Έστω γλώσσες $A, B, C \subseteq \{0,1\}^*$. Αν $A \leq_m B$ και $B \in \mathsf{REC}^C$ ($B \in \mathsf{RE}^C$) τότε $A \in \mathsf{REC}^C$ ($A \in \mathsf{RE}^C$ αντίστοιχα).

Απόδειξη. Η απόδειξη είναι εντελώς αντίστοιχη με την απόδειξη του Θεωρήματος 5.2.7. □

Στο πλαίσιο του σχετικού υπολογισμού γίνεται πιο εύκολα αντιληπτό ότι η σχέση που ορίζει η αναγωγή ισχύει γενικότερα και μπορεί να χρησιμοποιηθεί για τη διερεύνηση του αν μια γλώσσα ανήκει σε πιο ευρείες κλάσεις από τις REC και RE.

[1] Θα δείξουμε μόνο το i., η απόδειξη για το ii. είναι εντελώς αντίστοιχη.

8.2 Αριθμητική Ιεραρχία

Ορισμός 8.2.1. Έστω μία κλάση γλωσσών $\mathcal{C} \subseteq 2^{\{0,1\}^*}$. Ορίζουμε τις ακόλουθες κλάσεις γλωσσών ως προς τη $\mathcal{C}$:

- $\mathsf{RE}^{\mathcal{C}} = \bigcup_{A \in \mathcal{C}} \mathsf{RE}^A$
- $\mathsf{REC}^{\mathcal{C}} = \bigcup_{A \in \mathcal{C}} \mathsf{REC}^A$

Παρατήρηση 8.2.2. Από το Θεώρημα 8.1.21 προκύπτει ότι $\mathsf{REC}^{\mathsf{REC}} = \mathsf{REC}$ και $\mathsf{RE}^{\mathsf{REC}} = \mathsf{RE}$.

Οι κλάσεις που απαρτίζουν την *Αριθμητική Ιεραρχία* δίνονται στον ακόλουθο Ορισμό.

Ορισμός 8.2.3 (Αριθμητική Ιεραρχία)**.** Ορίζουμε αναδρομικά για κάθε $n \geq 1$ τις κλάσεις γλωσσών:

$$\begin{aligned} \Sigma_1^0 &= \mathsf{RE} \\ \Delta_1^0 &= \mathsf{REC} \\ \Sigma_{n+1}^0 &= \mathsf{RE}^{\Sigma_n^0} \\ \Delta_{n+1}^0 &= \mathsf{REC}^{\Sigma_n^0} \end{aligned}$$

και τις κλάσεις γλωσσών:

$$\Pi_n^0 = \text{co-}\Sigma_n^0$$

Οι κλάσεις αυτές αποτελούν μία κατάταξη μερικών γλωσσών του $\{0,1\}^*$ ως προς τον βαθμό μη αποφανσιμότητας τους καθώς, όπως θα δούμε στο Θεώρημα 8.2.10, για κάθε $n \geq 2$ υπάρχει γλώσσα που ανήκει στην κλάση $\Sigma_{n+1}^0 \setminus \Sigma_n^0$, ή αλλιώς γλώσσα που δεν αρκεί να χρησιμοποιήσουμε μαντείο «επιπέδου» Σ_{n-1}^0 για να την ημι-αποφασίσουμε, αλλά πρέπει να χρησιμοποιήσουμε μαντείο «επιπέδου» Σ_n^0.

Προκειμένου να έχουν νόημα αυτές οι κλάσεις θα πρέπει να δείξουμε ότι οι προφανείς εγκλεισμοί είναι γνήσιοι. Το αποτέλεσμα αυτό είναι γνωστό ως *Θεώρημα Αριθμητικής Ιεραρχίας* (Θεώρημα 8.2.10) και για να το αποδείξουμε θα χρειαστεί πρώτα να κάνουμε αρκετή προεργασία.

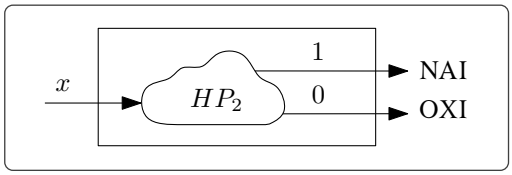
Ορισμός 8.2.4. Ορίζουμε αναδρομικά για κάθε $n \geq 1$ τις γλώσσες:

$$\begin{aligned} HP_1 &= HP \\ HP_{n+1} &= \{\langle M, w\rangle \in \{0,1\}^* \mid M^{HP_n}(w)\downarrow\} \end{aligned}$$

Πρόταση 8.2.5. Για κάθε $n \geq 1$ ισχύει ότι $HP_n \in \mathsf{REC}^{HP_{n+1}}$.

Απόδειξη. Θα το δείξουμε κάνοντας επαγωγή στο n.

Βάση: Για $n = 1$ πρέπει να δείξουμε ότι $HP \in \mathsf{REC}^{HP_2}$. Παρατηρήστε ότι μπορούμε να θεωρήσουμε ότι μία ΤΜ είναι ΟΤΜ που χρησιμοποιεί μαντείο για την HP (απλά δεν «ρωτάει» ποτέ αυτό το μαντείο, δες Σύμβαση 8.1.16). Συνεπώς η ΟΤΜ του Σχήματος 8.2.1 αποφασίζει την HP καθώς:



Σχήμα 8.2.1: *Η ΤΜ που αποφασίζει την HP χρησιμοποιώντας μαντείο για την HP_2.*

- Αν υπάρχει ΤΜ M και λέξη $w \in \{0,1\}^*$ τέτοιες ώστε $x = \langle M, w\rangle$ και το μαντείο για την HP_2 επιστρέψει 1 τότε $\langle M, w\rangle \in HP_2$, δηλαδή $M^{HP}(w)\downarrow$. Όμως θεωρούμε ότι η ΤΜ M, παρόλο που την αντιμετωπίζουμε σαν ΟΤΜ, δεν ρωτάει ποτέ το μαντείο της, συνεπώς $M(w)\downarrow$ [1]. Οπότε $x \in HP$.
- Αν είτε δεν υπάρχουν ΤΜ M και λέξη $w \in \{0,1\}^*$ τέτοιες ώστε $x = \langle M, w\rangle$, είτε υπάρχουν αλλά το μαντείο για την HP_2 επιστρέφει 0, εύκολα καταλήγουμε ότι $x \notin HP$.

Επαγωγική υπόθεση: Υποθέτουμε ότι $HP_n \in \mathsf{REC}^{HP_{n+1}}$.

Επαγωγικό βήμα: Αρκεί να δείξουμε ότι $HP_{n+1} \leq_m HP_{n+2}$ καθώς (προφανώς) ισχύει ότι $HP_{n+2} \in \mathsf{REC}^{HP_{n+2}}$ και έτσι, από το Θεώρημα 8.1.28, έπεται ότι $HP_{n+1} \in \mathsf{REC}^{HP_{n+2}}$.

Από την επαγωγική υπόθεση έχουμε ότι υπάρχει ΟΤΜ $M_{HP_n}^{HP_{n+1}}$ που αποφασίζει την HP_n. Θεωρούμε τη συνάρτηση $\phi : \{0,1\}^* \to \{0,1\}^*$ με:

$$\phi(x) = \begin{cases} \langle M_1, w\rangle & , \text{ αν υπάρχει ΟΤΜ } M \text{ και } w \in \{0,1\}^* \text{ τέτοια ώστε } x = \langle M, w\rangle \\ x & , \text{ αλλιώς} \end{cases}$$

όπου η ΟΤΜ M_1 απεικονίζεται στο Σχήμα 8.2.2, και παρατηρούμε ότι:

1. ϕ πλήρης και υπολογίσιμη.
2. $\langle M, w\rangle \in HP_{n+1} \Leftrightarrow M^{HP_n}(w)\downarrow \Leftrightarrow M_1^{HP_{n+1}}(w)\downarrow \Leftrightarrow \langle M_1, w\rangle \in HP_{n+2}$

Επομένως η ϕ είναι αναγωγή της HP_{n+1} στην HP_{n+2}. □

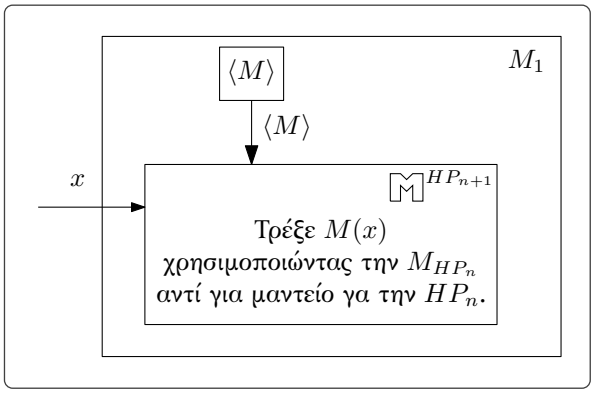
Λήμμα 8.2.6. Για κάθε $n \geq 1$ ισχύει ότι $HP_{n+1} \notin \mathsf{REC}^{HP_n}$.

Απόδειξη. Η απόδειξη είναι αντίστοιχη με την απόδειξη της Πρότασης 8.1.23 [2]. □

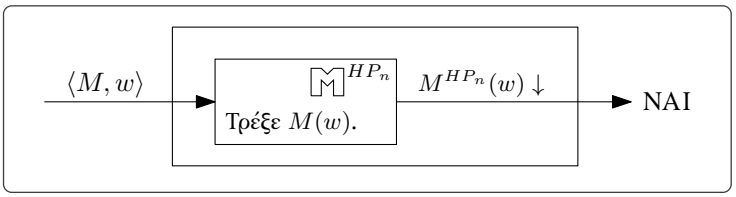
Λήμμα 8.2.7. Για κάθε $n \geq 1$ ισχύει ότι $HP_n \in \Sigma_n^0$.

[1] Το γεγονός ότι τερματίζει δεν οφείλεται στους «χρησμούς» του μαντείου, αλλά στην σχεδίασή της και (φυσικά) στη λέξη εισόδου w. Για να είμαστε απολύτως τυπικοί θα πρέπει να ελέγξουμε τι γίνεται με την περίπτωση όπου $x = \langle M, w\rangle$ και η M είναι ΟΤΜ (και όχι απλή ΤΜ) και ισχύει ότι $M^{HP}(w)\downarrow$, αλλά ο τερματισμός της $M^{HP}(w)$ βασίζεται στους«χρησμούς» του μαντείου. Στην περίπτωση αυτή η ΟΤΜ του Σχήματος 8.2.1 θα επιστρέψει ΝΑΙ αλλά θα έπρεπε να επιστρέψει ΟΧΙ (καθώς η M δεν είναι απλή ΤΜ). Για να αποφύγουμε τη λάθος απάντηση της ΟΤΜ του Σχήματος 8.2.1 θα πρέπει πρώτα να ελέγξουμε αν η M είναι απλή ΤΜ ή όχι (ελέγχοντας την κωδικοποίησή της για να δούμε αν ικανοποιεί την ιδιότητα της Σύμβασης 8.1.16).

[2] Για την ακρίβεια, στην Πρόταση 8.1.23 δείξαμε ότι $HP_2 \notin \mathsf{REC}^{HP_1}$.



Σχήμα 8.2.2: *Η OTM M_1 στην αναγωγή της HP_{n+1} στην HP_{n+2}.*



Σχήμα 8.2.3: *Η OTM στην απόδειξη του Λήμματος 8.2.7.*

Απόδειξη. Θα το δείξουμε κάνοντας επαγωγή στο n.

Βάση: Για $n = 1$ στην απόδειξη του Θεωρήματος 5.2.1 δείξαμε ότι $HP \in \mathsf{RE}$ (δηλαδή ότι $HP_1 \in \Sigma_1^0$).

Επαγωγική υπόθεση: Υποθέτουμε ότι $HP_n \in \Sigma_n^0$.

Επαγωγικό βήμα: Παρατηρούμε ότι η ΟΤΜ του Σχήματος 8.2.3 ημι-αποφασίζει την HP_{n+1} χρησιμοποιώντας για μαντείο την HP_n. Από την επαγωγική υπόθεση έχουμε ότι $HP_n \in \Sigma_n^0$, άρα $HP_{n+1} \in \Sigma_{n+1}^0$. □

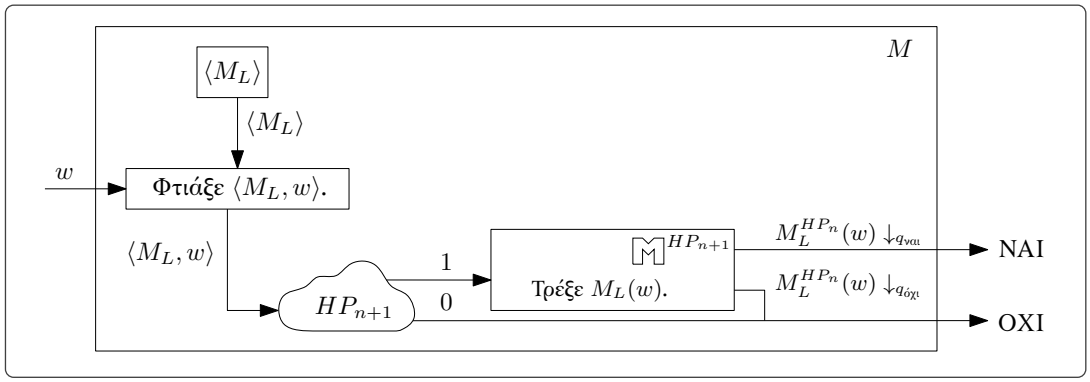
Λήμμα 8.2.8. Για κάθε $n \geq 1$ ισχύει ότι $\Sigma_n^0 \subseteq \mathsf{REC}^{HP_n}$.

Απόδειξη. Θα το δείξουμε κάνοντας επαγωγή στο n.

Βάση: Για $n = 1$ πρέπει να δείξουμε ότι $\Sigma_1^0 \subseteq \mathsf{REC}^{HP_1}$ ή αλλιώς ότι $\mathsf{RE} \subseteq \mathsf{REC}^{HP}$ το οποίο ισχύει από την Πρόταση 8.1.22.

Επαγωγική υπόθεση: Υποθέτουμε ότι $\Sigma_n^0 \subseteq \mathsf{REC}^{HP_n}$.

Επαγωγικό βήμα: Έστω $L \in \Sigma_{n+1}^0$, δηλαδή υπάρχει γλώσσα $A \in \Sigma_n^0$ τέτοια ώστε $L \in \mathsf{RE}^A$. Από την επαγωγική υπόθεση προκύπτει ότι $A \in \mathsf{REC}^{HP_n}$, συνεπώς από το Θεώρημα 8.1.27 έπεται ότι $L \in \mathsf{RE}^{HP_n}$, άρα υπάρχει ΟΤΜ $M_L^{HP_n}$ που την ημι-αποφασίζει. Θεωρούμε την ΟΤΜ M του Σχήματος 8.2.4. Η χρησμοληπτική καθολική ΤΜ του Σχήματος 8.2.4 χρησιμοποιεί μαντείο για την HP_{n+1} και όχι για την HP_n. Για να προσομοιώσουμε όμως την λειτουργία



Σχήμα 8.2.4: *Η ΟΤΜ M στην απόδειξη του Λήμματος 8.2.8.*

της $M_L^{HP_n}$ χρειαζόμαστε μαντείο για την HP_n αντ' αυτής όμως χρησιμοποιούμε την HP_{n+1}. Αυτό είναι εφικτό καθώς στην Πρόταση 8.2.5 δείξαμε ότι $HP_n \in \mathsf{REC}^{HP_{n+1}}$, άρα μπορούμε να χρησιμοποιήσουμε στη θέση του μαντείου για την HP_n την ΟΤΜ που αποφασίζει την HP_n και χρησιμοποιεί μαντείο για την HP_{n+1}.

Παρατηρούμε ότι η ΟΤΜ $M^{HP_{n+1}}$ του Σχήματος 8.2.4 αποφασίζει την L, άρα $L \in \mathsf{REC}^{HP_n+1}$. □

Παρατήρηση 8.2.9. Έστω γλώσσα $L \subseteq \{0,1\}^*$. Για κάθε $n \geq 2$ αν $L \in \Sigma_n^0$ ($L \in \Delta_n^0$) τότε $L \in \mathsf{RE}^{HP_{n-1}}$ ($L \in \mathsf{REC}^{HP_{n-1}}$ αντίστοιχα).

Πράγματι, αν $L \in \Sigma_n^0$ τότε υπάρχει γλώσσα $A \in \Sigma_{n-1}^0$ τέτοια ώστε $L \in \mathsf{RE}^A$. Από το Λήμμα 8.2.8 ισχύει ότι $\Sigma_{n-1}^0 \subseteq \mathsf{REC}^{HP_{n-1}}$, άρα $A \in \mathsf{REC}^{HP_{n-1}}$, οπότε, από το Θεώρημα 8.1.27, προκύπτει ότι $L \in \mathsf{RE}^{HP_{n-1}}$.

Πλέον είμαστε σε θέση να αποδείξουμε ότι ο Ορισμός 8.2.3 δεν ήταν εις μάτην, καθώς καμία από τις κλάσεις Σ_n^0, Π_n^0 και Δ_n^0 δεν «καταρρέει» μέσα σε κάποια άλλη. Η απόδειξη αυτού του ισχυρισμού δίνεται στο ακόλουθο Θεώρημα.

Θεώρημα 8.2.10 (Θεώρημα Αριθμητικής Ιεραρχίας, Kleene-Turing). Για κάθε $n \geq 1$ ισχύει ότι:

i. $\Sigma_n^0 \subset \Sigma_{n+1}^0$ και $\Pi_n^0 \subset \Pi_{n+1}^0$

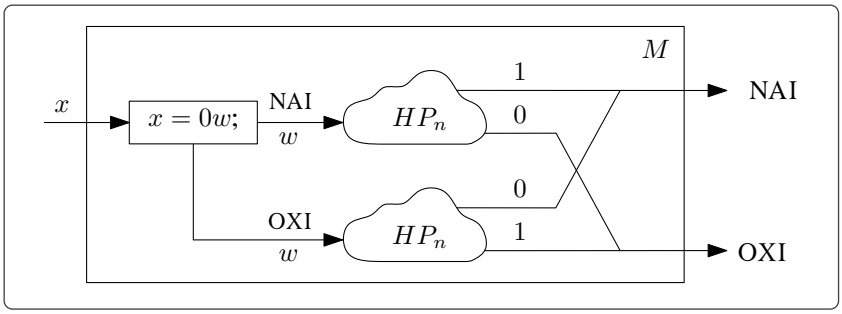
ii. $\Sigma_n^0 \notin \Pi_n^0$ και $\Pi_n^0 \notin \Sigma_n^0$

iii. $\Sigma_n^0 \cup \Pi_n^0 \subset \Delta_{n+1}^0$

iv. $\Sigma_n^0 \cap \Pi_n^0 = \Delta_n^0$

v. $\Delta_n^0 \subset \Sigma_n^0$ και $\Delta_n^0 \subset \Pi_n^0$

Απόδειξη. i. Από το Λήμμα 8.2.8 ξέρουμε ότι $\Sigma_n^0 \subseteq \mathsf{REC}^{HP_n}$, άρα και ότι $\Sigma_n^0 \subseteq \mathsf{RE}^{HP_n}$. Από το Λήμμα 8.2.7 ξέρουμε ότι $HP_n \in \Sigma_n^0$. Συνεπώς $\Sigma_n^0 \subseteq \Sigma_{n+1}^0$. Επίσης, αν $L \in \Pi_n^0$ τότε $\overline{L} \in \Sigma_n^0 \subseteq \Sigma_{n+1}^0$, άρα $L \in \Pi_{n+1}^0$, Συνεπώς $\Pi_n^0 \subseteq \Pi_{n+1}^0$.



Σχήμα 8.2.5: *Η ΟΤΜ M που αποφασίζει την $0HP_n \cup 1\overline{HP}_n$ αν χρησιμοποιήσουμε μαντείο για την HP_n (τυπικά πρέπει πρώτα να ελέγξουμε αν $x = \epsilon$).*

Ας δείξουμε τώρα ότι οι εγκλεισμοί είναι γνήσιοι. Από το Λήμμα 8.2.7 ξέρουμε ότι $HP_{n+1} \in \Sigma^0_{n+1}$, από το Λήμμα 8.2.8 ότι $\Sigma^0_n \subseteq \mathsf{REC}^{HP_n}$ και από το Λήμμα 8.2.6 ότι $HP_{n+1} \notin \mathsf{REC}^{HP_n}$, άρα $HP_{n+1} \notin \Sigma^0_n$. Επίσης, $\overline{HP}_{n+1} \in \Pi^0_{n+1}$, αφού $HP_{n+1} \in \Sigma^0_{n+1}$, αλλά $\overline{HP}_{n+1} \notin \Pi^0_n$ καθώς τότε θα ίσχυε ότι $HP_{n+1} \in \Sigma^0_n$.

ii. Από το Λήμμα 8.2.7 ξέρουμε ότι $HP_n \in \Sigma^0_n$ και από την Παρατήρηση 8.2.9 ότι $\Sigma^0_n \subseteq \mathsf{RE}^{HP_{n-1}}$ για $n \geq 2$ [1]. Συνεπώς $HP_n \in \mathsf{RE}^{HP_{n-1}}$. Αν ίσχυε ότι $\Sigma^0_n \subseteq \Pi^0_n$ τότε $HP_n \in \Pi^0_n$, οπότε $\overline{HP}_n \in \Sigma^0_n$. Όπως πριν μπορούμε να δείξουμε ότι $\overline{HP}_n \in \mathsf{RE}^{HP_{n-1}}$. Συνεπώς, από το Θεώρημα 8.1.26 θα ίσχυε ότι $HP_n \in \mathsf{REC}^{HP_{n-1}}$ πράγμα που αντιβαίνει στο Λήμμα 8.2.6.

Με αντίστοιχο τρόπο (χρησιμοποιώντας την $\overline{HP}_n$) δείχνουμε ότι $\Pi^0_n \notin \Sigma^0_n$.

iii. Από το Λήμμα 8.2.8 ξέρουμε ότι $\Sigma^0_n \subseteq \mathsf{REC}^{HP_n}$. Από το Λήμμα 8.2.7 ξέρουμε ότι $HP_n \in \Sigma^0_n$. Συνεπώς $\Sigma^0_n \subseteq \Delta^0_{n+1}$. Επίσης, αν $L \in \Pi^0_n$ τότε $\overline{L} \in \Sigma^0_n \subseteq \mathsf{REC}^{HP_n}$. Από το Θεώρημα 8.1.24 έπεται ότι και $L \in \mathsf{REC}^{HP_n}$, άρα, όπως πριν, $\Pi^0_n \subseteq \Delta^0_{n+1}$.

Ας δείξουμε τώρα ότι οι εγκλεισμοί είναι γνήσιοι. Θεωρούμε τη γλώσσα:

$$0HP_n \cup 1\overline{HP}_n = \{0w \in \{0,1\}^* \mid w \in HP_n\} \cup \{1w \in \{0,1\}^* \mid w \notin HP_n\}$$ [2]

Παρατηρούμε ότι $0HP_n \cup 1\overline{HP}_n \in \mathsf{REC}^{HP_n}$ καθώς η ΟΤΜ M^{HP_n} του Σχήματος 8.2.5 την αποφασίζει. Άρα $0HP_n \cup 1\overline{HP}_n \in \Delta^0_{n+1}$.

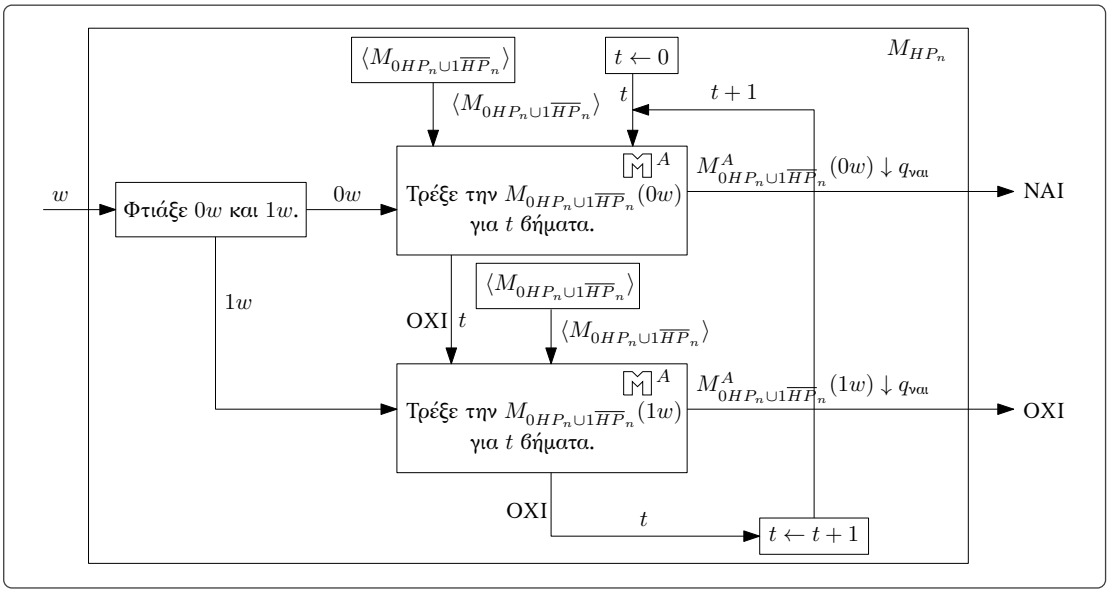
Έστω (προς άτοπο) ότι $0HP_n \cup 1\overline{HP}_n \in \Sigma^0_n$ για $n \geq 2$ [3], δηλαδή υπάρχει γλώσσα $A \in \Sigma^0_{n-1}$ και ΟΤΜ, έστω $M^A_{0HP_n \cup 1\overline{HP}_n}$, που την ημι-αποφασίζει. Η ΟΤΜ $M^A_{HP_n}$ του Σχήματος 8.2.6 αποφασίζει την HP_n, συνεπώς $HP_n \in \mathsf{REC}^A$. Καθώς $A \in \Sigma^0_{n-1}$ και (λόγω του Λήμματος 8.2.8) $\Sigma^0_{n-1} \subseteq \mathsf{REC}^{HP_{n-1}}$, έπεται ότι $HP_n \in \mathsf{REC}^{HP_{n-1}}$ (λόγω του Θεωρήματος 8.1.27) πράγμα που αντιβαίνει στο Λήμμα 8.2.6.

Μένει να δείξουμε ότι $0HP_n \cup 1\overline{HP}_n \notin \Pi^0_n$, ή αλλιώς ότι $\overline{0HP_n \cup 1\overline{HP}_n} \notin \Sigma^0_n$. Παρατη-

[1] Για $n = 1$ το ζητούμενο προκύπτει άμεσα από το γεγονός ότι $\overline{HP} \notin RE$.

[2] Θυμηθείτε τον Ορισμό 0.2.19.

[3] Για $n = 1$ είναι προφανές ότι $0HP \cup 1\overline{HP} \notin \mathsf{REC}$ (η απόδειξη είναι αντίστοιχη με αυτή για $n \geq 2$ μόνο που δεν χρησιμοποιούμε μαντεία).



Σχήμα 8.2.6: *Η OTM M_{HP_n} που (υποθετικά) αποφασίζει την HP_n αν χρησιμοποιήσει μαντείο για την $A \in \Sigma^0_{n-1}$.*

ρούμε ότι:

$$\begin{aligned}
\overline{0HP_n \cup 1\overline{HP}_n} &= \overline{\{0w \in \{0,1\}^* \mid w \in HP_n\} \cup \{1w \in \{0,1\}^* \mid w \notin HP_n\}} \\
&= \overline{\{0w \in \{0,1\}^* \mid w \in HP_n\}} \setminus \{1w \in \{0,1\}^* \mid w \notin HP_n\} \\
&= \big(\{x \in \{0,1\}^* \mid \exists w \in \{0,1\}^* (x = 1w)\} \cup \{0w \in \{0,1\}^* \mid w \notin HP_n\} \cup \{\epsilon\}\big) \\
&\quad \setminus \{1w \in \{0,1\}^* \mid w \notin HP_n\} \\
&= \big(\{x \in \{0,1\}^* \mid \exists w \in \{0,1\}^* \ (x = 1w)\} \cup 0\overline{HP_n} \cup \{\epsilon\})\big) \setminus 1\overline{HP_n} \\
&= 1HP_n \cup 0\overline{HP_n} \cup \{\epsilon\}
\end{aligned}$$

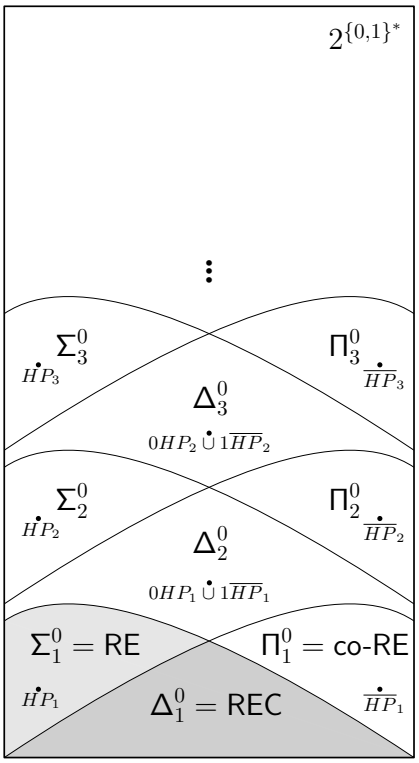
Επαναλαμβάνοντας την παραπάνω απόδειξη, με το 0 και το 1 στην αρχή των λέξεων αντεστραμμένα (λαμβάνοντας υπόψιν και την ϵ), αποδεικνύουμε ότι $1HP_n \cup 0\overline{HP_n} \cup \{\epsilon\} \notin \Sigma^0_n$ από το οποίο άμεσα προκύπτει το ζητούμενο.

iv. Έστω γλώσσα $L \in \Delta^0_n$ για $n \geq 2$ [1], δηλαδή υπάρχει $A \in \Sigma^0_{n-1}$ τέτοια ώστε $L \in \mathsf{REC}^A$. Από το Θεώρημα 8.1.24 έπεται ότι $\overline{L} \in \mathsf{REC}^A$ επίσης. Άρα:

$$\left.\begin{aligned} L \in \mathsf{REC}^A \Rightarrow L \in \mathsf{RE}^A \Rightarrow L \in \Sigma^0_n \\ \overline{L} \in \mathsf{REC}^A \Rightarrow \overline{L} \in \mathsf{RE}^A \Rightarrow \overline{L} \in \Sigma^0_n \end{aligned}\right\} \Rightarrow L \in \Sigma^0_n \cap \Pi^0_n$$

Έστω τώρα γλώσσα $L \in \Sigma^0_n \cap \Pi^0_n$, δηλαδή οι L και $\overline{L}$ ανήκουν στην κλάση Σ^0_n. Σύμφωνα με την Παρατήρηση 8.2.9 έπεται ότι $L, \overline{L} \in \mathsf{RE}^{HP_{n-1}}$, ή αλλιώς ότι $L \in \mathsf{RE}^{HP_{n-1}} \cap \text{co-}\mathsf{RE}^{HP_{n-1}}$.

[1] Για $n = 1$ το ζητούμενο προκύπτει από τα Θεωρήματα 1.5.3 και 1.5.4.



Σχήμα 8.2.7: *Η Αριθμητική Ιεραρχία.*

Τέλος, από το Θεώρημα 8.1.26 έπεται ότι $L \in \mathsf{REC}^{HP_{n-1}}$ και από το Λήμμα 8.2.7 ότι $HP_{n-1} \in \Sigma_{n-1}^0$, άρα $L \in \Delta_n^0$.

v. Έστω (προς άτοπο) ότι $HP_n \in \Delta_n^0$ για $n \geq 2$ [1]. Από την Παρατήρηση 8.2.9 έπεται ότι $HP_n \in \mathsf{REC}^{HP_{n-1}}$, πράγμα που αντιβαίνει στο Λήμμα 8.2.6. Αντίστοιχα αποδεικνύεται ότι $\overline{HP_n} \notin \Delta_n^0$. □

Οι κλάσεις γλωσσών της Αριθμητικής Ιεραρχίας φαίνονται στο Σχήμα 8.2.7.

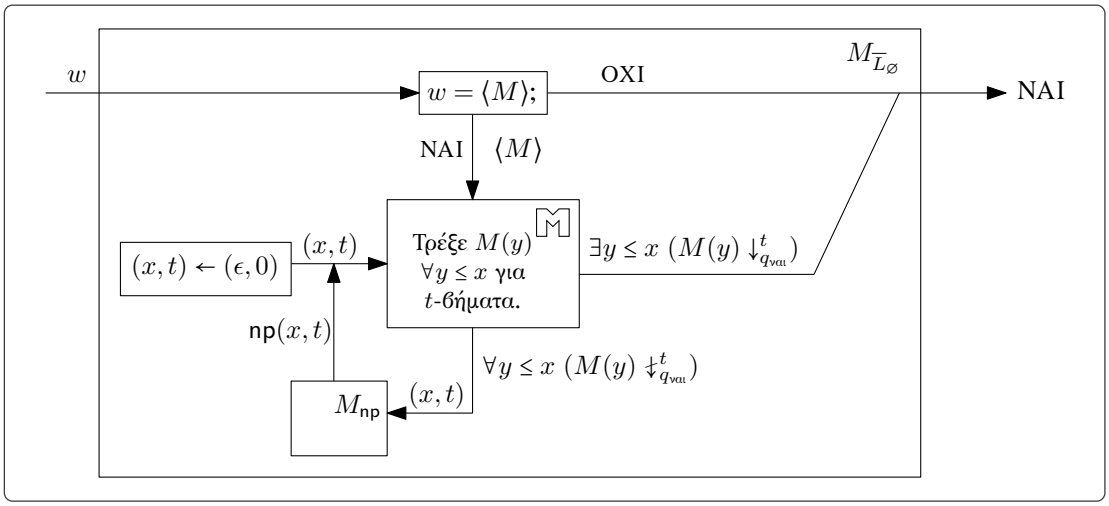
8.3 Αλγοριθμικές Αναγωγές

Οι χρησμοληπτικές TM και τα μαντεία χρησιμοποιούνται για να ορίσουμε μία ακόμα μορφή αναγωγής μεταξύ γλωσσών. Οι αναγωγές αυτές μπορεί να θεωρηθούν γενίκευση των απεικονιστικών αναγωγών για λόγους που θα συζητήσουμε στη συνέχεια.

Ορισμός 8.3.1. Έστω γλώσσες $A, B \subseteq \{0,1\}^*$. Η A *ανάγεται (αλγοριθμικά ή κατά Turing) στη* B, συμβολισμός $A \leq_T B$, ανν $A \in \mathsf{REC}^B$.

Στο Παράδειγμα 8.1.12 είδαμε ότι $L_{\text{Αποδοχής}} \leq_T HP$. Ας δούμε ένα ακόμα παράδειγμα.

[1] Για $n = 1$ στο Κεφάλαιο 5 δείξαμε ότι $HP, \overline{HP} \notin \mathsf{REC}$.



Σχήμα 8.3.1: *Η ΤΜ που ημι-αποφασίζει την $\overline{L}_\varnothing$, όπου M_{np} η ΤΜ της Παρατήρησης 1.4.18.*

Παράδειγμα 8.3.2. Θα δείξουμε ότι η γλώσσα $L_\varnothing$ του Παραδείγματος 5.2.20 ανάγεται αλγοριθμικά στην HP. Πρώτα θα δείξουμε ότι $L_\varnothing \in$ co-RE, δηλαδή ότι $\overline{L}_\varnothing \in$ RE. Παρατηρούμε ότι:

$$\overline{L}_\varnothing = \{w \in \{0,1\}^* \mid (\exists \text{ ΤΜ } M\ (w = \langle M \rangle)) \rightarrow (L(M) \neq \varnothing)\}$$

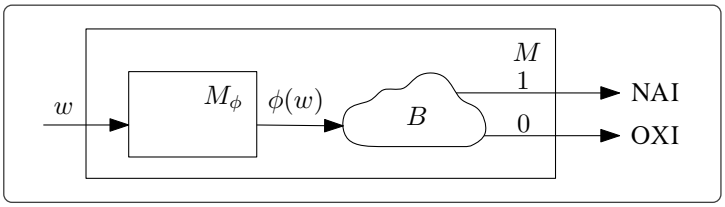
και ότι η ΤΜ $M_{\overline{L}_\varnothing}$ του Σχήματος 8.3.1 την ημι-αποφασίζει. Από το Θεώρημα 8.2.10 (το ii.), αφού $L_\varnothing \in \Pi^0_1$, προκύπτει ότι $L_\varnothing \in \Delta^0_2$. Από την Παρατήρηση 8.2.9 έπεται ότι $L_\varnothing \in \mathsf{REC}^{HP}$. Επομένως $L_\varnothing \leq_T HP$.

Επιπλέον, αφού $L_\varnothing \notin$ REC (δες Παράδειγμα 5.2.20), μπορούμε να κατατάξουμε την $L_\varnothing$ στην Αριθμητική Ιεραρχία. Έπεται ότι $L_\varnothing \in \Pi^0_1 \setminus \Delta^0_1$.

Διαισθητικά ο ορισμός της αλγοριθμικής αναγωγής μας λέει ότι αν η ύπαρξη ενός αλγορίθμου για τη γλώσσα B μπορεί να χρησιμοποιηθεί, έστω και με «μη ρεαλιστικό» τρόπο (μέσω ενός μαντείο για τη B), για να αποφασίσουμε την A, τότε $A \leq_T B$. Αν έχουμε έναν «ρεαλιστικό» τρόπο (μέσω μίας υπολογίσιμης συνάρτησης) να εκμεταλλευτούμε την ύπαρξη αλγορίθμου για την B τότε η A ανάγεται απεικονιστικά στην B.

Μία πιο ουσιαστική διαφορά μεταξύ των δύο μορφών αναγωγής προκύπτει όταν ενδιαφερθούμε και για τον χρόνο υπολογισμού. Προφανώς αν $A \leq_T B$ και υπάρχει αλγόριθμος που αποφασίζει τη B τότε υπάρχει αλγόριθμος που αποφασίζει την A [1]. Καθώς όμως μπορεί να γίνονται πολλά ερωτήματα προς το μαντείο, αυτός ο αλγόριθμος για την A πιθανώς να χρειάζεται παραπάνω χρόνο από τον αλγόριθμο για τη B (περισσότερο και από την ΟΤΜ που αποφασίζει την A ως προς τη B, αν δεν μετρήσουμε στον χρόνο αυτόν τα ερωτήματα προς το μαντείο). Στις απεικονιστικές αναγωγές όμως ο χρόνος του αλγορίθμου για την A είναι πάντα ο χρόνος που χρειαζόμαστε για να υπολογίσουμε τη συνάρτηση της αναγωγής

[1] Αντικαθιστούμε κάθε αλληλεπίδραση με το μαντείο με μία εκτέλεση του αλγορίθμου για τη B, με είσοδο τη λέξη για την οποία έγινε το ερώτημα προς το μαντείο.



Σχήμα 8.3.2: *Η ΟΤΜ M στην απόδειξη της Πρότασης 8.3.3.*

συν τον χρόνο που χρειάζεται ο αλγόριθμος για τη B (με είσοδο την εικόνα της αναγωγής). Στην Υπολογιστική Πολυπλοκότητα οι αλγοριθμικές αναγωγές είναι γνωστές και ως *αναγωγές Cook* [1] (προς τιμήν του *Stephen Cook*), ενώ οι απεικονιστικές αναγωγές ως *αναγωγές Karp* [2] (προς τιμήν του *Richard Karp*).

Παρατηρήστε ότι μπορούμε να θεωρήσουμε ότι οι απεικονιστικές αναγωγές είναι στην ουσία αλγοριθμικές αναγωγές, μόνο που έχουμε το δικαίωμα να κάνουμε ένα και μόνο ερώτημα στο μαντείο (για τη λέξη που προκύπτει εφαρμόζοντας τη συνάρτηση αναγωγής πάνω στη λέξη εισόδου) και η απάντηση που θα επιστρέψει η μηχανή μας είναι ακριβώς η απάντηση του μαντείου. Αυτή είναι η ιδέα της απόδειξης της πρότασης που ακολουθεί.

Πρόταση 8.3.3. Έστω γλώσσες $A, B \subseteq \{0,1\}^*$. Αν $A \leq_m B$ τότε $A \leq_T B$.

Απόδειξη. Έστω ϕ η αναγωγή της A στη B και M_ϕ η ΤΜ που την υπολογίζει. Παρατηρούμε ότι η ΟΤΜ M^B του Σχήματος 8.3.2 αποφασίζει την A, καθώς:

- $w \in A \Leftrightarrow \phi(w) \in B \Leftrightarrow$ Το μαντείο θα επιστρέψει 1 $\Leftrightarrow M^B(w) \downarrow_{q_{\text{ναι}}}$
- $w \notin A \Leftrightarrow \phi(w) \notin B \Leftrightarrow$ Το μαντείο θα επιστρέψει 0 $\Leftrightarrow M^B(w) \downarrow_{q_{\text{όχι}}}$

Συνεπώς $A \leq_T B$. □

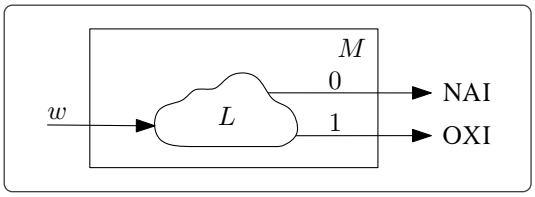
Συνεπώς οι αλγοριθμικές αναγωγές αποτελούν γενίκευση των απεικονιστικών. Η γενίκευση αυτή είναι ουσιαστική, καθώς, όπως μας δείχνει η ακόλουθη παρατήρηση, το αντίστροφο της Πρότασης 8.3.3 δεν ισχύει.

Παρατήρηση 8.3.4. Έστω γλώσσα $L \subseteq \{0,1\}^*$. Παρατηρούμε ότι $L \leq_T \overline{L}$ καθώς η ΟΤΜ M^L του Σχήματος 8.3.3 την αποφασίζει. Αυτό φυσικά δεν ισχύει με τις απεικονιστικές αναγωγές, καθώς η γλώσσα $\overline{HP}$ δεν ανάγεται απεικονιστικά στην HP, καθώς τότε θα ίσχυε ότι $\overline{HP} \in \mathsf{RE}$.

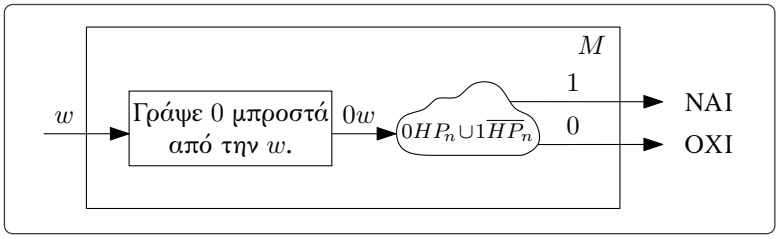
Παρατήρηση 8.3.5. Η σχέση $\leq_T$ είναι μεταβατική λόγω του Θεωρήματος 8.1.27 (το ii.).

[1] Εκεί μπορούμε να κάνουμε μόνο ένα πολυωνυμικό πλήθος ερωτημάτων προς το μαντείο και, φυσικά, η ΟΤΜ χρειάζεται πολυωνυμικό πλήθος βημάτων για να τερματίσει.

[2] Η συνάρτηση της αναγωγής πρέπει να είναι υπολογίσιμη σε πολυωνυμικό χρόνο.



Σχήμα 8.3.3: *Η ΟΤΜ M που αποφασίζει την $\overline{L}$ αν χρησιμοποιήσει μαντείο για την L.*



Σχήμα 8.4.1: *Η ΟΤΜ M στην απόδειξη της Πρότασης 8.4.3.*

8.4 Πληρότητα γλωσσών ως προς σχέση αναγωγής

Μία ακόμα έννοια (ενδεχομένως) γνωστή από την Υπολογιστική Πολυπλοκότητα είναι η έννοια της *πληρότητας* μίας γλώσσα σε μία κλάση γλωσσών.

Ορισμός 8.4.1. Έστω κλάση γλωσσών $\mathcal{C} \subseteq 2^{\{0,1\}^*}$ και γλώσσα $B \subseteq \{0,1\}^*$. Η B καλείται *$\mathcal{C}$-δύσκολη ως προς τη σχέση αναγωγής $\trianglelefteq \in \{\leq_m, \leq_T\}$* ανν για κάθε $A \in \mathcal{C}$ ισχύει ότι $A \trianglelefteq B$. Αν επιπλέον ισχύει ότι $B \in \mathcal{C}$, τότε η B καλείται *$\mathcal{C}$-πλήρης ως προς τη $\trianglelefteq$*.

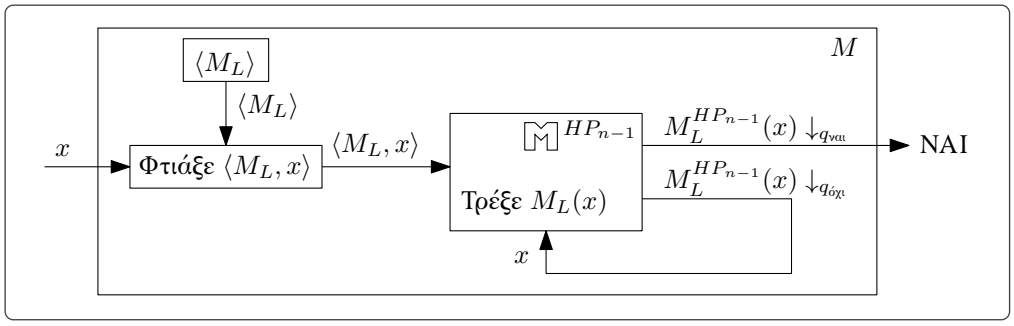
Παρατήρηση 8.4.2. Από το Λήμμα 8.2.8 προκύπτει ότι για κάθε $n \geq 1$ η HP_n είναι Σ_n^0-δύσκολη ως προς τη $\leq_T$ και από το Λήμμα 8.2.7 ότι είναι και Σ_n^0-πλήρης ως προς τη $\leq_T$. Αναλόγως προκύπτει ότι η $\overline{HP}_n$ είναι Π_n^0-πλήρης ως προς τη $\leq_T$.

Παρατηρήστε όμως και το εξής: Ως προς την $\leq_T$ η HP_n είναι Π_n^0-δύσκολη και η $\overline{HP}_n$ είναι Σ_n^0-δύσκολη, όπως επίσης η HP_n είναι Δ_{n+1}^0-πλήρης [1]!

Πρόταση 8.4.3. Για κάθε $n \geq 1$ η γλώσσα $0HP_n \cup 1\overline{HP}_n$ είναι Δ_{n+1}^0-πλήρης ως προς τη $\leq_T$.

Απόδειξη. Στο ii. της απόδειξης του Θεωρήματος 8.2.10 δείξαμε ότι $0HP_n \cup 1\overline{HP}_n \in \Delta_{n+1}^0$, συνεπώς αρκεί να δείξουμε ότι είναι Δ_{n+1}^0-δύσκολη ως προς τη $\leq_T$. Έστω $L \in \Delta_{n+1}^0$. Από την Παρατήρηση 8.2.9 έπεται ότι $L \in \mathsf{REC}^{HP_n}$, άρα $L \leq_T HP_n$. Παρατηρούμε ότι η ΟΤΜ $M^{0HP_n \cup 1\overline{HP}_n}$ του Σχήματος 8.4.1 αποφασίζει την HP_n, άρα $HP_n \leq_T 0HP_n \cup 1\overline{HP}_n$ και από τη μεταβατικότητας της $\leq_T$ έπεται ότι $L \leq_T 0HP_n \cup 1\overline{HP}_n$. □

[1] Αυτός είναι ο βασικός λόγος που αποφεύγουμε να χρησιμοποιούμε αλγοριθμικές αναγωγές στην υπολογιστική πολυπλοκότητα: Δεν είναι αρκετά «ευαίσθητες» στη διαφορετικότητα των κλάσεων πολυπλοκότητας (π.χ. κάθε NP-πλήρης γλώσσα είναι co-NP-δύσκολη ως προς $\leq_T$).



Σχήμα 8.4.2: *Η ΟΤΜ M στην απόδειξη του Θεωρήματος 8.4.4.*

Ας δούμε τι συμβαίνει όσον αφορά την πληρότητα των κλάσεων Σ_n^0 και Π_n^0 ως προς τη $\leq_m$.

Θεώρημα 8.4.4. Για κάθε $n \geq 1$ ισχύει ότι:

i. Η γλώσσα HP_n είναι Σ_n^0-πλήρης ως προς τη $\leq_m$.

ii. Η γλώσσα $\overline{HP}_n$ είναι Π_n^0-πλήρης ως προς τη $\leq_m$.

Απόδειξη. [1] i. Από το Λήμμα 8.2.7 προκύπτει ότι $HP_n \in \Sigma_n^0$. Μένει να δείξουμε ότι η HP_n είναι Σ_n^0-δύσκολη ως προς τη $\leq_m$. Έστω γλώσσα $L \in \Sigma_n^0$. Από την Παρατήρηση 8.2.9 έπεται ότι $L \in \mathsf{RE}^{HP_{n-1}}$, άρα υπάρχει ΟΤΜ $M_L^{HP_{n-1}}$ που την ημι-αποφασίζει. Θεωρούμε συνάρτηση $\phi : \{0,1\}^* \to \{0,1\}^*$ με $\phi(w) = \langle M, w\rangle$ όπου M η ΟΤΜ του Σχήματος 8.4.2 και παρατηρούμε ότι:

1. ϕ πλήρης και υπολογίσιμη.

2. - $w \in L \Rightarrow M_L^{HP_{n-1}}(w) \downarrow_{q_{\text{ναι}}} \Rightarrow M^{HP_{n-1}}(w) \downarrow \Rightarrow \langle M, w\rangle \in HP_n$
   - $w \notin L \Rightarrow M_L^{HP_{n-1}}(w) \downarrow_{q_{\text{ναι}}} \Rightarrow M^{HP_{n-1}}(w) \uparrow \Rightarrow \langle M, w\rangle \notin HP_n$

Συνεπώς $L \leq_m HP_n$.

ii. Από το Λήμμα 8.2.7 προκύπτει ότι $HP_n \in \Sigma_n^0$, άρα $\overline{HP}_n \in \Pi_n^0$. Μένει να δείξουμε ότι η $\overline{HP}_n$ είναι Π_n^0-δύσκολη ως προς τη $\leq_m$. Έστω γλώσσα $L \in \Pi_n^0$, δηλαδή $\overline{L} \in \Sigma_n^0$. Από το i. έπεται ότι $\overline{L} \leq_m HP_n$ και την Πρόταση 5.2.22 ότι $L \leq_m \overline{HP}_n$. □

Η απόδειξη του παρακάτω θεωρήματος αφήνεται ως άσκηση.

Θεώρημα 8.4.5. Για κάθε $n \geq 1$ ισχύει ότι η γλώσσα $0HP_n \cup 1\overline{HP_n}$ είναι Δ_{n+1}^0-πλήρης ως προς τη $\leq_m$.

[1] Θα αποδείξουμε το θεώρημα για $n \geq 2$. Η περίπτωση όπου $n = 1$ αφήνεται ως άσκηση.

8.5 Πέρα από την Αριθμητική Ιεραρχία

Σε αυτήν την παράγραφο θα δώσουμε έναν εναλλακτικό ορισμό των κλάσεων της Αριθμητικής Ιεραρχίας, χωρίς τη χρήση των μαντείων.

Ορισμός 8.5.1. Ένα *n-μελές κατηγόρημα*, για $n \in \mathbb{N}$, είναι μία σχέση του $(\{0,1\}^*)^n$.

Συμβολισμός 8.5.2. Έστω n-μελές κατηγόρημα R. Αντί για $(x_1, \dots, x_n) \in R$ θα γράφουμε $R(x_1, \dots, x_n)$.

Ορισμός 8.5.3. Ένα *n-μελές κατηγόρημα* R είναι *αποφάνσιμο* ανν η γλώσσα:

$$L_R = \{\langle x_1, \dots, x_n\rangle \in \{0,1\}^* \mid R(x_1, \dots, x_n)\}$$

είναι αναδρομική.

Το παρακάτω Θεώρημα-Ορισμός δίνεται χωρίς απόδειξη.

Θεώρημα 8.5.4 (Ποσοδεικτικός ορισμός Αριθμητικής Ιεραρχίας)**.** Έστω μία γλώσσα $L \subseteq \{0,1\}^*$. Ισχύει ότι:

i. $L \in \Sigma_n^0$ ανν υπάρχει αποφάνσιμο $(n+1)$-μελές κατηγόρημα R τέτοιο ώστε:

$$L = \{x \in \{0,1\}^* \mid \exists y_1 \ \forall y_2 \cdots * y_n \ R(x, y_1, \dots, y_n)\}$$

$$\text{όπου } * = \begin{cases} \exists & \text{, αν το } n \text{ είναι περιττό} \\ \forall & \text{, αλλιώς} \end{cases}.$$

ii. $L \in \Pi_n^0$ ανν υπάρχει αποφάνσιμο $(n+1)$-μελές κατηγόρημα R τέτοιο ώστε:

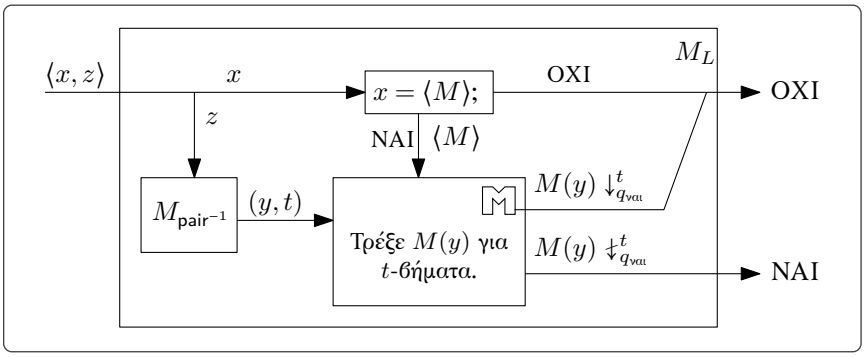
$$L = \{x \in \{0,1\}^* \mid \forall y_1 \ \exists y_2 \cdots * y_n \ R(x, y_1, \dots, y_n)\}$$

$$\text{όπου } * = \begin{cases} \forall & \text{, αν το } n \text{ είναι περιττό} \\ \exists & \text{, αλλιώς} \end{cases}.$$

Παρατήρηση 8.5.5. Παρατηρήστε ότι ο ποσοδεικτικός ορισμός των κλάσεων της Αριθμητικής Ιεραρχίας επεκτείνει τον ορισμό της κλάσης RE που είδαμε στην Άσκηση 1.9.

Παρατήρηση 8.5.6. Το πως εναλλάσσονται οι ποσοδείκτες είναι αυτό που διαχωρίζει τις γλώσσες σε αυτές που ανήκουν στη Σ_n^0 και σε αυτές που ανήκουν στην Π_n^0. Το πλήθος των εναλλαγών είναι εξίσου σημαντικό καθώς από το Θεώρημα 8.2.10 προκύπτει ότι υπάρχουν γλώσσες που ορίζονται με n-εναλλαγές ποσοδεικτών αλλά όχι με $n-1$.

Ο ορισμός αυτός είναι πολύ χρήσιμος για να κατατάσσουμε τις γλώσσες στην Αριθμητική Ιεραρχία. Ας δούμε μερικά παραδείγματα.



Σχήμα 8.5.1: *Η ΤΜ του Παραδείγματος 8.5.7.*

Παράδειγμα 8.5.7. Θα δείξουμε ότι η γλώσσα $L_\varnothing$ του Παραδείγματος 5.2.20 ανήκει στο Π^0_1 χρησιμοποιώντας τον ποσοδεικτικό ορισμό της Αριθμητικής Ιεραρχίας [1]. Παρατηρούμε ότι:

$$\begin{aligned} L_\varnothing &= \{\langle M\rangle \in \{0,1\}^* \mid L(M) = \varnothing\} \\ &= \{\langle M\rangle \in \{0,1\}^* \mid \forall y\ \forall t\ (M(y) \not\downarrow^t_{q_{\nu\alpha\iota}})\}\ ^{[2]} \\ &= \{x \in \{0,1\}^* \mid \forall y\ \forall t\ (x = \langle M\rangle \wedge M(y) \not\downarrow^t_{q_{\nu\alpha\iota}})\} \end{aligned}$$

Μπορούμε να «συνδυάσουμε» τους δύο καθολικούς ποσοδείκτες σε έναν χρησιμοποιώντας την 1-1 και επί συνάρτηση $\mathsf{pair} : (\{0,1\}^*)^2 \to \{0,1\}^*$, με $\mathsf{pair}(y,t) =$ «Η $\left(\binom{i+j+1}{2} + i\right)$-οστή λέξη στη λεξικογραφική διάταξη», όπου i και j η σειρά εμφάνισης της y και t στη λεξικογραφική διάταξη. Συνεπώς μπορούμε να γράψουμε:

$$L_\varnothing = \{x \in \{0,1\}^* \mid \forall z\ (x = \langle M\rangle \wedge \mathsf{pair}^{-1}(z) = (y,t) \wedge M(y) \not\downarrow^t_{q_{\nu\alpha\iota}})\}$$

Η γλώσσα $L = \{\langle x, z\rangle \in \{0,1\}^* \mid x = \langle M\rangle \wedge z = \mathsf{pair}^{-1}(y,t) \wedge M(y) \not\downarrow^t_{q_{\nu\alpha\iota}}\}$ είναι αναδρομική, καθώς η ΤΜ του Σχήματος 8.5.1 την αποφασίζει ($M_{\mathsf{pair}^{-1}}$ είναι η ΤΜ που υπολογίζει την pair^{-1} [3]). Άρα, από το Θεώρημα 8.5.4 έπεται ότι $L_\varnothing \in \Pi^0_1$.

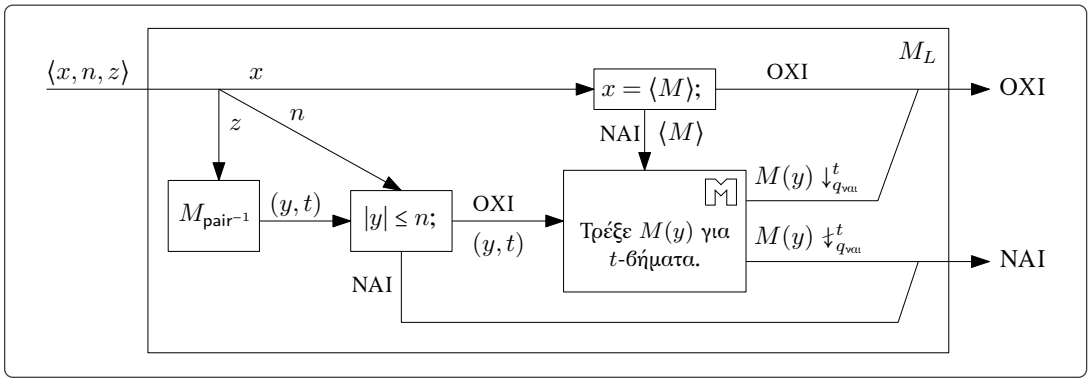
Παράδειγμα 8.5.8. Θα δείξουμε ότι η γλώσσα $L_{\mathbb{N}}$ του Παραδείγματος 6.1.2 είναι Σ^0_2-πλήρης ως προς τη $\leq_m$. Πρώτα θα δείξουμε ότι ανήκει στο Σ^0_2. Παρατηρούμε ότι:

$$\begin{aligned} L_{\mathbb{N}} &= \{\langle M\rangle \in \{0,1\}^* \mid |L(M)| \in \mathbb{N}\} \\ &= \{\langle M\rangle \in \{0,1\}^* \mid \exists n\ \forall y\ (y > n \to y \notin L(M))\} \\ &= \{\langle M\rangle \in \{0,1\}^* \mid \exists n\ \forall y\ \forall t\ (y \leq n \vee M(y) \not\downarrow^t_{q_{\nu\alpha\iota}})\} \\ &= \{x \in \{0,1\}^* \mid \exists n\ \forall z\ (x = \langle M\rangle \wedge \mathsf{pair}^{-1}(z) = (y,t) \wedge (y \leq n \vee M(y) \not\downarrow^t_{q_{\nu\alpha\iota}}))\} \end{aligned}$$

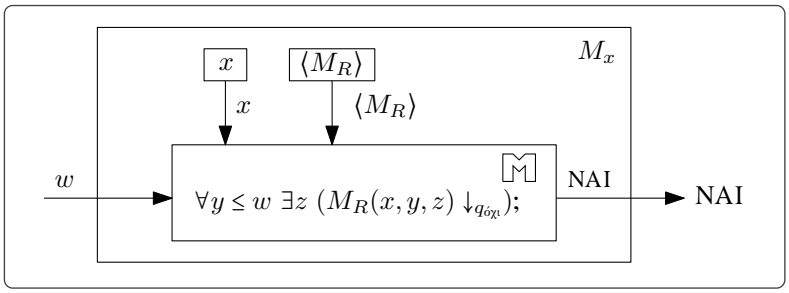
[1] Έχουμε ήδη δείξει ότι $L_\varnothing \in \Pi^0_1$ στο Παράδειγμα 8.3.2.

[2] Εδώ «ταυτίζουμε» τη λέξη t με τη σειρά εμφάνισής της στη λεξικογραφική διάταξη προκειμένου να τη «χρησιμοποιήσουμε» ως αριθμό.

[3] Η pair^{-1} είναι υπολογίσιμη συνάρτηση καθώς η pair είναι υπολογίσιμη συνάρτηση (δες Πρόταση 1.2.36, για να είμαστε τυπικοί, σε αυτή την περίπτωση θα πρέπει η ΤΜ του Σχήματος 1.2.14 να «δοκιμάζει» ζευγάρια και όχι μεμονωμένες λέξεις).



Σχήμα 8.5.2: *Η ΤΜ M_L του Παραδείγματος 8.5.8.*



Σχήμα 8.5.3: *Η ΤΜ M_x του Παραδείγματος 8.5.8. Να τονίσουμε ότι μέσα στην καθολική ΤΜ ο έλεγχος για την ύπαρξη του z γίνεται χωρίς κάποια επιπλέον φροντίδα. Δοκιμάζουμε όλα τα $z \in \{0,1\}^*$ ακολουθώντας όποια σειρά μας αρέσει.*

Η γλώσσα $L = \{\langle x,n,z\rangle \in \{0,1\}^* \mid x = \langle M\rangle \wedge \mathsf{pair}^{-1}(z) = (y,t) \wedge (y \le n \vee M(y)\downarrow^t_{q_{\nu\alpha\iota}})\}$ είναι αναδρομική, καθώς η ΤΜ του Σχήματος 8.5.2 την αποφασίζει. Άρα, από το Θεώρημα 8.5.4 έπεται ότι $L_{\mathbb{N}} \in \Sigma^0_2$.

Έστω τώρα γλώσσα $L \in \Sigma^0_2$, δηλαδή υπάρχει αποφάνσιμο 3-μελές κατηγόρημα R τέτοιο ώστε:

$$L = \{x \in \{0,1\}^* \mid \exists y\ \forall z\ R(x,y,z)\}$$

Έστω επίσης ότι η ΤΜ M_R αποφασίζει την L_R. Θεωρούμε τη συνάρτηση $\phi : \{0,1\}^* \to \{0,1\}^*$ με $\phi(x) = \langle M_x\rangle$ όπου M_x η ΤΜ του Σχήματος 8.5.3. Παρατηρούμε ότι:

1. ϕ πλήρης και υπολογίσιμη.
2. - $x \in L \Rightarrow \exists y_0\ \forall z\ (M_R(x,y_0,z)\downarrow_{q_{\nu\alpha\iota}}) \Rightarrow$ Αν $w \ge y_0$ τότε $M_x(w)\uparrow$ καθώς ισχύει ότι $M_R(x,y_0,z)\downarrow_{q_{\nu\alpha\iota}}$ για κάθε $z \Rightarrow L(M_x) \subseteq \{w \in \{0,1\}^* \mid w < y_0\} \Rightarrow |L(M_x)| \in \mathbb{N} \Rightarrow \langle M_x\rangle \in L_{\mathbb{N}}$
   - $x \notin L \Rightarrow \forall y\ \exists z\ (M_R(x,y,z)\downarrow_{q_{\acute{o}\chi\iota}}) \Rightarrow \forall w\ (\forall y \le w\ \exists z\ (M_R(x,y,z)\downarrow_{q_{\acute{o}\chi\iota}})) \Rightarrow \forall w\ (M_x(w)\downarrow_{q_{\nu\alpha\iota}}) \Rightarrow L(M_x) = \{0,1\}^* \Rightarrow |L(M_x)| = \aleph_0 \Rightarrow \langle M_x\rangle \notin L_{\mathbb{N}}$

Ορισμός 8.5.9. [1] Για κάθε $n \geq 1$ ορίζουμε τη γλώσσα:

$$T_n = \{\langle\varphi\rangle \in \{0,1\}^* \mid \varphi = \exists y_1\ \forall y_2 \cdots * y_n\ \psi(y_1, \dots, y_n) \text{ και } \mathfrak{N} \vDash \varphi\}$$

όπου ψ πρόταση της $\Gamma_1^{\theta\alpha}$, $* = \begin{cases} \exists & \text{, αν το } n \text{ είναι περιττό} \\ \forall & \text{, αλλιώς} \end{cases}$ και $\langle\varphi\rangle$ είναι η λέξη του $\{0,1\}^*$ που αντιστοιχούμε στον φυσικό αριθμό που κωδικοποιεί την πρόταση φ σύμφωνα με την Παράγραφο Α.5.l.

Θεώρημα 8.5.10. Για κάθε $n \geq 1$ η T_n είναι Σ_n^0-δύκολη γλώσσα ως προς τη $\leq_m$.

Απόδειξη. Έστω γλώσσα $L \in \Sigma_n^0$, δηλαδή υπάρχει αποφάνσιμο $(n+1)$-μελές κατηγόρημα R τέτοιο ώστε:

$$L = \{x \in \{0,1\}^* \mid \exists y_1 \forall y_2 \cdots * y_n\ R(x, y_1, \dots, y_n)\}$$

όπου $* = \begin{cases} \exists & \text{, αν το } n \text{ είναι περιττό} \\ \forall & \text{, αλλιώς} \end{cases}$.

Αφού το R είναι αποφάνσιμο από το Θεώρημα Α.5.ll έπεται ότι είναι αναπαραστάσιμο στο P έστω από τον τύπο $\varphi_R(x, y_1, \dots, y_n)$. Θεωρούμε συνάρτηση $\phi : \{0,1\}^* \to \{0,1\}^* v$ με $\phi(x) = \langle\varphi_x\rangle$ όπου:

$$\varphi_x = \exists y_1\ \forall y_2 \cdots * y_n\ \varphi_R(\underline{x}, y_1, \dots, y_n)$$

και παρατηρούμε ότι:

l. ϕ πλήρης και υπολογίσιμη.

2. - Αν $x \in L$ τότε:

Υπάρχει y_1*, για κάθε* y_2*, ···, υπάρχει (ή για κάθε)* y_n *ισχύει* $R(x, y_1, \dots, y_n)$.

Αφού ο $\varphi_R(x, y_1, \dots, y_n)$ αναπαριστά το R στο P προκύπτει ότι:

Υπάρχει y_1*, για κάθε* y_2*, ···, υπάρχει (ή για κάθε)* y_n *ισχύει* $P \vdash \varphi_R(\underline{x}, \underline{y_1}, \dots, \underline{y_n})$.

Από το Θεώρημα Εγκυρότητας (λόγω και του ότι $\mathfrak{N} \vDash P$) έπεται ότι:

Υπάρχει y_1*, για κάθε* y_2*, ···, υπάρχει (ή για κάθε)* y_n *ισχύει* $\mathfrak{N} \vDash \varphi_R(\underline{x}, \underline{y_1}, \dots, \underline{y_n})$.

Οπότε από τον Ορ. Tarski έχουμε $\mathfrak{N} \vDash \exists y_1\ \forall y_2 \cdots * y_n\ \varphi_R(\underline{x}, y_1, \dots, y_n)$. Άρα $\mathfrak{N} \vDash \varphi_x$ και τελικά $\langle\varphi_x\rangle \in T_n$.

- Αν $x \notin L$ με αντίστοιχο τρόπο καταλήγουμε ότι $\langle\varphi_x\rangle \notin T_n$.

Συνεπώς $L \leq_m T_n$. □

Ορισμός 8.5.11. Ορίζουμε τη γλώσσα:

$$Truth = \{\langle\varphi\rangle \in \{0,1\}^* \mid \varphi \text{ πρόταση και } \mathfrak{N} \vDash \varphi\}$$

Θεώρημα 8.5.12 (Θεώρημα Tarski). Η γλώσσα $Truth$ δεν ανήκει στην Αριθμητική Ιεραρχία.

[1] Δες Ορισμούς Α.2.5, Α.5.l και Α.5.2

Απόδειξη. Έστω (προς άτοπο) ότι η $Truth$ ανήκει στην Αριθμητική Ιεραρχία, δηλαδή υπάρχει $n \in \mathbb{N}$ τέτοιο ώστε $Truth \in \Sigma_n^0$. Παρατηρούμε ότι $T_{n+1} \leq_m Truth$ [1]. Από το Θεώρημα 8.5.10 η T_{n+1} είναι Σ_{n+1}^0-δύσκολη ως προ τη $\leq_m$, άρα έπεται ότι $HP_{n+1} \leq_m T_{n+1}$. Από τη μεταβατικότητα της $\leq_m$ έπεται ότι $HP_{n+1} \leq_m Truth$. Τέλος, από την Πρόταση 8.3.3 προκύπτει ότι $HP_{n+1} \leq_T Truth$, δηλαδή ότι $HP_{n+1} \in \mathsf{REC}^{Truth} \subseteq \mathsf{REC}^{\Sigma_n^0} = \Delta_{n+1}^0$. Όμως, από την Παρατήρηση 8.2.9, γνωρίζουμε ότι $\Delta_{n+1}^0 \subseteq \mathsf{REC}^{HP_n}$, οπότε $HP_{n+1} \in \mathsf{REC}^{HP_n}$ πράγμα που φυσικά αντιβάινει στο Λήμμα 8.2.6. □

Το παραπάνω θεώρημα μας αποδεικνύει ότι υπάρχουν γλώσσες που δεν ανήκουν σε καμία κλάση της αριθμητικής ιεραρχίας. Μία επέκταση της Αριθμητικής Ιεραρχίας είναι η *Αναλυτική Ιεραρχία* η οποία ορίζεται πάνω σε λογικούς τύπους της *δευτεροβάθμιας λογικής*.

Ασκήσεις

8.1 (★☆☆). Δείξτε ότι η συνάρτηση K της Άσκησης 7.5 είναι υπολογίσιμη χρησιμοποιώντας μαντείο για τη γλώσσα $L_{\text{Αποδοχής}}$.

8.2 (☆☆☆). Δείξτε ότι μια γλώσσα $L \subseteq \{0,1\}^*$ είναι αναδρομική (αναδρομικά απαριθμήσιμη) ανν για κάθε γλώσσα $L' \subseteq \{0,1\}^*$ υπάρχει OTM $M^{L'}$ που αποφασίζει (ημι-αποφασίζει αντίστοιχα) την L.

8.3 (★☆☆). Έστω γλώσσες $A, B, C \subseteq \{0,1\}^*$. Ισχύει ότι αν $A \in \mathsf{RE}^B$ και $B \in \mathsf{RE}^C$ τότε $A \in \mathsf{RE}^C$;

8.4 (☆☆☆). Έστω $A, B \in \{0,1\}^*$. Δείξτε ότι $A \leq_T B$ ανν $\overline{A} \leq_T \overline{B}$.

8.5 (★★★). Δείξτε ότι υπάρχουν δύο γλώσσες $A, B \in \{0,1\}^*$ τέτοιες ώστε $A \not\leq_T B$ και $B \not\leq_T A$.

8.6 (★☆☆). Αποδείτε το Θεώρημα 8.4.4 για n=1.

8.7 (★★☆). Αποδείτε το Θεώρημα 8.4.5.

8.8 (★☆☆). Δείξτε ότι για κάθε $n \geq 1$:

- Η HP_n δεν είναι Π_n^0-δύσκολη ως προς την $\leq_m$.
- Η $\overline{HP}_n$ δεν είναι Σ_n^0-δύσκολη ως προς την $\leq_m$.
- Η HP_n δεν είναι Δ_{n+1}^0-δύσκολη ως προς την $\leq_m$.

[1] Η εν λόγω αναγωγή είναι η ταυτοτική συνάρτηση για τις προτάσεις φ που έχουν τη μορφή $\exists y_1 \forall y_2 \cdots * y_{n+1} \psi(y_1, \ldots, y_{n+1})$ ενώ για τις υπόλοιπες λέξεις είναι η σταθερή συνάρτηση με τιμή $\langle x \wedge \neg x \rangle$.

8.9 (★☆☆). Κατατάξτε τη γλώσσα $L = \{\langle M\rangle \in \{0,1\} \mid$ Δεν υπάρχει λέξη w που ξεκινάει με 001 τέτοια ώστε $w \in L(M)\}$ στην Αριθμητική Ιεραρχία.

8.10 (★★☆). Έστω A $\leq_m$-πλήρης γλώσσα για το Σ^0_n. Δείξτε ότι η γλώσσα $L^A_{\mathbb{N}} = \{\langle M\rangle \in \{0,1\}^* \mid |L(M^A)| \in \mathbb{N}\}$ είναι $\leq_m$-πλήρηςγια το Σ^0_{n+2}.

8.11 (★★☆). Κατατάξτε τη γλώσσα $L_{\equiv} = \{\langle M_1, M_2\rangle \in \{0,1\}^* \mid L(M_1) = L(M_2)\}$ στην Αριθμητική Ιεραρχία.

8.12 (★★☆). Κατατάξτε τη γλώσσα $L = \{\langle M_1, M_2\rangle \in \{0,1\}^* \mid \epsilon \in L(M_1) \setminus L(M_2)\}$ στην Αριθμητική Ιεραρχία.

8.13 (★★☆). Δείξτε ότι η γλώσσα $L_{\varnothing} = \{\langle M\rangle \in \{0,1\}^* \mid L(M) = \varnothing\}$ είναι $\leq_m$-πλήρης για το Π^0_1.

8.14 (★★★). Δείξτε ότι η γλώσσα $L_{\text{Συνπεπερασμενότητα}} = \{\langle M\rangle \in \{0,1\}^* \mid |\overline{L(M)}| \in \mathbb{N}\}$ είναι $\leq_m$-πλήρης για το Σ^0_3.

ΠΑΡΑΡΤΗΜΑ Α

ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΠΡΩΤΟΒΑΘΜΙΑ ΛΟΓΙΚΗ

Α.1 Βασικές έννοιες

Ορισμός Α.1.1. Μία *πρωτοβάθμια γλώσσα* Γ_1 αποτελείται από:

1. Ένα άπειρο σύνολο *μεταβλητών* $M(\Gamma_1) = \{x_0, x_1, ...\}$.
2. Τους *λογικούς συνδέσμους* $\neg, \rightarrow$ (οι σύνδεσμοι $\vee, \wedge, \leftrightarrow$ εισάγονται ως συντομεύσεις).
3. Τις παρενθέσεις $(,)$.
4. Το *σύμβολο της ισότητας* $\approx$.
5. Τον *καθολικό ποσοδείκτη* $\forall$ (ο υπαρξιακός ποσοδείκτης $\exists$ εισάγεται ως συντόμευση).
6. Για κάθε φυσικό $n \geq 0$ ένα σύνολο (ενδεχομένως κενό) $\{P_i \mid i \in I\}$ από *n-μελή κατηγορηματικά σύμβολα*.
7. Για κάθε φυσικό $n \geq 0$ ένα σύνολο (ενδεχομένως κενό) $\{f_i \mid i \in I\}$ από *n-θέσια συναρτησιακά σύμβολα*. Τα 0-θέσια συναρτησιακά σύμβολα καλούνται *σταθερές*.

Σημείωση Α.1.2. Τα σύμβολα των κατηγοριών 2.–5. καλούνται *λογικά σύμβολα* και είναι ίδια για κάθε πρωτοβάθμια γλώσσα. Τα σύνολα των κατηγοριών 6.–7. περιέχουν τα *μη-λογικά σύμβολα* μίας γλώσσας και αλλάζουν από γλώσσα σε γλώσσα. Τα σύμβολα αυτά –σε αντίθεση με τα λογικά σύμβολα– μπορούν να «ερμηνευτούν» στη μεταγλώσσα με πάρα πολλούς τρόπους [1].

Ορισμός Α.1.3. Μία λέξη του Γ_1^* είναι *όρος της* Γ_1 ανν:

[1] Οι πρωτοβάθμιες γλώσσες της λογικής δεν θα πρέπει να συγχέονται με τις γλώσσες που ορίσαμε στην Παράγραφο 0.2, καθώς εκεί είχαμε πεπερασμένο αλφάβητο ενώ εδώ έχουμε ένα αριθμησίμως άπειρο σύνολο συμβόλων.

1. είναι μεταβλητή,

2. είναι σταθερά,

3. είναι της μορφής $ft_1, \dots, t_n$, όπου $t_1, \dots, t_n$ όροι και f n-θέσιο συναρτησιακό σύμβολο της Γ_1 [1].

Το σύνολο των όρων της Γ_1 το συμβολίζουμε ως $O(\Gamma_1)$.

Ορισμός Α.1.4. Μία λέξη του Γ_1^* είναι *τύπος της* Γ_1 ανν:

1. είναι της μορφής $\approx t_1 t_2$, όπου $t_1, t_2 \in O(\Gamma_1)$ [2],

2. είναι της μορφής $Rt_1, \dots, t_n$ όπου $t_1, \dots, t_n \in O(\Gamma_1)$ και R n-μελές κατηγορηματικό σύμβολο της Γ_1 [3],

3. είναι της μορφής $(\neg\varphi), (\varphi \to \psi), (\forall x\varphi)$ όπου φ, ψ τύποι της Γ_1 και x μεταβλητή της Γ_1.

Το σύνολο των τύπων της Γ_1 το συμβολίζουμε ως $T(\Gamma_1)$. Οι τύποι της μορφής 1. και 2. ονομάζονται *ατομικοί τύποι.*

Σύμβαση Α.1.5. Θα γράφουμε $(\exists x\varphi), (\varphi \wedge \psi), (\varphi \vee \psi)$ και $(\varphi \leftrightarrow \psi)$ αντί για $(\neg(\forall x(\neg\varphi)))$, $(\neg(\varphi \to (\neg\psi))), ((\neg\varphi) \to \psi)$ και $((\varphi \to \psi) \wedge (\psi \to \varphi))$. Επίσης θα παραλείπουμε όσες παρενθέσεις δεν είναι απαραίτητες για τη μοναδική αναγνωσιμότητα ενός τύπου (όπως είναι για παράδειγμα οι εξωτερικές παρενθέσεις).

Ορισμός Α.1.6. Έστω $\varphi \in T(\Gamma_1)$ και μεταβλητή x. Η x *εμφανίζεται ελεύθερη στον* φ ανν:

1. Ο φ είναι ατομικός (και φυσικά) η x εμφανίζεται στον φ.

2. Ο φ είναι της μορφής $(\neg\psi)$ και η x εμφανίζεται ελεύθερη στον ψ.

3. Ο φ είναι της μορφής $(\chi \to \psi)$ και η x εμφανίζεται ελεύθερη στον χ ή στον ψ.

4. Ο φ είναι της μορφής $(\forall y\psi)$ και η x εμφανίζεται ελεύθερη στον ψ (όπου $y \neq x$).

Μία εμφάνιση μεταβλητής που δεν είναι ελεύθερη θα ονομάζεται *δεσμευμένη.* Αν στον τύπο φ όλες οι εμφανίσεις μεταβλητών είναι δεσμευμένες τότε ο φ καλείται *πρόταση της* Γ_1.

Συμβολισμός Α.1.7. Θα γράφουμε $\varphi(x_1, \dots, x_n)$ για να δηλώνουμε το γεγονός ότι οι μεταβλητές $x_1, \dots, x_n$ (και μόνο αυτές) εμφανίζονται ελεύθερες στον φ.

[1] Αντί για $ft_1, \dots, t_n$ από εδώ και στο εξής θα γράφουμε $f(t_1, \dots, t_n)$.
[2] Αντί για $\approx t_1 t_2$ από εδώ και στο εξής θα γράφουμε $t_1 \approx t_2$.
[3] Αντί για $Rt_1, \dots, t_n$ από εδώ και στο εξής θα γράφουμε $R(t_1, \dots, t_n)$.

Α.2 Σημασιολογία

Ορισμός Α.2.1. Έστω πρωτοβάθμια γλώσσα Γ_1. *Δομή (ή ερμηνεία)* $\mathfrak{A}$ για τη Γ_1 είναι ένα σύστημα αποτελούμενο από:

1. Ένα μη κενό σύνολο A (το *σύμπαν* της δομής, συνήθως το συμβολίζουμε $|\mathfrak{A}|$).
2. Για κάθε n-μελές κατηγορηματικό σύμβολο P μία n-μελή σχέση $P^{\mathfrak{A}} \subseteq A^n$.
3. Για κάθε n-θέσιο συναρτησιακό σύμβολο μία συνάρτηση $f^{\mathfrak{A}} : A^n \to A$.
4. Για κάθε σύμβολο σταθεράς c μία τιμή $c^{\mathfrak{A}} \in A$.

Παρατήρηση Α.2.2. Είδισται όταν ορίζουμε μία πρωτοβάθμια γλώσσα να έχουμε στο μυαλό μας μία ερμηνεία για τα μη-λογικά σύμβολά της. Αυτήν την ερμηνεία συνήθως την αποκαλούμε *προτιθέμενη* (δες Ορισμό Α.5.2 για ένα παράδειγμα).

Ορισμός Α.2.3. Έστω πρωτοβάθμια γλώσσα Γ_1 και δομή $\mathfrak{A}$. *Αποτίμηση* είναι μία συνάρτηση $v : M(\Gamma_1) \to |\mathfrak{A}|$. Επεκτείνουμε την αποτίμηση v σε μία συνάρτηση $\bar{v} : O(\Gamma_1) \to |\mathfrak{A}|$ έτσι ώστε:

1. $\bar{v}(c) = c^{\mathfrak{A}}$, όπου c σταθερά της Γ_1.
2. $\bar{v}(f(t_1, \dots, t_n)) = f^{\mathfrak{A}}(\bar{v}(t_1), \dots, \bar{v}(t_n))$, όπου f n-θέσιο συναρτησιακό σύμβολο της Γ_1 και $t_1, \dots, t_n \in O(\Gamma_1)$.

Ορισμός Α.2.4. Έστω πρωτοβάθμια γλώσσα Γ_1, δομή $\mathfrak{A}$, αποτίμηση v και μεταβλητή x. Ορίζουμε την αποτίμηση $v(x/a)$, όπου $a \in |\mathfrak{A}|$, ως εξής:

$$v(x/a)(y) = \begin{cases} a & , \text{ αν } y = x \\ v(y) & , \text{ αλλιώς} \end{cases}$$

Ορισμός Α.2.5 (Ορισμός αλήθειας Tarski). Έστω πρωτοβάθμια γλώσσα Γ_1, δομή $\mathfrak{A}$, αποτίμηση v και $\varphi \in T(\Gamma_1)$. Θα λέμε ότι *η ερμηνεία $\mathfrak{A}$ ικανοποιεί τον τύπο φ για την αποτίμηση v*, συμβολισμός $\mathfrak{A} \vDash \varphi[v]$, ανν:

1. Ο φ είναι της μορφής $t_1 \approx t_2$, όπου $t_1, t_2 \in O(\Gamma_1)$, και ισχύει ότι $\bar{v}(t_1) = \bar{v}(t_2)$.
2. Ο φ είναι της μορφής $R(t_1, \dots, t_n)$, και ισχύει ότι $(\bar{v}(t_1), \dots, \bar{v}(t_n)) \in R^{\mathfrak{A}}$.
3. Ο φ είναι της μορφής $(\neg\chi)$, και δεν ισχύει ότι $\mathfrak{A} \vDash \chi[v]$.
4. Ο φ είναι της μορφής $(\chi \to \psi)$, και ισχύει ότι αν $\mathfrak{A} \vDash \chi[v]$ τότε $\mathfrak{A} \vDash \psi[v]$.
5. Ο φ είναι της μορφής $(\forall x\chi)$, και ισχύει ότι για κάθε $a \in |\mathfrak{A}|$, $\mathfrak{A} \vDash \chi[v(x/a)]$.

Ορισμός Α.2.6. Έστω $\varphi \in T(\Gamma_1)$ και $T \subseteq T(\Gamma_1)$. Θα λέμε ότι:

1. Ο τύπος φ είναι *ικανοποιήσιμος* ανν υπάρχει δομή $\mathfrak{A}$ και αποτίμηση v τέτοια ώστε $\mathfrak{A} \vDash \varphi[v]$. Σε αυτήν την περίπτωση θα λέμε ότι *οι $\mathfrak{A}, v$ ικανοποιούν τον φ* [1].

[1] Αν ο φ είναι πρόταση η ικανοποιησιμότητά του είναι ανεξάρτητη από την εκάστοτε αποτίμηση, καθώς δεν εμφανίζονται σε αυτόν ελεύθερες μεταβλητές.

2. *Η δομή* $\mathfrak{A}$ *και η αποτίμηση* v *ικανοποιούν το* T ανν ικανοποιούν κάθε στοιχείο του T.

3. Το T είναι *ικανοποιήσιμο* αν και μόνον αν υπάρχουν δομή $\mathfrak{A}$ και αποτίμηση v που το ικανοποιούν.

4. Το T *συνεπάγεται λογικά* τον φ, συμβολισμός $T \vDash \varphi$, ανν κάθε δομή και αποτίμηση που ικανοποιούν το T ικανοποιούν και το φ.

Συμβολισμός Α.2.7. Καθώς μία πρόταση φ ικανοποιείται σε μία δομή $\mathfrak{A}$ ανεξάρτητα από την αποτίμηση (όλες οι μεταβλητές εμφανίζονται δεσμευμένες στη φ) θα γράφουμε $\mathfrak{A} \vDash \varphi$ και θα λέμε ότι η $\mathfrak{A}$ είναι *μοντέλο* της φ. Επίσης αν ο τύπος $\forall x\chi$ είναι πρόταση, εφαρμόζοντας τον Ορισμό του Tarski θα γράφουμε $\mathfrak{A} \vDash \forall x\chi$ ανν για κάθε $a \in |\mathfrak{A}|$, $\mathfrak{A} \vDash \chi(x/a)$. Τέλος, αντί για $\neg(t_1 \approx t_2)$, όπου $t_1,\ t_2$ όροι, θα γράφουμε $t_1 \not\approx t_2$.

Α.3 Τυπικές αποδείξεις

Ορισμός Α.3.1. Έστω πρωτοβάθμια γλώσσα Γ_1. Ένα *αξιωματικό σύστημα* $\mathcal{A}$ για την Γ_1 αποτελείται από

1. ένα σύνολο *αξιωμάτων* $A \subseteq T(\Gamma_1)$ και

2. ένα σύνολο *αποδεικτικών κανόνων* K,

όπου *αποδεικτικός κανόνας* $\kappa \in K$ είναι μια διμελής σχέση $\kappa \in 2^{T(\Gamma_1)} \times T(\Gamma_1)$. Αν $(B, \varphi) \in \kappa$, τότε λέμε ότι *ο* φ *είναι άμεσο συμπέρασμα της εφαρμογής του* κ *στα στοιχεία του* B. Το A χωρίζεται σε δύο ξένα σύνολα Λ και M (δηλαδή $A = \Lambda \cup M$), όπου Λ είναι το σύνολο των *λογικών αξιωμάτων* (το ίδιο για κάθε γλώσσα) και M το σύνολο των *μη-λογικών αξιωμάτων* (διαφέρει για κάθε γλώσσα).

Ορισμός Α.3.2. Έστω $\mathcal{A} = (A, K)$ ένα αξιωματικό σύστημα, $T \subseteq T(\Gamma_1)$, και φ τύπος. Θα λέμε ότι *ο* φ *αποδεικνύεται* από τα στοιχεία του T (το *σύνολο υποθέσεων*) στο $\mathcal{A}$, συμβολισμός $T \vdash_{\mathcal{A}} \varphi$, αν υπάρχει μία πεπερασμένη ακολουθία τύπων $\tau_1, \dots, \tau_n$, όπου $\tau_n = \varphi$, και για κάθε τ_i ισχύει ένα από τα ακόλουθα:

1. $\tau_i \in A \cup T$, είναι δηλαδή αξίωμα ή *υπόθεση*, ή

2. το τ_i είναι άμεσο συμπέρασμα της εφαρμογής κανόνα $\kappa \in K$ σε ένα σύνολο $S \subseteq \{\tau_1, \dots, \tau_{i-1}\}$.

Συμβολισμός Α.3.3. Έστω x μεταβλητή, t όρος, και φ τύπος της Γ_1. Συμβολίζουμε με φ_t^x τον τύπο που προκύπτει από τον φ, με αντικατάσταση όλων των ελεύθερων εμφανίσεων της x από τον όρο t.

Ορισμός Α.3.4. Η μεταβλητή x καλείται *αντικαταστάσιμη* από τον όρο t στον τύπο φ, αν με την αντικατάσταση των ελεύθερων εμφανίσεων της x από τον t στον φ, δεν δεσμεύονται μεταβλητές του t.

Ορισμός Α.3.5. Γενίκευση του φ καλείτε οποιοσδήποτε τύπος της μορφής $\forall x_1 \cdots \forall x_n \varphi$, όπου x_i μεταβλητές για $n \geq 0$.

Ορισμός Α.3.6. Το αξιωματικό σύστημα $\mathcal{A}_1 = (A_1, K_1)$ για την πρωτοβάθμια λογική, έχει ως λογικά αξιώματα όλες τις γενικεύσεις των ακόλουθων *αξιωματικών σχημάτων* [1]:

ΑΣ1 $\varphi \to (\psi \to \varphi)$

ΑΣ2 $(\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi))$

ΑΣ3 $(\neg\varphi \to \neg\psi) \to ((\neg\varphi \to \psi) \to \varphi)$

ΑΣ4 $\forall x \varphi \to \varphi_t^x$, με την προϋπόθεση ότι η μεταβλητή x είναι αντικαταστάσιμη από τον όρο t στον φ

ΑΣ5 $\forall x(\varphi \to \psi) \to (\forall x\varphi \to \forall x\psi)$

ΑΣ6 $\varphi \to \forall x\varphi$, με την προϋπόθεση ότι η x δεν εμφανίζεται ελεύθερη στον φ

ΑΣ7 $x \approx x$

ΑΣ8 $x \approx y \to (\varphi \to \varphi^*)$, όπου φ ατομικός τύπος, και φ^* ο (ατομικός) τύπος που προκύπτει από τον φ αντικαθιστώντας μερικές (ή και όλες) τις εμφανίσεις της x από τη y

και K_1 που περιέχει μόνον έναν κανόνα, τον *Modus Ponens (M.P.)*:

$$\frac{\varphi \qquad \varphi \to \psi}{\psi}\ \text{M.P.}$$

Σύμβαση Α.3.7. Αντί για $T \vdash_{\mathcal{A}_1} \varphi$ θα γράφουμε $T \vdash \varphi$ και αντί για $\varnothing \vdash \varphi$ θα γράφουμε $\vdash \varphi$. Παρατηρήστε επίσης ότι μπορούμε να θεωρήσουμε το σύνολο των μη λογικών αξιωμάτων ως υποθέσεις.

Ορισμός Α.3.8. Έστω T σύνολο μη-λογικών αξιωμάτων για μία πρωτοβάθμια γλώσσα Γ_1. Το T είναι *συνεπές* ανν δεν υπάρχει $\varphi \in T(\Gamma_1)$ τέτοιος ώστε $T \vdash \varphi$ και $T \vdash \neg\varphi$.

Α.4 Τα Θεωρήματα Εγκυρότητας και Πληρότητας

Θεώρημα Α.4.1 (Θεώρημα Εγκυρότητας). Για κάθε σύνολο τύπων T και τύπο φ μίας πρωτοβάθμιας γλώσσας ισχύει ότι αν $T \vdash \varphi$ τότε $T \vDash \varphi$.

Θεώρημα Α.4.2 (Θεώρημα Πληρότητας). Για κάθε σύνολο τύπων T και τύπο φ μίας πρωτοβάθμιας γλώσσας ισχύει ότι αν $T \vDash \varphi$ τότε $T \vdash \varphi$.

[1] Περιέχει δηλαδή όλους τους τύπους που μπορούν να προκύψουν αν αντικαταστήσουμε τις συντακτικές μεταβλητές (φ, ψ, χ, t, x και y) σε αυτά τα «σχήματα» με οποιουσδήποτε τύπους της γλώσσας που εξετάζουμε.

Ο μη εξοικειωμένος με τη λογική αναγνώστης θα βρίσκεται σίγουρα σε σύγχυση από το γεγονός πως έχουμε ένα Θεώρημα Πληρότητας και ένα Θεώρημα Μη-πληρότητας. Το Θεώρημα Μη-πληρότητας αφορά όμως δύο «διαφορετικές» (και ισοδύναμες μεταξύ τους) έννοιες πληρότητας από αυτήν του Θεωρήματος Α.4.2: την *τυπική πληρότητα* ενός συνόλου αξιωμάτων (ή υποθέσεων) και την *πληρότητα ως προς μοντέλο* του συνόλου αξιωμάτων.

Ορισμός Α.4.3. Έστω A σύνολο με λογικών αξιωμάτων για τη Γ_1 και $\mathfrak{A}$ μοντέλο του A.

1. Το A είναι *τυπικά πλήρες* ανν για κάθε πρόταση φ της Γ_1 ισχύει ότι $A \vdash \varphi$ ή $A \vdash \neg\varphi$.
2. Το A είναι *πλήρες ως προς το* $\mathfrak{A}$ ανν για κάθε πρόταση φ της Γ_1, αν ισχύει ότι $\mathfrak{A} \vDash \varphi$ τότε $A \vdash \varphi$.

Ο παραπάνω Ορισμός (το 2.) ίσως προσθέτει ακόμα μεγαλύτερη σύγχυση, καθώς από το Θεώρημα Α.4.2 προκύπτει ότι (αφού $\mathfrak{A} \vDash A$) αν $A \vDash \varphi$ (οπότε και $\mathfrak{A} \vDash \varphi$) θα έχουμε ότι $A \vdash \varphi$. Το Θεώρημα Α.4.1 όμως για να ισχύσει απαιτεί κάτι πολύ πιο ειδικό από την προϋπόθεση (του 2. του) του Ορισμού Α.4.3: Απαιτεί από όλα τα μοντέλα του A να ικανοποιούν τον φ και όχι μόνο το $\mathfrak{A}$. Τέλος, η πληρότητα ως προς μοντέλο προϋποθέτει την ύπαρξη ενός μοντέλου για το A, δηλαδή ότι το A είναι ικανοποιήσιμο. Αυτό δεν μπορεί να ισχύει αν το A δεν είναι συνεπές (γιατί;) [1].

Α.5 Αριθμητική Peano

Ορισμός Α.5.1. Η γλώσσα της *Θεωρίας Αριθμών*, συμβολισμός $\Gamma_1^{\partial\alpha}$, αποτελείται από τη σταθερά $\mathbf{0}$, το μονοθέσιο συναρτησιακό σύμβολο $\prime$, και τα διθέσια συναρτησιακά σύμβολα $\oplus$ και $\odot$.

Ορισμός Α.5.2. Η *κύρια (ή προτιθέμενη) ερμηνεία* για τη $\Gamma_1^{\partial\alpha}$ είναι η $\mathfrak{N}$ όπου:

- $|\mathfrak{N}| = \mathbb{N}$ (σύμπαν είναι οι φυσικοί αριθμοί),
- $\prime^{\mathfrak{N}} = \mathsf{S}$ (η συνάρτηση του επόμενου),
- $\oplus^{\mathfrak{N}} = +$ (η συνάρτηση της πρόσθεσης),
- $\odot^{\mathfrak{N}} = \cdot$ (η συνάρτηση του πολλαπλασιασμού),
- $\mathbf{0}^{\mathfrak{N}} = 0$ (το μηδέν).

Ορισμός Α.5.3. Το σύνολο P των (μη-λογικών) αξιωμάτων της *αριθμητικής Peano* για τη $\Gamma_1^{\partial\alpha}$ είναι το εξής:

P1 $\forall x_1 (x_1\prime \not\approx \mathbf{0})$

P2 $\forall x_1 \forall x_2 (x_1\prime = x_2\prime \to x_1 = x_2)$

[1] Αν το A δεν είναι συνεπές είναι όμως τετριμμένα τυπικά πλήρες. Αυτό ισχύει επειδή αν μπορούμε να αποδείξουμε έναν τύπο και την άρνηση του μπορούμε να αποδείξουμε οποιονδήποτε τύπο καθώς $\vdash \neg\varphi \to (\varphi \to \psi)$.

P3 $\forall x_1(x_1 \oplus \mathbf{0} = x_1)$

P4 $\forall x_1 \forall x_2(x_1 \oplus x_2\prime = (x_1 \oplus x_2)\prime)$

P5 $\forall x_1(x_1 \odot \mathbf{0} = \mathbf{0})$

P6 $\forall x_1 \forall x_2(x_1 \odot x_2\prime = x_1 \odot x_2 \oplus x_2)$

P7 $\forall x_1 \cdots \forall x_n(\varphi(x_1, \dots, x_n, \mathbf{0}) \wedge \forall x_0(\varphi(x_1, \dots, x_n, x_0) \to \varphi(x_1, \dots, x_n, x_0\prime)) \to \forall x_0 \varphi(x_1, \dots, x_n, x_0))$

Συμβολισμός Α.5.4. Συμβολίζουμε με $\underline{n}$ τον όρο που αντιστοιχεί στο *ψηφίο* του αριθμού $n \in \mathbb{N}$, δηλαδή

$$\underline{n} = \mathbf{0}\underbrace{\prime\prime\cdots\prime}_{n\text{-φορές}}$$

Ορισμός Α.5.5. Έστω $T \subseteq T(\Gamma_1^{\mathfrak{Da}})$ και $R \subseteq \mathbb{N}^n$, όπου $n \geq 1$. Η σχέση R είναι *αναπαραστάσιμη στο* T ανν υπάρχει τύπος $\varphi(x_1, \dots, x_n)$ τέτοιος ώστε για κάθε $m_1, \dots, m_n \in \mathbb{N}$ να ισχύει ότι:

1. αν $(m_1, \dots, m_n) \in R$ τότε $T \vdash \varphi(\underline{m_1}, \dots, \underline{m_n})$
2. αν $(m_1, \dots, m_n) \notin R$ τότε $T \vdash \neg\varphi(\underline{m_1}, \dots, \underline{m_n})$

Αντίστοιχα, μία συνάρτηση $f : \mathbb{N}^n \to \mathbb{N}$ είναι *αναπαραστάσιμη στο* T ανν υπάρχει τύπος $\varphi(x_1, \dots, x_{n+1})$ τέτοιος ώστε για κάθε $m_1, \dots, m_{n+1} \in \mathbb{N}$ να ισχύει ότι:

1. αν $f(m_1, \dots, m_n) = m_{n+1}$ τότε $T \vdash \varphi(\underline{m_1}, \dots, \underline{m_{n+1}})$
2. αν $f(m_1, \dots, m_n) \neq m_{n+1}$ τότε $T \vdash \neg\varphi(\underline{m_1}, \dots, \underline{m_{n+1}})$

Θεώρημα Α.5.6. Κάθε ελαχιστικά αναδρομική συνάρτηση είναι αναπαραστάσιμη στο P.

Το παραπάνω Θεώρημα μας δίνει το δικαίωμα να περάσουμε από τον κόσμο των αριθμητικών συναρτήσεων στους τύπους της $\Gamma_1^{\mathfrak{Da}}$. Ισχύει και το αντίστροφό του, με την προϋπόθεση όμως ότι το P είναι συνεπές.

Α.5.1 Αριθμητικοποίηση

Σημείωση Α.5.7. Έχει επικρατήσει η διαδικασία που αντιστοιχεί φυσικούς αριθμούς σε «οντότητες», όπως είναι οι ακολουθίες φυσικών αριθμών ή οι λογικοί τύποι, να αποκαλείται *αριθμητικοποίηση*.Ένα Παράδειγμα είδαμε στο Κεφάλαιο 2, άλλο ένα θα δούμε εδώ.

Τελευταία ενημέρωση 10/1/2025, στις 08:17.

Αριθμητικοποίηση των τύπων της $\Gamma_1^{\partial\alpha}$

Αντιστοιχούμε σε κάθε σύμβολο της $\Gamma_1^{\partial\alpha}$ έναν φυσικό αριθμό ως εξής:

$$\begin{array}{l|l} \langle x_i\rangle_{\mathbb{N}} = 3^{i+1},\ i=0,1,... & \langle\approx\rangle_{\mathbb{N}} = 19 \\ \langle\neg\rangle_{\mathbb{N}} = 5 & \langle\prime\rangle_{\mathbb{N}} = 23 \\ \langle\to\rangle_{\mathbb{N}} = 7 & \langle\oplus\rangle_{\mathbb{N}} = 27 \\ \langle\forall\rangle_{\mathbb{N}} = 11 & \langle\odot\rangle_{\mathbb{N}} = 29 \\ \langle(\rangle_{\mathbb{N}} = 13 & \langle\mathbf{0}\rangle_{\mathbb{N}} = 31 \\ \langle)\rangle_{\mathbb{N}} = 17 & \end{array}$$

Έστω $\varphi = a_1\cdots a_n \in T(\Gamma_1^{\partial\alpha})$, όπου $a_1,...,a_n \in \{\neg,\to,\forall,(,),\approx,\prime,\oplus,\odot,\mathbf{0}\}\cup M(\Gamma_1^{\partial\alpha})$, αντιστοιχούμε στον φ τον αριθμό:

$$\langle\varphi\rangle_{\mathbb{N}} = \mathsf{enc}_n(\langle a_1\rangle_{\mathbb{N}},...,\langle a_n\rangle_{\mathbb{N}})$$

όπου enc_n η συνάρτηση του Ορισμού 2.3.1. Ο αριθμός $\langle\varphi\rangle_{\mathbb{N}}$ καλείται *αριθμός Gödel* του φ.

Έστω $\varphi_1,...,\varphi_n$ πεπερασμένη ακολουθία τύπων της $\Gamma_1^{\partial\alpha}$. Αντιστοιχούμε την ακολουθία αυτή στον αριθμό:

$$\langle\varphi_1,...,\varphi_n\rangle_{\mathbb{N}} = \mathsf{enc}_n(\langle\varphi_1\rangle_{\mathbb{N}},...,\langle\varphi_n\rangle_{\mathbb{N}})$$

Παρατηρήστε ότι κατά αυτόν τον τρόπο μπορούμε να αντιστοιχίσουμε τυπικές αποδείξεις από το P σε φυσικούς αριθμούς.

Παρατήρηση Α.5.8. Υπάρχει ΤΜ $M_{\mu\to\varphi}$ που δέχεται σαν είσοδο την κωδικοποίηση μίας ελαχιστικά αναδρομικής συνάρτησης f και επιστρέφει τον αριθμό Gödel του τύπου φ που την αναπαριστά.

Για να κατασκευάσουμε την ΤΜ $M_{\mu\to\varphi}$ πρέπει πρώτα να περάσουμε μέσα από τις λεπτομέρειες της απόδειξης του Θεωρήματος Α.5.6, θέμα που ξεφεύγει των σκοπών αυτών των σημειώσεων.

Πρόταση Α.5.9. Η σχέση $\mathsf{Proof}\subseteq\mathbb{N}^2$ με $(x,y)\in\mathsf{Proof}$ ανν

> *"Ο y είναι αριθμός που αντιστοιχεί σε τυπική απόδειξη από το P της οποίας ο τελευταίος τύπος είναι ο τύπος με αριθμό Gödel x."*

είναι ελαχιστικά αναδρομική.

Σημείωση Α.5.10. Για να αποδείξουμε ότι η Proof είναι ελαχιστικά αναδρομική σχέση πρέπει πρώτα να αποδείξουμε ότι 16 ακόμα συναρτήσεις και σχέσεις [1] είναι ελαχιστικά αναδρομικές

Θεώρημα Α.5.11. Κάθε n-μελές αποφάνσιμο κατηγόρημα R είναι αναπαραστάσιμο στο P από έναν τύπο με n-ελεύθερες μεταβλητές.

[1] Οι σχέσεις αυτές ελέγχουν παραδείγματος χάρη αν ο x είναι αριθμός Gödel τύπου της $\Gamma_1^{\partial\alpha}$, αν ο x είναι αριθμός Gödel αξιώματος, αν ο x είναι αριθμός που αντιστοιχεί σε τυπική απόδειξη κλπ..

Απόδειξη. Αφού το R είναι αποφάνσιμο κατηγόρημα έπεται ότι $L_R \in \mathsf{REC}$. Παρατηρούμε ότι η χαρακτηριστική συνάρτηση της L_R είναι υπολογίσιμη (δες Πρόταση 1.2.38), άρα από το Θεώρημα 2.5.1 είναι ελαχιστικά αναδρομική και από το Θεώρημα Α.5.6 είναι αναπαραστάσιμη στο P, έστω από τον τύπο $\varphi_R(y_1, \dots, y_n, x)$. Ο τύπος $\varphi_R(y_1, \dots, y_n, \underline{1})$ αναπαριστά το R. □

ΒΙΒΛΙΟΓΡΑΦΙΑ

Οι σημειώσεις αυτές βασίστηκαν (κατά κύριο λόγο) στα μαθήματα που διδάχθηκα από τον Καθ. Δ. Μ. Θηλυκό και στα ακόλουθα:

Επιστημονικά συγγράμματα:

[1] Michael Sipser: *Εισαγωγή στην Θεωρία Υπολογισμού*, Πανεπιστημιακές Εκδόσεις Κρήτης.

[2] Harry R. Lewis, Χρήστος Παπαδημητρίου: *Στοιχεία Θεωρίας Υπολογισμού*, Εκδόσεις Κριτική.

[3] John E. Hopcroft, Jefrey D. Ullman: *Introduction to Automata Theory, Languages, and Computation (1st edition)*, Addison-Wesley.

[4] Dexter C. Kozen: *Automata and Computability*, Springer.

[5] Γιάννης Ν. Μοσχοβάκης: *Αναδρομή και Υπολογισιμότητα*.

[6] Αθανάσιος Τζουβάρας: *Θεωρία Αναδρομικών Συναρτήσεων και Υπολογισιμότητας*.

[7] Thomas Sudkamp: *Languages and Machines An Introduction to the Theory of Computer Science (3rd Edition)*, Pearson.

[8] Κώστας Ι. Δημητρακόπουλος: *Σημειώσεις Μαθηματικής Λογικής*.

[9] Roland Hausser: *Foundations of Computational Linguistics*, Springer.

[10] J. Roger Hindley, Jonathan P. Seldin: *Lambda-Calculus and Combinators, An Introduction*, Cambridge University Press

[11] Γεώργιος Κολέτσος: *Εφαρμογές της Λογικής στην Πληροφορική (Λάμδα-Λογισμοί)*

Λοιπά συγγράμματα:

[12] Νίκος Καζαντζάκης: *Ασκητική*, Εκδόσεις Καζαντζάκη.

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΕΥΡΕΤΗΡΙΟ ΟΡΩΝ ΚΑΙ ΣΥΜΒΟΛΩΝ

Τελευταία ενημέρωση 10/1/2025, στις 08:17.